

ТЕМА НОМЕРА

# ПРОГРАММНО ОПРЕДЕЛЯЕМЫЕ ХРАНИЛИЩА

Тренды российских ИТ	18	Сертификация СКС	57
Карта вендоров	32	КЗс: сильный и легкий	68
Анализ отказов в ЦОДах	52	Небезопасные мессенджеры	74

ИнформКурьер-Связь

**ИКС**

издается с 1992 года

Дарья  
Алексанкина

*Генеральный  
директор  
C3 Solutions*

**C3 Solutions:  
новые линейки  
и безупречный сервис**

Реклама

# МЕРОПРИЯТИЯ ИКС-МЕДИА



# 2024

CLOUD & CONNECTIVITY 21.03  
СКС. ЦОДы, офисы, общественные  
пространства 09.04  
ЦОД: модели,  
сервисы, инфраструктура 25.04/18.06/26.11

Data Center Design & Engineering 21.05  
ЦОД 2024 05.09  
Data Center & Cloud Kazakhstan 08.10  
Eurasia Data Center & Cloud Forum 05.11

Реклама/16+

## География:

- Москва
- Санкт-Петербург
- Новосибирск
- Екатеринбург
- Ташкент
- Алматы

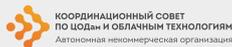


подробнее  
на сайте [iksmedia.ru](https://iksmedia.ru)

Издается с мая 1992 г.

**Издатель**  
ООО «ИКС-МЕДИА»

участник  
АНО КС ЦОД



**Генеральный директор**  
Д.Р. Бедердинов  
dmitry@iksmedia.ru

**Учредитель:**  
ООО «ИКС-МЕДИА»

**Главный редактор**  
А.Г. Барсков  
a.barskov@iksmedia.ru

**РЕДАКЦИЯ**  
iks@iksmedia.ru

**Ответственный редактор**  
Н.Н. Шталтовная  
ns@iksmedia.ru

**Обозреватель**  
Н.В. Носов  
nikolay.nosov@iksmedia.ru

**Корректор**  
Е.А. Краснушкина

**Дизайн и верстка**  
Е.В. Денисова

**КОММЕРЧЕСКАЯ СЛУЖБА**  
Г.Н. Новикова, коммерческий директор – galina@iksmedia.ru  
Е.О. Самохина, ст. менеджер – es@iksmedia.ru  
Д.А. Устинова, ст. менеджер – ustynova@iksmedia.ru  
А.Д. Остапенко, ст. менеджер – a.ostapenko@iksmedia.ru  
Д.Ю. Жаров, координатор – dim@iksmedia.ru

**СЛУЖБА РАСПРОСТРАНЕНИЯ**  
Выставки, конференции  
expro@iksmedia.ru  
Подписка  
podpiska@iksmedia.ru

Журнал «ИнформКурьер-Связь» зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, регистрационный номер ПИ № ФС77-82469 от 30 декабря 2021 г. Мнения авторов не всегда отражают точку зрения редакции. Статьи с пометкой «бизнес-партнер» публикуются на правах рекламы. За содержание рекламных публикаций и объявлений редакция ответственности не несет. Любое использование материалов журнала допускается только с письменного разрешения редакции и со ссылкой на журнал.

Рукописи не рецензируются и не возвращаются.

© «ИнформКурьер-Связь», 2023

**Адрес редакции и издателя:**  
105082, Россия, г. Москва,  
2-й Ирининский пер, д. 3  
Тел./факс: (495) 150-6424  
E-mail: iks@iksmedia.ru  
Адрес в Интернете: www.iksmedia.ru

Дата подписания в печать: 03.11.23.  
Дата выхода в свет: 14.11.23.  
Тираж 5 000 экз. Свободная цена.  
Формат 64x84/8  
Типография: ООО «ПРОПЕЧАТЬ»,  
адрес типографии 119618, г. Москва,  
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

## Ждать нельзя строить



Рынок коммерческих ЦОДов развивается волнообразно. В текущем году – очередной гребень волны: по предварительным данным iKS-Consulting, число стоек вырастет на рекордные 20,7%. Но надо понимать, что вводимые сейчас в эксплуатацию новые ЦОДы начинали проектировать в 2020–2021 гг., когда ставка ЦБ находилась на уровне 5%, а курс доллара – 75 руб. Сегодня деньги стали существенно дороже (ставка ЦБ – 15%), а рубль сильно ослабел (за \$1 дают около 100 руб.), а потому строить ЦОДы становится невыгодно. Окупаемость таких объектов растягивается до 15 лет и более, и они теряют свою инвестиционную привлекательность.

Произошло это во многом из-за существенного увеличения капитальных затрат на строительство ЦОДов. Хотя на рынке оборудования для инженерной инфраструктуры на первые роли все чаще выходят отечественные производители, стоимость их продукции, как правило, привязана к доллару. Причина тоже понятна: ключевые элементы многих инженерных систем – компрессоры, ЕС-вентиляторы, силовая электроника, автоматика – в России не производятся и привозятся из-за рубежа. Да и настоящих производителей в стране немного, в основном сборщики и продавцы, что неудивительно, ведь себестоимость выпуска инженерного оборудования в России существенно, иногда вдвое, выше себестоимости аналогов, производимых в Китае.

Чем чревата ситуация, когда ЦОДы перестают быть привлекательными для инвесторов? Тем, что через два-три года (когда должны были бы «выстрелить» закладываемые сегодня проекты) на рынке ЦОДов возникнет «демографическая яма». Примечательно, что и самим владельцам коммерческих ЦОДов становится выгодно не строить. Дефицит стойко-мест, который возникнет через пару лет, позволит поднять на них цену и больше заработать на уже имеющихся объектах, не рискуя со строительством новых.

Вот только подобная «яма» вряд ли выгодна стране. Ведь дефицит ЦОДов поставит под угрозу цифровизацию экономики, а также выполнение задач перспективного нацпроекта «Экономика данных». Надеюсь, в правительстве это понимают и примут соответствующие меры. Одна из очевидных и наиболее действенных – введение механизма субсидирования кредитной ставки при реализации проектов ЦОДов. И тогда можно будет снова говорить об инвестиционной привлекательности и ускорении развития отрасли.

Поставьте запятую в заголовке правильно,  
**Александр Барсков**



# Программно определяемые хранилища с. 26

## 1 КОЛОНКА РЕДАКТОРА

### 4 ИКС-Панорама

- 4 В будущее – с оптимизмом
- 8 Узбекистан: потребность в современных ЦОДах все острее
- 11 ЦОДы в Казахстане – приоритет высшего уровня
- 14 ДАЙДЖЕСТ ОТРАСЛИ ЦОДов
- 16 Е. Вирцер. Неизменные обязательства в условиях турбулентности

### 18 Экономика и бизнес

- 18 Н. Носов. Новые тренды российских ИТ
- 22 Д. Алексанкина. Новые линейки и безупречный сервис. С3 Solutions – еще ближе к заказчикам
- 24 Д. Аверьянов. Кадровый ЭДО: навигация среди айсбергов. Окончание

### 26 Инфраструктура

- 26 Н. Носов. Программно определяемые хранилища: наращивая функционал
- 30 М. Чусавитин. В чем российские SDS уступают зарубежным



с. 4

В будущее –  
с оптимизмом



с. 24

Д. Аверьянов.  
Кадровый ЭДО: навигация  
среди айсбергов



с. 38

**А. Барсков.**  
**Не доверяй и проверяй!**

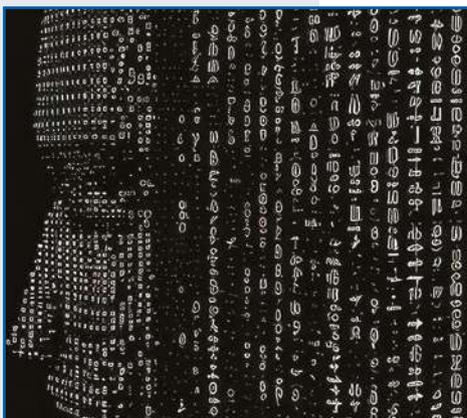


с. 64

**Н. Носов.** Дрон на охране картошки,  
 или Цифровизация в агрокомплексе

**Н. Носов.** «Серый» цифровой профиль,  
 или Все под прицелом

с. 70



- 32** А. Барсков. Карта вендоров – зеркало рынка
- 36** М. Каширских. Охлаждение от Systeme Electric: все, что нужно заказчикам
- 38** А. Барсков. Не доверяй и проверяй!
- 42** В. Халфин. NED: конструктор систем охлаждения для ЦОДов
- 44** Е. Кривоносов, О. Линднер. Не все DCIM-системы одинаково хороши
- 48** А. Тепляков, С. Смолев. Шкафы для любого формата
- 50** А. Чураков. ЕКФ целится в будущие проекты
- 52** Э. Лоуренс, Л. Саймон. Анализ отказов в ЦОДах
- 57** Е. Оганесян. Сертификация СКС: чем и зачем?
- 62** NTSS ODF PROF – компактность и сверхвысокая плотность портов

## 64 Сервисы и приложения

- 64** Н. Носов. Дрон на охране картошки, или Цифровизация в агрокомплексе
- 68** Д. Афанасьев. Сильный, но легкий: K3s – упрощенная версия Kubernetes

## 70 Безопасность

- 70** Н. Носов. «Серый» цифровой профиль, или Все под прицелом
- 74** Н. Носов. Небезопасные мессенджеры
- 77** А. Грецкий. Защита данных в сети

## 79 Новые продукты

# В будущее – с оптимизмом



**Российский рынок коммерческих ЦОДов уверенно преодолевает трудности и продолжает рост. Это подтвердили выступления участников 18-го ежегодного форума «ЦОД», проведенного «ИКС-Медиа».**

Форум «ЦОД» давно стал зеркалом отрасли, отражающим ее проблемы и достижения. На этой площадке делегаты знакомятся с новинками индустрии, налаживают контакты и заключают сделки. Не удивляют традиционно повышенный интерес к мероприятию и переполненные залы. С учетом смотревших прямые трансляции через интернет в форуме участвовало более 1800 человек.

## Стабильный рост

По данным iKS-Consulting, в 2022 г. объем российского рынка коммерческих ЦОДов за год вырос на 28% и составил 89,1 млрд руб., причем сохранился тренд к уменьшению доли услуг colocation за счет увеличения (до 55%) доли более маржинальных облачных услуг.

По прогнозу, число стоек в коммерческих ЦОДах в 2023 г. вырастет на 21%, а в 2024 г. – еще на 19% и достигнет 84 тыс. (рис. 1). При этом стоит учитывать, что и сами стойки будут другими – на смену ставшим стандартом стойкам мощностью 5 кВт приходят высоконагруженные на 8–12 кВт.

Драйверы развития отрасли примерно те же, что и в прошлом году. Это процессы цифровизации, увеличение

объема накапливаемых данных, рост количества интернет-пользователей, повышение требований к скорости и качеству работы интернет-сервисов, импортозамещение цифровых услуг и подъем российских облачных сервисов. Единственное отличие от прошлого года – отсутствие дефицита стоек в Москве.

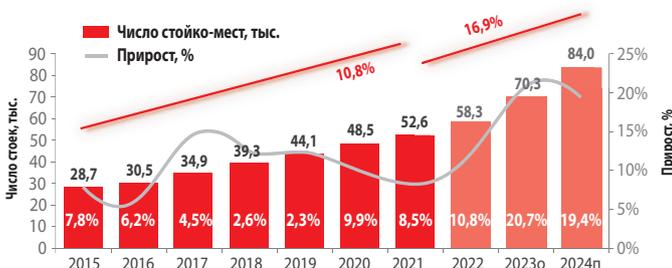
## Профицит – гарантия размещения

«Дефицит стоек – хорошо для инвесторов, но плохо для клиентов», – напомнил генеральный директор компании 3data Илья Хала. В условиях дефицита клиентам тяжело планировать развитие ИТ-систем, и многие начинают строить свои дата-центры, так как не могут найти свободные места для размещения стоек на рынке. Это негативно сказывается и на бизнесе операторов.

В ответ компания 3data запустила проект HyperScale – клуб крупных заказчиков с гарантией размещения и договорами на пять-семь лет. Профицит стоек обеспечивает первый большой ЦОД 3data HyperScale и аренда площадей у партнерских дата-центров.

## Девелоперы в помощь

Специализация повышает эффективность работы. «На западных рынках строительством ЦОДов занимаются девелоперы индустриальной недвижимости. На российском – операторы. Содержат свои строительные и проектные команды и тратят силы не на основной бизнес – предоставление услуг, а на строительство», – отметил коммерческий директор PNC group Евгений Скаридов. Подобная ситуация раньше наблюдалась и на рынке ин-



В 2023 г. рынок коммерческих ЦОДов демонстрирует рост в 21%

Источник: iKS-Consulting

◀ Рис. 1. Динамика роста рынка коммерческих ЦОДов в России



Илья Хала



Евгений Скаридов



Константин Степанов



Дарья Алексанкина



Андрей Аксенов

дустриальной недвижимости – все занимались строительством самостоятельно: например, компания по производству мороженого строила специализированный склад для мороженого. Так уже никто не делает. Теперь, по мнению эксперта, очередь дошла и до дата-центров.

Использование профессионалов в области индустриальной недвижимости позволяет сократить срок строительства ЦОДа и сэкономить финансовые ресурсы. Большое преимущество – финансирование строительства из инвестиционного фонда. Успешные примеры уже есть – в 2022–2023 гг. девелопер PNK group построил в PNK парке Медведково в Москве ЦОДы на 9600 стоек общей мощностью 72 МВт. Оператором одного дата-центра стал 3data HyperScale.

### Операция «Эвакуация»

«События 2022 г. скорректировали наши планы, мы немного притормозили региональное развитие, тем не менее оно идет», – отметил И. Хала. Во Владивостоке уже работает ЦОД, построенный по франшизе 3data компанией Key Point, в Краснодаре ЦОД (также по франшизе 3data) строит компания Alias Group. Выполняются проекты в ряде других городов.

В регионах компания продолжает политику строительства небольших ЦОДов шаговой доступности премиального класса, уступая крупным заказчикам более сильным конкурентам. Самым мощным из них является компания «Ростелеком – ЦОД», имеющая самую большую сеть региональных ЦОДов в стране.

«У нас в эксплуатацию введен 21 дата-центр, 22-й введем до конца года в Екатеринбурге», – поделился планами Константин Степанов, директор по развитию ЦОД компании «Ростелеком – ЦОД». Строятся дата-центры в Нижнем Новгороде и Армении; компания ищет дополнительные площадки для строительства в Хабаровске и Новосибирске (рис. 2).

Развитие региональных дата-центров получило дополнительный импульс после атак украинских дронов на столицу. К счастью, дата-центры не пострадали, но, как отмечалось на облачной секции и в кулуарах, некоторые заказчики решили минимизировать риски и уже перенесли продуктовые системы за Урал.

Сказались боевые действия и на работе компании C3 Solutions, которой пришлось переносить завод подальше от украинской границы – из Шебекино в Белгород – и заключать OEM-соглашения с производственными площадками в Костроме, Рязани и Московской области. «Самое сложное было перевезти людей. Местная специфика – люди живут на земле, у них есть домашнее хозяйство: как минимум собаки и кошки или даже коровы», – рассказала Дарья Алексанкина, генеральный директор C3 Solutions. Проблему удалось решить, с пережившими поделились жильем и всем необходимым.

### Зеленая энергетика

Несмотря на санкции, сложности с импортозамещением и политическую нестабильность, дата-центры не забывают о «зеленой» повестке. ЦОДы вырабатыва-



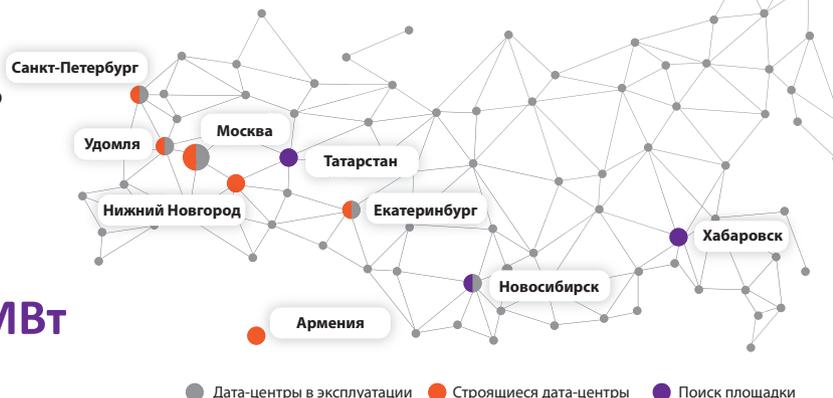
21  
дата-центр



19,2  
тыс. стоек



160 МВт  
мощность



◀ Рис. 2.  
Геораспределенная сеть дата-центров Tier III

Источник:  
«Ростелеком – ЦОД»



**Денис Горяченков**



**Роман Шмаков**



**Сергей Соколов**



**Евгений Колосков**

ют огромное количество тепла, которое без пользы выбрасывается в атмосферу. По оценкам генерального директора IXcellerate Андрея Аксенова, только ЦОДы IXcellerate смогли бы «отопить» 50 тыс. жителей Москвы, что сопоставимо с населением района Алтуфьево. А все ЦОДы столицы способны обеспечить теплом 400–500 тыс. москвичей, т.е. примерно население пяти-шести районов города.

Технические решения есть и уже применяются для отопления административных и производственных помещений IXcellerate. В ЦОДе MOS2 реализован тепловой насос «воздух – вода». Нагретый в машинном зале воздух проходит через фреоновый прецизионный кондиционер и ох-

лаждается, нагревая конденсаторный блок; теплоноситель проходит через конденсатор, нагревается и подается в тепловой пункт. По оценкам эксперта, экономия за отопительный сезон составляет около 1,5 млн руб. (рис. 3).

ЦОД не должен являться «гарантирующим поставщиком». Скорее, он может служить дополнительным источником тепла для городского коммунального хозяйства. Можно отапливать не только жилой фонд, но и коммерческие объекты: бассейны, дороги, тротуары. Дело за малым – преодолением административных и нормативных барьеров для интеграции систем охлаждения ЦОДов с городскими службами. Здесь IXcellerate надеется на помощь АНО КС ЦОД и готова участвовать в рабочей группе по этому вопросу.

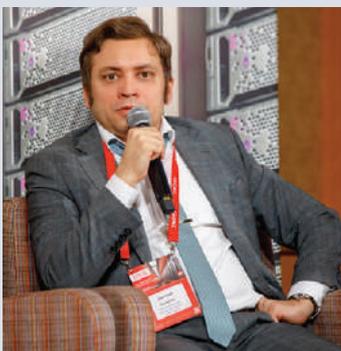


**▲ Рис. 3. Зачем тепловой насос ЦОДу**

### Серверная стойка в формате Open Compute Project

Выставка-конференция «ЦОД» – лучшее место для представления отрасли новых решений. Компания ДКС официально анонсировала стойку OCP ДКС. «Продукты данного типа в России с успехом применяет одна из наших крупнейших ИТ-компаний, «Яндекс», с рынка идет большой запрос на этот продукт», – объяснил запуск нового направления руководитель отдела продаж ИТ компании Денис Горяченков.

Эксперт назвал преимущества решения: увеличенная как минимум на 50% плотность размещения оборудования в стойке, возможность применения единой токоведущей шины постоянного тока 12 В, а также монтаж и обслуживание серверов без использования инструментов.



**Дмитрий Никитин**, директор Департамента развития отрасли ИТ, Минцифры России

Центры обработки данных – неотъемлемая часть цифровой инфраструктуры, и одна из задач государственной политики в области ИКТ – обеспечить доступность необходимых мощностей ЦОДов для нужд бизнеса и госорганов. Решение этой задачи ведется по нескольким направлениям. Первое – стимулирование спроса на услуги коммерческих ЦОДов со стороны государства. С этой целью уже введены необходимые требования для госорганов и созданы условия для размещения ГИС в коммерческих ЦОДах.

Второе направление – введение понятия ЦОДа в законодательное поле. Соответствующий законопроект принят Госдумой в первом чтении и стоит в очереди на рассмотрение в осеннюю сессию. Третье – обеспечение льготных кредитов на строительство ЦОДов и налоговых льгот на этапе их эксплуатации. Проработка таких инструментов ведется в рамках подготовки нового национального проекта «Экономика данных». И четвертое – это предупреждение рисков избыточного регулирования, а также снятие барьеров, препятствующих реализации проектов создания инфраструктуры ЦОДов.



Полный цикл выпуска ОСР-стоек развернут на производственной площадке в Твери. Продукт будет доступен к заказу начиная с середины сентября, и по стоимости он «почти совпадает» с анонсированной недавно новой моделью iPhone.

### Подхватывая штурвал

Компания Systeme Electric представила новый флагманский трехфазный модульный ИБП для ЦОДов. Особенность серии Excelente – высокий показатель эффективности: КПД в режиме двойного преобразования достигает 96,6%. «Мы уже принимаем заказы, просчитываем технические конфигурации, в ближайшее время ИБП будет доступен для тестирования в России», – заявил первый заместитель генерального директора Systeme Electric по рынку «ИТ-решения» и сервису Роман Шмаков.

Systeme Electric подхватила штурвал, выпавший из рук ушедшей с российского рынка французской компании Schneider Electric, постаралась взять все лучшее из ее решений и адаптировать к потребностям российского рынка. По-прежнему работают три завода и центр инноваций, российская компания выполняет ремонт и поддержку поставленного оборудования ушедшего гиганта. Осталась и главная «фишка» – предложение комплексной экосистемы сервисов и инструментов с полной совместимостью. Так что в будущем не исключено появление новых моновендорных ЦОДов – теперь уже под брендом российской фирмы.

### Импортозамещение комплектующих

Уход западных вендоров был неожиданным, многие проекты остались незавершенными, и возникла острая необходимость в поставках совместимых с уже развернутым иностранным оборудованием решений и устройств.

Российские вендоры откликнулись на запросы рынка. «Помимо нашей собственной продукции под торговой маркой KLM мы имеем возможность изготавливать элементы шинопроводов иностранных производителей, ушедших с рынка. У нас уже есть объекты, где мы допоставили компоненты, недопоставленные зарубежным производителем», – рассказал руководитель проекта «Албимакс Металл» (KLM) Сергей Соколов. В новых проектах компания предлагает использовать свои шинопроводы, произведенные на заводе во Владимире.

### Вызовы и решения

Потребности заказчиков не изменились – всем нужны современные технологичные, качественные и надежные решения, поставленные в сжатые сроки. «С началом СВО мы оказались в подвешенном состоянии – ушли привычные производители, с которыми были налажены длительные доверительные отношения, обучены инженеры и сервисные специалисты. Наблюдаем рост стоимости оборудования и материалов, вызванный падением курса рубля и дефицитом продукции. Сроки поставки большинства комплектующих непредсказуемы. Видим дефицит квалифицированных специалистов, и с каждым годом ситуация ухудшается. Усложнился доступ к мировому опыту», – перечислил сегодняшние проблемы технический директор компании «Свободные Технологии Инжиниринг» Евгений Колосков.

Участникам рынка приходится много времени уделять изучению технологических процессов и тестированию продуктов новых поставщиков. Аккумулировать опыт компаний, использующих инженерные решения для ЦОДов, помогают карты вендоров, которые разрабатывает iKS-Consulting. Вендоры оцениваются по потенциалу – способности к развитию в РФ в текущих условиях – и представленности – присутствию решений вендора в инфраструктуре и восприятию заказчиков. Делегатам конференции предложили карты восприятия вендоров ИБП, охлаждения, ИТ-стоек, СКС, ДГУ и prefab-ЦОДов.

В интегральном топе вендоров инженерных решений для ЦОДов – хорошо известные на рынке компании. Тройку лидеров возглавляют Systeme Electric, C3 Solutions и «Парус электро» (→ см. с. 32). В топ попали и ушедшая с рынка Schneider Electric, и заморозившая работу в России Huawei, хотя, если динамика не изменится, в следующем году они покинут список.

Проектировать и строить ЦОДы стало сложнее. Порой приходится упрощать решения, ориентируясь на доступную продукцию с гарантированным сервисом. Однако при правильном подходе, как отметил Е. Колосков, дата-центры не становятся менее надежными. А спрос на них в любом случае будет расти. В будущем эксперты отрасли смотрят с оптимизмом.

Николай Носов

# Узбекистан: потребность в современных ЦОДах все острее



**Усиливающаяся цифровизация всех сфер жизни – от аэропортов до электронного правительства – подталкивает развитие рынка ЦОДов в Узбекистане. Но пока уровень проникновения услуг коммерческих дата-центров в республике очень низкий.**

Большой интерес к различным аспектам построения и использования дата-центров проявили участники форума Eurasia Data Center & Cloud Forum, организованного в Ташкенте «ИКС-Медиа» и собравшего более 200 делегатов из Узбекистана и других стран Центральной Азии.

Согласно оценке iKS-Consulting, объем общей потребности экономики Республики Узбекистан в инфраструктуре дата-центров составляет 3,6 тыс. стоек. Вместе с тем, по данным того же iKS-Consulting, объем рынка коммерческих ЦОДов Узбекистана в настоящее время составляет около 500 стойко-мест. Текущее состояние рынка КЦОДов республики Татьяна Толмачева, управляющий партнер iKS-Consulting, описывает как зачаточное. Оно характеризуется дефицитом высококачественного предложения и слабым развитием отрасли ИКТ в целом.



Узбекский рынок, как и российский, имеет региональную диспропорцию, которая обусловлена тем, что 60% экономической активности республики сконцентрировано в Ташкенте. Наиболее крупные ЦОДы принадлежат «Узбектелекому», Uzinfocom, East Telecom, а также Университету Инха. По прогнозу, к 2025 г. этот объем вырастет до 1760 стоек.



**Татьяна Толмачева (iKS-Consulting)**

Наибольший вклад внесет ЦОД DSS, первая очередь которого (960 стоек) должна быть запущена во II квартале 2025 г.

Налицо предпосылки для ускорения развития отрасли дата-центров Узбекистана. Во-первых, хорошими темпами развивается телеком-инфраструктура, необходимая для подключения ЦОДов. Во-вторых, с 2013 г. активно реализуются инициативы электронного правительства: уже введен в эксплуатацию дата-центр электронного правительства, работают единая система электронного документооборота и защищенная система электронной почты. Наконец, разработаны амбициозные государственные программы по цифровизации экономики. А уровень цифровизации отдельных объектов, например, нового аэропорта в Самарканде, уже впечатляет.

## ЦОДы «все в одном»

Однако на данный момент большинство узбекских компаний и организаций используют собственные серверные комнаты и небольшие ЦОДы. При этом мало кто хочет заниматься инсталляцией и эксплуатацией инженерных систем, в том числе из-за отсутствия необходимой экспертизы. Поэтому неудивительно, что большой интерес на форуме вызвали решения «всё в одном», включающие все необходимые инженерные компоненты ЦОДа: ИБП, блоки распределения питания, средства охлаждения, стойки/шкафы, а также системы пожарной безопасности. Такие ЦОДы могут быть разными по размеру: от микроЦОДов на одну стойку до контейнерных и модульных на несколько десятков и даже сотен стоек. Решения этого класса представили сразу несколько участников Eurasia Data Center & Cloud Forum: и компании с мировым именем (Delta Electronics и Schneider Electric), и производители с российскими корнями – Astergo, ИТК и НАГ.

Astergo – абсолютно новое имя на рынке цодостроения, о котором впервые было заявлено на форуме в Ташкенте. В основе Astergo – команда и ресурсы известного российского производителя C3 Solutions. В арсенале – все основные инженерные системы для ЦОДов, включая ИБП, системы охлаждения, стойки (в том числе OCP-модели). Как рассказал Роман Монахов, генеральный директор Astergo, компания уже открыла офисы в Ташкенте, Каире (Египет), Дубае (ОАЭ), Йоханнесбурге (ЮАР), Шэньчжэне (КНР) и Сингапуре. А микроЦОДы Astergo используются в одном из проектов, реализуемых в Узбекистане.



**Роман Монахов (Astergo)**

Микро- и модульные ЦОДы, предлагаемые ИТК (бренд ГК ИЕК), основаны на решениях двух ведущих производителей такой продукции в России: компаний «Утилекс» и GreenMDC. Для наполнения конструктивов ИТК задействованы компоненты (включая ИБП и кондиционеры), предоставляемые под собственным брендом.

НАГ использует собственные конструктивы, в которые также устанавливает все необходимые инженерные компоненты. О серьезности намерений компании на рынках Центральной Азии свидетельствует наличие офисов в Ташкенте и Алматы.

Наиболее широкую линейку модульных и контейнерных ЦОДов – от одностоечного микроЦОДа Xibus Edge до предсборанного контейнерного ЦОДа Xibus Node с мощностью ИТ-нагрузки 18–90 кВт – представила в Ташкенте компания Delta Electronics. Следует также отметить ориентированный на телеком-заказчиков мини-ЦОД Xibus FlexiNode, который поддерживает различные варианты фрикулинга и альтернативные источники питания, в том числе солнечные. Использование солнечных батарей в Узбекистане может оказаться очень актуальным.

## ESG и снижение расходов

Другой мировой поставщик комплексных решений для ЦОДов, включающих различные варианты модульных и контейнерных решений, на форуме в Ташкенте сделал акцент на принципах устойчивого развития (ESG), реализацию которых считает



**Денис Вайнер (Schneider Electric)**

стратегическим направлением развития ЦОДов во всем мире. Как отметил Денис Вайнер, директор по продажам в странах СНГ компании Schneider Electric, на дата-центры уже приходится 1–2% общемирового потребления электричества. «Цифровая трансформация и автоматизация всего и вся требуют всё больших вычислительных мощностей и, как следствие, ЦОДов,

что привлекает внимание различных экологических групп и потребителей, обеспокоенных климатическими изменениями».

Следует отметить, что отрасль ЦОДов одной из первых обеспокоилась повышением энергоэффективности, внедрив показатель PUE. За прошедшие годы усилия представителей этой отрасли позволили добиться значительных улучшений – среднегодовой PUE дата-центров снизился с 2,5 до 1,59 (данные Uptime Institute).

Существует стереотип, что чем выше эффективность технического решения, тем оно дороже. На самом деле это не так. Как подчеркнул Д. Вайнер, есть много решений, которые обеспечивают и достижение целей устойчивого развития, и уменьшение CAPEX и OPEX. В качестве систем, повышающих эффективность использования энергии и при этом позволяющих сократить CAPEX и OPEX, эксперт Schneider Electric назвал возобновляемые источники энергии – солнечные батареи и ветровые генераторы, микросети с устройствами хранения электроэнергии и средства оптимизации воздушных потоков в машинных залах ЦОДов. Очевидное снижение OPEX дает применение высокоэффективных (с высоким КПД) источников бесперебойного питания и литий-ионных батарей. Понятно, что все эти решения Schneider предлагает в том числе на рынках Центральной Азии.

## Когда важна бесперебойность

Тема систем бесперебойного питания и накопителей энергии стала на форуме одной из ключевых. Такие решения позволяют обеспечить бесперебойное снабжение качественным электричеством ИТ-оборудования, а значит, непрерывное предоставление ИТ-сервисов. Для Узбекистана этот вопрос важен вдвойне, поскольку в стране довольно низкое качество энергетической системы, энергопотребности в дефиците. Часто происходят аварийные и веерные отключения электричества, а заказчики испытывают сложности в получении ТУ на присоединение к технологическим сетям.



Schneider Electric и Delta Electronics входят в число мировых лидеров в области ИБП, предлагаемые ими изделия характеризуются одним из наиболее высоких показателей энергоэффективности и энергетической плотности. Но даже когда показатель КПД современных ИБП уже достиг, кажется, своего максимума, лидеры работают над его повышением. Впечатлило сделанное Delta Electronics в Ташкенте объявление о выпуске в начале следующего года нового ИБП, у которого КПД в режиме двойного преобразования равен 97,5%.



**Михаил Сазонов,**  
**продакт-менеджер**  
**по региону EMEA,**  
**(Delta Electronics)**

Оба гранда предлагают ИБП с литий-ионными аккумуляторами, причем у Delta Electronics есть собственное производство таких аккумуляторов. Высокая энергетическая плотность ЛИ АКБ привлекает все больше заказчиков. Свои решения на базе ЛИ АКБ представила на конференции и компания ENERCON, которая имеет офисы в Турции, Казахстане и Узбекистане. Компания выпускает комплексные решения на базе различных литий-ионных технологий (NMC, LFP), раз-

личной мощности и емкости, в том числе накопитель энергии на базе контейнера.

### Коннективность и облака

Еще один важный элемент ЦОДов – кабельная система. В Ташкенте соответствующие решения представили компания Siemon, занимающая в мире ведущие позиции в этой области, и уже упомянутые Astergo и ИТК. В ЦОДах в основном используются высокоплотные и высокопроизводительные оптические системы, которые есть в арсенале перечисленных компаний. Для автоматизации процедур эксплуатации СКС эффективны интеллектуальные системы управления. Такую систему предлагает Siemon, а ИТК разрабатывает подобное решение.

Понятно, что ИБП, СКС и другая «инженерка» нужны для обеспечения главного – работы ИТ-сервисов. Все больше, причем даже для критичных приложений, используются облачные услуги. Ссылаясь на результаты

проведенного исследования, Максим Захаренко, CEO облачного провайдера Cloupard, сообщил, что облака в Узбекистане задействуют уже две трети компаний.

Свои комплексные решения для построения облачных платформ на Eurasia Data Center & Cloud Forum представила НЗС. Выполнившая ряд крупных проектов в Китае, компания, по словам ее технического директора в СНГ Михаила Воробьева, «обладает полным стеком решений для построения ЦОДов и облаков». Это, в частности, коммутаторы (в том числе для ядра 400G), серверы, программные СХД и системы виртуализации. Интересны наработки компании в сфере жидкостного охлаждения серверов и коммутаторов.

Одной из важных тенденций ИТ-отрасли руководитель отдела СХД компании Netsystems Александр Мионов назвал ширящееся использование бизнесом суперкомпьютерных технологий. Это, безусловно, связано с взрывной популярностью приложений на основе искусственного интеллекта. Такие приложения предъявляют повышенные требования не только к энерго-



**Михаил Воробьев (НЗС)**

потреблению стоек, но и к характеристикам СХД. Эксперт рекомендует использовать в этой области решения NetApp, которые упрощают установку, конфигурирование и эксплуатацию систем для поддержки рабочих нагрузок ИИ. Особенностью Eurasia Data Center & Cloud Forum этого года стало проведение наряду с «классическими» конференцией и выставкой практических семинаров. На семинарах разбирались примеры проектов создания ЦОДов, преимущества сертификации дата-центров по уровню Tier III, вопросы выбора контейнерных ЦОДов, а также систем охлаждения и огнетушащих веществ. Подобные практические рекомендации от ведущих экспертов в своих областях крайне важны для набирающего обороты рынка цодостроения Узбекистана, где пока квалифицированных специалистов сильно не хватает.

**Александр Барсков**  
**Ташкент — Москва**

# ЦОДы в Казахстане – приоритет высшего уровня



**Всемерное развитие ЦОДов – такая задача поставлена руководством Республики Казахстан. Подходы и технологии для ее выполнения обсуждались на форуме Data Center & Cloud Kazakhstan, организованном «ИКС-Медиа» в Алматы.**

Президент Казахстана Касым-Жомарт Токаев определил стратегию превращения республики в ИТ-страну. Неотъемлемая составляющая этой стратегии – развитие цифровой инфраструктуры и ЦОДов как ее основных элементов. А в недавнем послании главы государства народу Казахстана «Экономический курс Справедливого Казахстана», в частности, указано, что «страна может стать площадкой для продажи вычислительных мощностей глобальным игрокам. Поэтому необходимо создать самые привлекательные условия, включая преференции для привлечения инвестиций в строительство крупных дата-центров и продвижения казахстанских интересов в сфере хранения и обработки данных».

Особое внимание руководство страны уделяет развитию технологий искусственного интеллекта. «Успешное развитие этого сектора может обеспечить значительный прирост ВВП отдельным странам. Если мы полноценно используем возможности искусственного интеллекта, то сможем совершить качественный рывок к экономике знаний», – говорится в обращении президента Казахстана.

## ЦОДы и государство

К.-Ж. Токаев поручил правительству в течение двух лет обеспечить строительство дата-центров, специализирующихся на системах искусственного интеллекта. Для

этого, по его словам, могут быть привлечены такие мировые игроки, как Amazon, Google, Mastercard и Citigroup. Соответствующие договоренности были достигнуты во время недавней поездки президента Казахстана в Нью-Йорк.

Еще одна инициатива, поддержанная руководством Казахстана, – создание в стране регионального цифрового хаба. В рамках этой инициативы будут проложены высокоскоростные ВОЛС по дну Каспийского моря и наземная магистраль запад – восток для расширения транзита трафика. В непосредственной близости от этой магистрали планируется построить два гиперЦОДа, причем на деньги частных инвесторов.

Как отметил, выступая на форуме Data Center & Cloud Kazakhstan, Абилкаир Болатбаев, руководитель управления развития новых технологий и инфраструктуры в области связи Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (МЦРИАП РК), для реализации столь амбициозных планов требуются изменения в нормативном правовом регулировании отрасли ЦОДов и облачных сервисов с учетом интересов крупных международных игроков и национальных инвесторов.

Одно из регуляторных направлений связано с классификацией данных – определением условий их размещения и доступа к ним. В первую очередь это важно для акти-



**Абилкаир Болатбаев**  
(МЦРИАП РК)



**Светлана Черненко** (Ассоциация операторов ЦОД и облачных сервисов РК)



Панельная дискуссия. Слева направо: Абилкаир Болатбаев (МЦРИАП РК), Светлана Черненко (Ассоциация операторов ЦОД и облачных сервисов РК), Денис Вайнер (Schneider Electric), Евгений Вирцер («Свободные Технологии Инжиниринг»), Илья Хала (3data), Татьяна Толмачева (iKS-Consulting)

визации работы в Казахстане мировых гиперскейлеров. Подобная классификация поможет и местным облачным провайдерам развивать бизнес в соседних странах и в мире в целом.

Другое ключевое направление – внесение в законодательство определения ЦОДов и облачных сервисов. Как пояснил А. Болатбаев, раньше в документах фигурировали «серверные комнаты», а ЦОДы указывались в скобках. Теперь «ЦОД» становится отдельным понятием. Также в ближайшее время в Казахстане планируется ввести классификацию ЦОДов и разработать правила технического аудита таких объектов.

В сфере правового регулирования представитель МЦРИАП особо отметил роль недавно созданной в Казахстане Ассоциации операторов ЦОД и облачных сервисов РК, объединяющей ведущих операторов и провайдеров ЦОДов и облачных сервисов. По словам Светланы Черненко, директора ассоциации и главы представительства в Казахстане международного агентства iKS-Consulting, само формирование такого профессионального объединения – признак зрелости рынка. В числе задач ассоциации она выделила популяризацию сервисной модели потребления ИКТ-услуг среди потенциальных пользователей, формирование единой позиции игроков рынка в отношении правового регулирования и мер поддержки отрасли, а также повышение инвестиционной привлекательности казахстанской отрасли ЦОДов и облаков. Кроме того, безусловно важными составляющими деятельности ассоциации

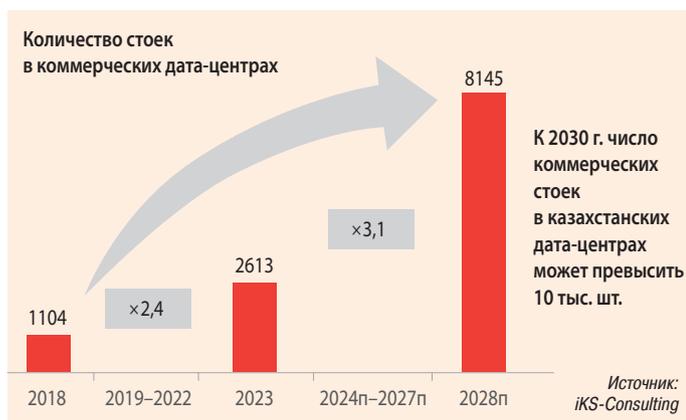
являются обмен профессиональными знаниями между игроками, повышение квалификации и уровня зрелости потребителей.

### Показатели роста

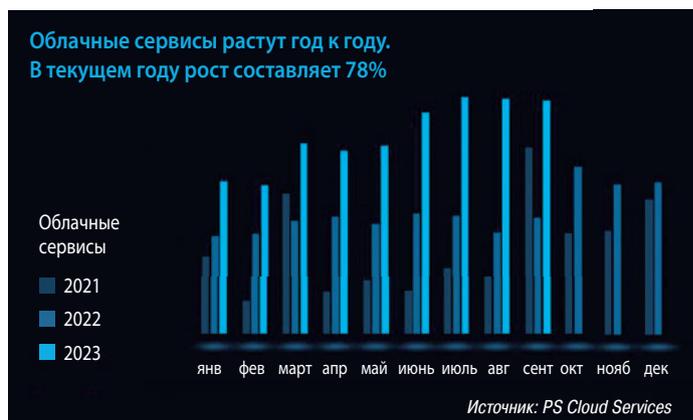
Если говорить о рынке коммерческих ЦОДов Казахстана, – а это ключевой индикатор развитости и зрелости цифровой инфраструктуры в целом, – то его емкость в 2023 г. составит около 2,6 тыс. стоек (по данным iKS-Consulting). По прогнозу С. Черненко, рынок находится в преддверии инфраструктурного скачка – через пять лет число стоек может вырасти до восьми с лишним тысяч, а к 2030 г. превысить 10 тыс.

Эксперты iKS-Consulting считают, что не только увеличится число стоек, но за счет сертификации площадок, в частности на соответствие уровням Tier III и Tier IV Uptime Institute, повысится и качество предложения. Также будет повышаться доля высоконагруженных стоек, которые необходимы, например, для систем искусственного интеллекта. Правда, при этом, очевидно, стоимость одного стойко-места тоже вырастет.

Развивается и облачный рынок – iKS-Consulting оценивает рост в 50%, причем инфраструктурные сервисы (IaaS/PaaS) доминируют над SaaS. У отдельных игроков рост значительно превышает средний показатель. Так, согласно данным компании PS Cloud Services, ее показатели текущего года существенно превосходят показатели 2021–2022 гг., а доходы от предоставления облачных сервисов в 2023 г. увеличатся на 78%. Этот казахстан-



▲ Рост числа стоек в коммерческих ЦОДах Казахстана



▲ Рост продаж облачных сервисов в компании PS Cloud Services

ский провайдер предоставляет услуги, используя шесть ЦОДов, четыре из которых расположены в Алматы и по одному – в Астане и в Ташкенте (Узбекистан).

### Спрос и предложение

Среди факторов, которые позволят в ближайшие пять лет поменять рыночный ландшафт в сегменте ЦОДов и облачных сервисов, С. Черненко выделяет появление у инвесторов веры в коммерческий потенциал рынка, что происходит во многом благодаря поддержке государства.

Анализируя возможные сложности реализации проектов ЦОДов в Казахстане, Евгений Вирцер, генеральный директор компании «Свободные Технологии Инжиниринг», на первое место ставит вопрос привлечения финансовых средств. «Проекты ЦОДов капиталоемкие. А базовая ставка (Национального банка Казахстана) даже выше, чем в РФ, что может затруднить реализацию таких проектов», – отмечает он.

Илья Хала, генеральный директор 3data, первоочередной задачей считает формирование спроса на услуги коммерческих ЦОДов. «Если спрос есть, то земля, энергетика и деньги найдутся, – аргументирует он. – На данный момент цены высокие, даже по мировым меркам. Емкость рынка пока небольшая, запускать ресурсоемкие проекты рискованно».

«До недавнего времени мы ориентировались на спрос. Сейчас поняли, что развитие инфраструктуры должно опережать спрос и менять парадигму взаимоотношений инвесторов и цодостроителей», – говорит С. Черненко. Она указала на то, что в Казахстане запускаются инфраструктурные проекты принципиально нового масштаба и уровня. Речь идет о проектах на несколько тысяч стоек, которые С. Черненко назвала переломными для рынка.

Один из таких проектов – ЦОД Akashi, который планируется построить в столице Казахстана Астане. Общая запланированная емкость объекта – 4096 стойко-мест (мощность 42 МВт). В случае успешной реализации это будет крупнейший объект такого уровня в Центральной Азии. Более того, ЦОД предполагается сертифицировать на соответствие наивысшему (в модели Uptime Institute) уровню отказоустойчивости – Tier IV. До объекта компания планирует провести собственную высоковольтную линию, а на площадке установить электрическую подстанцию 110/10 кВ и реализовать двойное резервирование всех систем.

Активно развивают свою инфраструктуру и признанные игроки казахстанского рынка. Как рассказал Сырым Толеулиев, заместитель председателя правления АО «Казтелепорт», компания в I квартале 2024 г. планирует ввести в эксплуатацию уже седьмой объект в своей сети геораспределенных дата-центров. Это ЦОД «Ерейментау», который строится в



В выставочной зоне форума Data Center & Cloud Kazakhstan

центре Астаны. Объект вместит 100 серверных стоек (7–10 кВт на стойку) и будет сертифицирован на соответствие уровню Tier III. Одна из его особенностей – использование ИБП с литий-ионными АКБ, а также резервирование компонентов электропитания по схеме 2N.

Для предоставления облачных услуг «Казтелепорт» предлагает широкий набор платформ. Войти в этот бизнес компания начинала с развертывания IaaS-платформы на базе VMware, затем стала также использовать платформу на основе KVM, а потом – предлагать сервисы на базе Azure Stack Hub. Облачные сервисы Azure «Казтелепорт» предоставляет из своего ЦОДа в Казахстане, обеспечивая возможность интеграции с глобальным облаком Azure. Сейчас же наибольшие средства компания вкладывает в развитие собственной платформы на базе OpenStack. Среди ее преимуществ С. Толеулиев назвал независимость от вендоров, гибкость за счет открытого кода ПО, удобный API для разработчиков, а также большое количество модулей, позволяющих подстраиваться под потребности клиента.

ЦОДы «Казтелепорта», конечно, использует не только сама компания, но и другие облачные провайдеры, например, ITglobal.com Group. Как рассказал Василий Белов, вице-президент этой компании, дата-центр в Алматы – один из 10, в которых развернуты ее облачные платформы (на основе vStack и решений VMware). ЦОДы расположены в разных странах, включая Россию, Нидерланды, США, Канаду и Турцию. Причем провайдер ориентируется на ЦОДы уровня Tier III, инфраструктуру которых можно обслуживать без прерывания ее работы, благодаря чему становится возможным бесперебойное предоставление облачных сервисов. А это, наряду с архитектурой, не имеющей единой точки отказа, важно для обслуживания клиентов сегмента enterprise.



Амбициозные задачи, поставленные президентом Казахстана, повышение профессионализма игроков и уровня зрелости рынка, а также доступность самых современных технологий и технических решений вселяют уверенность в том, что инфраструктурный скачок уже в ближайшие годы из презентаций аналитиков перейдет в реальные проекты.

**Александр Барсков**  
Алматы – Москва



**Сырым Толеулиев**  
(АО «Казтелепорт»)



## НОВОСТИ АНО КС ЦОД

ОКТАБРЬ 2023

### Новый участник АНО КС ЦОД

Облачный провайдер «Нубес» стал участником Координационного совета по ЦОДам и облачным технологиям. Этот шаг предоставляет компании возможность активно участвовать в разработке отраслевых стандартов в области дата-центров и облачных услуг. Участие в АНО КС ЦОД также позволит провайдеру обмениваться экспертизой с лидерами рынка и принимать участие в создании обучающих программ для специалистов отрасли.

### Первый очный обучающий тренинг и неделя ЦОДов в Казахстане



На тренинге «Построение ЦОДов» в Алматы

25 и 26 октября в Алматы впервые в Республике Казахстан прошел обучающий тренинг «Построение ЦОДов». Рынок услуг ЦОДов и облачных сервисов в стране входит в новую фазу развития: растет количество проектов и новых площадок, появляются новые игроки. На ежегодных конференциях «ИКС» в Алматы постоянно обсуждался дефицит профессиональных кадров, и многие специалисты обращались с пожеланиями организовать обучающие курсы АНО КС ЦОД в республике.

«Нам удалось переработать программу, собрать представительный пул лекторов, которые нашли время и возможность приехать в Алматы. Тренинги прошли успешно, и, надеюсь, они будут проходить в Казахстане регулярно, – сообщил Дмитрий Бедердинов, генеральный директор АНО КС ЦОД. – Перед тренингом, 23 и 24 октября, состоялась ежегодная конференция «ИКС», поэтому по сути в Алматы прошла полноценная неделя ЦОДов».

## НОВОСТИ ОТРАСЛИ

### ЦОД на 140 стоек появится в бизнес-пространстве Taller

Дата-центр с высоким уровнем надежности построят на территории формируемого бизнес-пространства в районе Даниловский на юге столицы. «Дата-центр мощностью в 1 МВт рассчитан на 140 серверных стоек и будет иметь высокий уровень надежности. Его интегрируют в состав бизнес-центра. Арендаторы смогут воспользоваться услугами дата-центра, а не создавать собственную серверную комнату для своей ИТ-инфраструктуры», – рассказал зам. мэра Москвы по вопросам

градостроительной политики и строительства Андрей Бочкарёв.

### В Архангельской области планируется строительство ЦОДа

На полях VIII Восточного экономического форума подписано трехстороннее соглашение о сотрудничестве между Министерством экономического развития, промышленности и науки, Агентством регионального развития Архангельской области и ГК Key Point в целях проработки проекта создания коммерческого ЦОДа на территории региона. Планируется на территории Архангельской области построить ЦОД уровня надежности Tier III, который позволит предприятиям и организациям любых отраслей развивать ИТ-сервисы, в том числе с использованием предлагаемого оператором услуг: аренды оборудования, сервисов информационной безопасности. Общий предполагаемый объем инвестиций в проект – не менее 300 млн руб.

### МТС в 1,5 раза увеличила мощности своего ЦОДа в Ленинградской области

Провайдер #CloudMTS объявил о вводе в эксплуатацию третьего модуля вместимостью 125 серверных стоек в центре обработки данных компании в пос. Федоровское Ленинградской области. После завершения строительства объекта его вместимость составляет 375 стоек. В новом модуле будут развернуты корпоративные системы МТС, в том числе облако #CloudMTS. Все три модуля дата-центра имеют международный сертификат надежности Tier III Constructed Facility. Общая мощность, подведенная к объекту, выросла с 8 до 16 МВт. В ЦОДе применяются энергоэффективные установки системы кондиционирования с адиабатическим охлаждением, что позволяет снизить значение PUE до 1,15 в годовом исчислении.

### В ОЭЗ «Дубна» планируют создать ЦОД Wildberries

Инициатором и инвестором проекта выступает компания Wildberries. По предвари-

тельной оценке, инвестиции в создание и оснащение ЦОДа мощностью 8 МВт составят 6,5 млрд руб. Об этом сообщила заместитель председателя правительства – министр инвестиций, промышленности и науки



Источник: Министерство инвестиций, промышленности и науки МО

Московской области Екатерина Зиновьева. ОЭЗ «Дубна» – одна из пяти подмосковных особых экономических зон. Сегодня здесь работают более 160 резидентов, статус которых обеспечивает им ряд налоговых льгот, позволяющих комфортно развивать бизнес.

### В Казахстане может появиться дата-центр Amazon

Президент Республики Казахстан (РК) Касым-Жомарт Токаев встретился с вице-президентом Amazon Сюзан Пойнтер. В ходе беседы с представителем крупнейшей в мире технологической компании были обсуждены возможности взаимовыгодного сотрудничества в развитии облачных технологий и строительстве дата-центров. В рамках встречи было подписано соглашение между Министерством цифрового развития, инноваций и аэрокосмической промышленности РК и Amazon Web Services о приобретении облачного решения Outpost и запуске пилотного проекта по его интеграции с платформой QazTech. Данный шаг заложит основу для размещения дата-центров глобальных игроков в Казахстане и реализации потенциала страны в качестве регионального ИТ-хаба.

### Стартовало раннее бронирование услуг ЦОДа «Иннополис» в Татарстане

Группа компаний «Атомдата» в лице АО «Атомдата-Иннополис» объявила об открытии раннего бронирования услуг ЦОДа «Иннополис». Ввод дата-центра в эксплуатацию запланирован на начало 2024 г. Первая очередь ЦОДа рассчитана на 1000 стойко-мест. Всего в ЦОДе мощностью 16 МВт разместится 2000 серверных стоек в двух корпусах общей площадью более 23 тыс. кв. м. Дата-центр соответствует требованиям к уровню безопасности и надежности стандарта Tier III. Новый ЦОД – крупнейший в Приволжском федеральном округе – расположен в городе Иннополис (Татарстан) и входит в геораспределенную катастрофоустойчивую сеть дата-центров концерна «Росэнергоатом» (Электроэнергетический дивизион госкорпорации «Росатом»).



Источник: atomdata.ru



СВОБОДНЫЕ  
ТЕХНОЛОГИИ  
ИНЖИНИРИНГ

# ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ  
И СТРОИТЕЛЬСТВО  
ДАТА-ЦЕНТРОВ

Реклама



Россия, 127055, Москва,  
Бутырский вал, д. 68/70, стр. 1

+7 (495) 120-28-66

info@sv-tech.ru  
www.sv-tech.ru

# Неизменные обязательства в условиях турбулентности

**Компания «Свободные Технологии Инжиниринг» была образована перед самым началом пандемии COVID-19. И развиваясь в столь непростое время, смогла стать одним из лидеров рынка цодостроения России.**

**– В чем секрет успешного развития компании в сегодняшних сложных условиях?**

– Если бы были четкие рецепты успеха, все бы ими пользовались. Отмечу четыре момента. Главный – это люди, команда. Ее авторитет на рынке, который позволил быстро получить первые заказы.

Второй момент: я всегда горжусь тем, что делает наша команда, но в любой ситуации считаю, что можно было бы сделать лучше. Поэтому постоянно пробуем усовершенствовать то, что делали раньше.

Третий момент связан с тем, что конкурентное поле за последние годы сильно изменилось. Сегодня среди наших конкурентов мы почти не видим классических интеграторов. Точнее, мы не пересекаемся с ними в проектах. Может быть, потому, что им такие проекты неинтересны. А может быть, потому, что заказчики больше не готовы платить за ту «надстройку», за которую обычно брали деньги интеграторы.

Какова была ситуация в «тучные» годы? С одной стороны, денег у заказчиков было много и они были дешевыми. С другой – интеграторы предлагали понятные продукты известных вендоров, и ни у кого даже не возникало вопросов об оптимизации и о том, можно ли эти решения сделать лучше, снизить стоимость. Теперь ситуация кардинально изменилась: денег стало меньше, они стали дороже, и считают их более тщательно. Известные вендоры ушли. И на первый план вышли команды, которые обладают глубокими инженерными компетенциями, умеют управлять всеми процессами при реализации крупных и сложных проектов.

Крайне важными стали способность оперативно реагировать на изменения, умение в условиях внешней турбулентности выполнять обязательства – по стоимости, по срокам и, разумеется, не в ущерб качеству. Вот пример. Мы зашли в проект. Подписали контракт. Доллар стоил 70 руб. К тому времени, когда начали получать финансирование, курс вырос до 90. В прошлой жизни все обратились бы к заказчику за увеличением бюджета. Мы пошли другим путем: смогли оптимизировать решение без ухудшения качества, требования Tier III выполнили, остались в рамках бюджета. Да, мы заработали несколько меньше, чем планировали, но заработали, а заказчик, не увеличивая смету, получил объект, который хотел. Не многие так умеют работать, считают, что раз внешние обстоятельства изменились, за это должен платить заказчик.

Вот я и подошел к четвертому условию успеха: умению соблюдать обязательства даже при существенном изменении внешних условий. Заказчики это ценят.

**– Какие основные трудности пришлось преодолеть вашей компании?**

– Как я уже говорил, главная причина успеха – кадры. Главные трудности тоже связаны с кадрами. Особенно в начале работы. Сложно было новой маленькой компании привлекать высококвалифицированных специалистов. Понятно, что у нас был костяк. К нему добавлялись профессионалы, с которыми мы много лет были хорошо знакомы. Поток новых для нас людей, специалистов высокого уровня, образовался последние год-полтора. Это снизило кадровый дефицит.

Других серьезных трудностей не назову. Как бы это ни казалось странным, но с деньгами проблем почти не возникает. Со всеми заказчиками «на берегу» договариваемся, что с них – деньги, с нас – работа. С объемом работ проблем также никогда не было – может быть, только первые полгода. Примечательно, что у нас в компании нет и не было ни одного продавца.

К сожалению для меня, но к радости для моих коллег, все больше проектов, от которых мы отказываемся. Либо видим подводные камни, на которые есть риск натолкнуться, либо понимаем, что не потянем по ресурсам, а к своей репутации привыкли относиться очень внимательно.

**– Что, на ваш взгляд, определяет сегодня быстрый рост рынка ЦОДов?**

– Не буду приводить уже ставшие общими аргументы о важности ИТ и цифровизации в целом. Скажу о другом. Если посмотреть на срез рынка по стойкам, которые были введены в эксплуатацию за последние пару лет или находятся в фазе строительства, то большую часть соответствующих проектов инициировали не традиционные операторы ЦОДов, а девелоперы. Девелоперы в широком смысле слова. Люди, которые поняли, что ЦОД – это дорогой объект недвижимости, который способен генерировать хороший денежный поток.

Наш Key Point (Евгений – сооснователь сети региональных ЦОДов Key Point. – Прим. ред.) тоже в чистом виде девелоперский проект. Мы сами не размещаем стойки в ЦОДах, а сдаем квадратные метры с электричеством и холодом. Сегодня жилье, бизнес-недвижимость стали менее интересными с точки зрения инвестиций, чем ЦОДы. Многие девелоперы это хорошо понимают. Если не считать девелоперские стойки, то я бы не говорил о быстром развитии рынка ЦОДов.



**Евгений Вирцер**, генеральный директор, «Свободные Технологии Инжиниринг»

– **Сегодня, когда деньги стали дорогими (ставка ЦБ – 15%), а курс доллара существенно вырос, все чаще говорят, что ЦОДы перестают быть привлекательными для инвесторов, срок окупаемости «вываливается» за 15 лет. Выгоднее не строить, а сидеть и ждать, когда возникнет дефицит стоек и можно будет больше зарабатывать на уже построенных объектах. Что вы об этом думаете?**

– Конечно, капзатраты стали существенно больше. Здесь сложно спорить. Но всегда есть возможность за счет оптимизации инженерных решений и других мероприятий хотя бы часть курсовой потери компенсировать.

Стратегия «ждать не строить» понятна. Деньги можно положить на депозит или вложить в другие проекты. Но мы не знаем, какая завтра будет ставка, какой курс, турбулентность действует на всю экономику, страдают не только ЦОДы. Если курс будет 100, стоимость стойко-мест, пусть с некоторой инерцией, поднимется, это снизит срок окупаемости новых объектов. Заказчикам же нужны стойки. Иначе что? Никому не развиваться? Стагнация всей экономики? Пока есть возможности, силы и желание, лучше двигаться вперед.

Мы свои новые проекты не останавливаем. Говорите, срок окупаемости более 15 лет? У нас другие, более оптимистичные оценки. Все зависит от того, как строить. Если затраты составляют \$70 тыс. за стойку, то, наверное, 15 лет – правильная оценка. Но мы умеем строить ощутимо дешевле, причем речь идет о ЦОДах, сертифицированных на соответствие Tier III.

– **И все же, каков главный барьер развития рынка ЦОДов? Как его устранить?**

– Считаю, что барьер один – стоимость денег. Нужны дешевые деньги и ничего более. Надеюсь, мы сможем доказать государству, что ЦОДы – это та инфраструктура, которая стране нужна не меньше, чем отдельным операторам, что наличие мощной цифровой инфраструктуры оказывает на экономику серьезное позитивное влияние, как прямое, так и опосредованное. И ЦОДы, наконец, получают возможность льготного кредитования.

Все остальное – льготное подключение к энергосетям, налоговые льготы – вторично. Считаю, что если бизнес нерентабелен при полноценной налоговой схеме, то он неправильный. Если бизнес генерирует нормальный доход, то с него не жалко заплатить налоги. Налоги надо закладывать в бизнес-план. Конечно, мы не будем отказываться от налоговых льгот, но сможем развиваться и без них.

– **По мнению ряда экспертов, даже при высоких темпах роста отрасли ЦОДов в России этих объектов строится меньше, чем нужно для развития экономики. Где искать резервы роста?**

– Во-первых, для меня неочевидно, что все, что сегодня строится, моментально продается. Во-вторых, как я уже говорил, на рынок цодостроения вышли новые игроки, девелоперы. Подождите год-два, если по первым проектам они почувствуют, что ЦОДы – перспективный бизнес, то пойдут дальше. Это основной ресурс для ускорения развития отрасли.

– **Если можно, два слова о технологиях. Существует ли риск, что пока мы решаем проблемы «замещения», мировая отрасль ЦОДов уйдет далеко вперед?**

– Вряд ли через пять лет мы обнаружим, что во всем мире ЦОДы уже не расходуют, а генерируют электроэнергию, а PUE стал меньше единицы (улыбается). Если появятся какие-либо кардинальные улучшения, они мимо нас не пройдут.

Давайте возьмем период, скажем, с 2010 до 2020 гг. Появилась ли технология, которая «перевернула» ЦОДы? Если брать не единичные ЦОДы гиперскейлеров, а массовый сектор. Остались те же ДГУ, ИБП, воздушное охлаждение... Да, характеристики оборудования улучшились, оно стало компактнее, повысился КПД.

Согласен с тем, что у ставшего недоступным нам европейского оборудования энергоэффективность выше, чем у китайского или российского. Но, пусть с опозданием, они тоже подтянутся. Рынок предъявляет все те же требования – и не только к тем, кто ушел, но и к тем, кто пришел.

– **А как изменилась стоимость строительства ЦОДов за последнее время?**

– Очень сложно считать. Если посчитать на входе в проект, то в долларах остались те же цифры. Если считать в рублях, сумма, конечно, поменялась. Но считать сложно. Как просчитать проект, который начинался при долларе по 75, потом полгода развивался при 60, сейчас «живет» при 100? Такая волатильность.

Мы на входе в проект устанавливаем твердые цену, срок и ТЗ. А дальше крутимся, чтобы управлять изменениями. Почти всегда можно найти варианты, как компенсировать удорожание по определенным позициям.

– **Вы фиксируете цену в рублях?**

– Как правило, у нас две цены: «тяжелое» оборудование – в валюте, все остальное – в рублях.

– **Каковы планы компании по расширению бизнеса, экспертизы, набора предоставляемых услуг?**

– Наши услуги традиционны: проектирование и строительство. Мы расширились количественно, чтобы одновременно вести больше проектов. Например, сегодня в фазе строительства проекты общей емкостью около 10 тыс. стоек. В глубокой проработке проекты еще более чем на 12 тыс. стоек – по ним в ближайшее время, надеюсь, будут подписаны контракты.

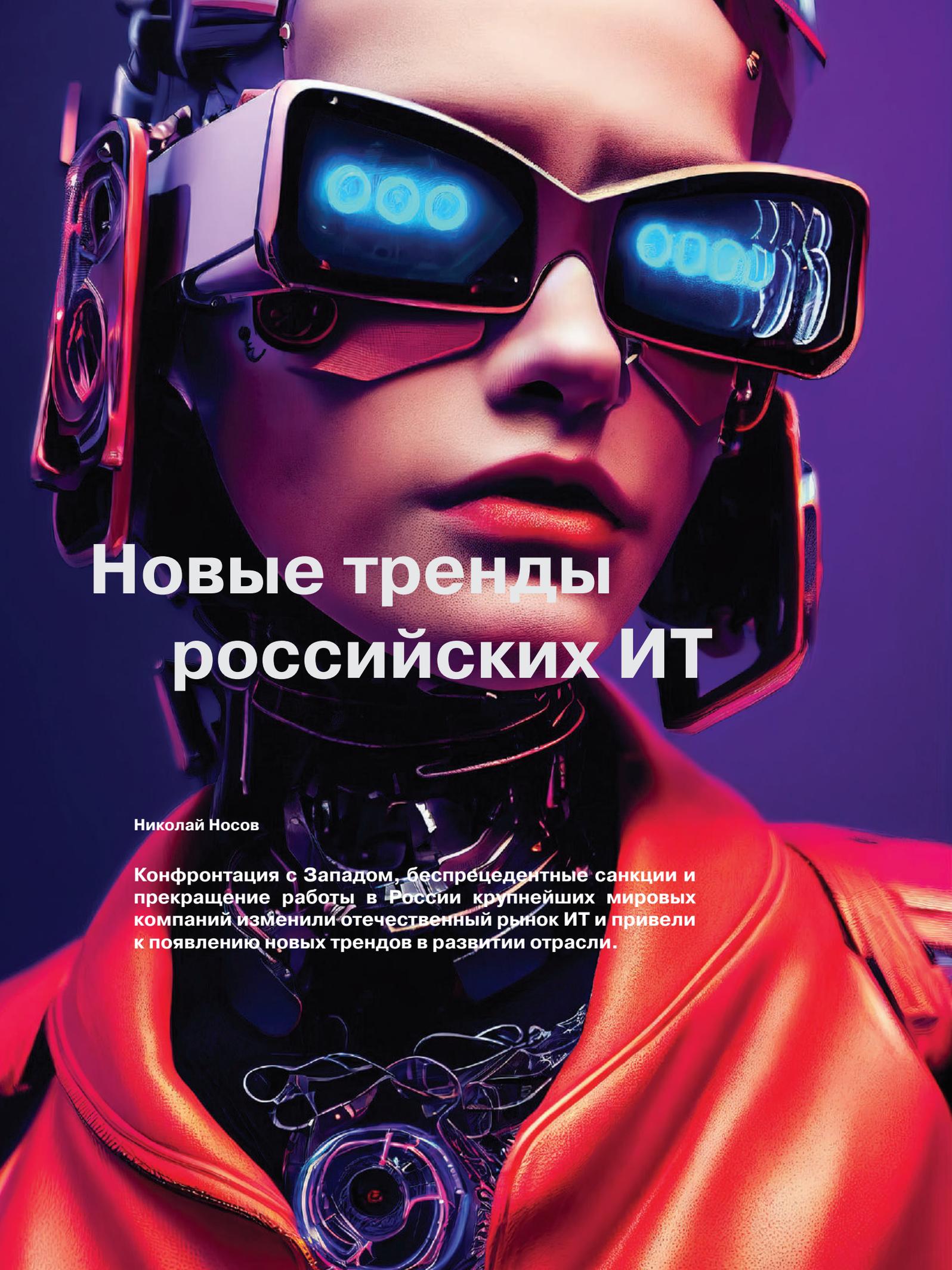
Если говорить о новых направлениях, то большие ресурсы мы вкладываем в развитие собственного производства. Сейчас у нас четыре разрозненные площадки в Рязани, на которых мы изготавливаем силовые шкафы, шкафы автоматики, системы изоляции горячих и холодных коридоров и различные префаб-решения, используемые нами в проектах. Такие решения позволяют убрать максимум операций со стройплощадок и выполнять их на производстве. Это сокращает сроки, повышает качество, снимает риски. В планах – в следующем году построить полноценное большое производство и существенно расширить ассортимент выпускаемой продукции.

Также в обозримом будущем очень хотим выйти на международный рынок. Не только в страны СНГ, а дальше, на Ближний Восток и в Южную Америку. Хочется попробовать там свои силы.



СВОБОДНЫЕ  
ТЕХНОЛОГИИ  
ИНЖИНИРИНГ

<http://sv-tech.ru>



# Новые тренды российских ИТ

Николай Носов

Конфронтация с Западом, беспрецедентные санкции и прекращение работы в России крупнейших мировых компаний изменили отечественный рынок ИТ и привели к появлению новых трендов в развитии отрасли.

## Тотальное импортозамещение

Уход мировых вендоров заставил отечественные компании резко ускорить импортозамещение. «Никогда в развитии российских цифровых технологий не было этапа, сопоставимого с сегодняшним по масштабу задач, которые стоят перед нашими заказчиками», – подчеркнул на пресс-конференции РУССОФТ «Развивая ИТ 2023: основные тренды и векторы развития отрасли» Владимир Лавров, CEO компании Softline.

Процессы импортозамещения подтолкнуло не только прекращение поддержки решений зарубежных вендоров, но и действия регуляторов – предприятия с КИИ должны перейти на импортонезависимое ПО с января 2025 г.

По данным Центра компетенций по импортозамещению в сфере ИКТ, объем закупок иностранного ПО, проводимых в рамках законов № 44-ФЗ и № 223-ФЗ, уменьшился в денежном выражении более чем на четверть – с 71,2 млрд руб. в 2021 г. до 52,51 млрд руб. в 2022 г., а их доля при этом сократилась с 26,6 до 7,34%. Вместе с тем расходы на российское ПО выросли более чем на 70% – с 59,6 млрд руб. в 2021 г. до 102,46 млрд руб. в 2022 г. Доля российских продуктов в закупленном госкомпаниями ПО увеличилась с трети до более чем половины (54%).

Однако не все компании перешли или собираются переходить на российские программы. «Около 40% рынка не подошли к задаче импортозамещения и продолжают использовать ранее закупленное ПО. Рынок «трофейного» ПО и его поддержки в параллельном формате значительный, в том числе в сегменте крупных предприятий», – указал CEO Softline.

## Фрагментация рынка

Раньше базовый контур корпоративной информационной системы строился на зрелых, обкатанных в мире решениях десятка глобальных поставщиков информационных технологий. После ухода с российского рынка мировых лидеров число предоставляющих базовое ПО вендоров перевалило за сотню. «Существенно усилилась фрагментация. В Едином реестре российского программного обеспечения более 15 тыс. продуктов, центры компетенций размылись», – отметил В. Лавров.

При этом возникли вопросы совместимости новых продуктов, их зрелости, отсутствия единой поддержки. Встала и проблема доверия – нет многолетней истории эксплуатации, нет гарантий финансовой устойчивости вендора. Предприятие, сделав ставку на новую платформу, не уверено, что она будет дальше развиваться и не придется терять инвестиции, меняя информационную систему.

Порядка 80% информационных систем в банках и более 400 ГИС построены на Java. Причем открытый исходный код и дистрибутивы на его основе, используемые в бизнесе, не одно и то же. Для создания безотказного и безопасного продукта необходимо обладать большой экспертизой, заниматься проверкой исходных кодов на ошибки и уязвимости, развертыванием обновлений и поддержкой. Это огромный труд».

Минцифры видит все эти сложности и даже заявляло о необходимости поддерживать только самые сильные и перспективные решения, но на практике не определилось даже с приоритетными операционными системами.

## Небезопасный open source

Невозможно, особенно в условиях цейтнота, изобретать велосипед и писать все замещающие программы самим. Да это и не нужно – все крупнейшие мировые вендоры используют готовые «кирпичики» и даже целые блоки из open source. Но их тоже нужно уметь готовить. Недостаточно сделать форк и отнести продукт на регистрацию в ЕРРП. Нужно иметь компетенции по развитию продукта и понимать, что внутри.

С началом СВО в обновлениях продуктов с открытым исходным кодом уже были выявлены целенаправленно сделанные закладки, через которые по территориальному признаку атакуют пользователей с российскими IP-адресами.

Перед использованием в бизнес-среде open source-программы и появляющиеся обновления надо проверять на ошибки и умышленно или неумышленно созданные уязвимости, что под силу только специализированным, имеющим экспертизу в продукте компаниям. Например, в Open JDK (Java Development Kit) ежегодно вносятся 100–150 критических патчей. Поэтому лучше всего брать коммерческий вариант решения на базе продукта с открытым исходным кодом с поддержкой от профессионалов.

Импортозамещение затрагивает не только операционные системы и офисные пакеты. Не стоит забывать и о связующем ПО, на котором работают бизнес-приложения.

Миф о том, что открытый код безопасен, так как его проверяют тысячи глаз, развеялся, но без использования open source не обойтись. Программы с открытым исходным кодом необходимы, но вот с доступом к ним из России возникают проблемы. Есть риски полного отключения российских пользователей от GitHub, уже принимались решения о создании его российского



**Роман Карпов,**  
директор по стратегии и развитию технологий,  
Axiom JDK



**Валентин Макаров,**  
президент,  
НП «РУССОФТ»

Многие российские ИТ-компании нашли способы работать на рынках недружественных стран, параллельно с этим развивая экспорт в дружественных странах. Это 7 млрд человек, которые на фоне того, что Россия не сломалась после ввода санкций и показала свою технологическую независимость, зовут нас к себе, чтобы мы помогли им построить собственную независимую ИТ-индустрию. Рынок, которому ранее уделялось гораздо меньше внимания, сейчас становится обладателем главного экспортного потенциала.

аналога – Национального хранилища программ с открытым исходным кодом, назначались сроки, но воз и ныне там.

### Бум заказной разработки

При всем разнообразии имеющихся на рынке продуктов пользователи сталкиваются с необходимостью их доработки. Массовый переход на новые программы вызвал бум заказной разработки. Этот тренд поддерживается необходимостью написания специализированных нишевых программ, которые замещают решения ушедших вендоров, отсутствующие среди решений open source. Обостряет проблему нехватка ресурсов для написания программ своими силами и дефицит квалифицированных разработчиков на рынке.

«Поддерживать и развивать ресурсы заказной разработки, развивать решения на долгосрочной основе становится сложной задачей, решение которой под силу только инсорсинговым компаниям крупных корпораций и внешним компаниям, специализирующимся на заказной разработке», – считает В. Лавров.

Разработав программы для своих нужд, компании стремятся окупить вложения и предлагают их рынку как самостоятельные продукты. «За последние два года мы видим значимые изменения в структуре запросов от заказчиков, когда методами заказной разработки создаются не только уникальные решения, но и решения, которые потенциально могут стать продуктами», – отметил управляющий партнер сегмента «Разработка и тестирование» компании IBS Павел Эйделанд.

### Дефицит высококвалифицированных кадров

Получила развитие за прошедший год не новая проблема дефицита кадров. Ситуацию усугубили новые тренды – повышение спроса на

заказную разработку и создание импортозамещающих продуктов. Появилось много закончивших базовые курсы «джунов» с низкой квалификацией, но специалистов, способных самостоятельно ставить и решать задачи, по-прежнему мало. И это несмотря на новый тренд – готовность к возвращению программистов, релоцировавшихся из страны после начала мобилизации.

По мнению председателя совета директоров «СёрчИнформ» Льва Матвеева, рынок ИТ-кадров остается рынком кандидатов, а не работодателей. Дефицит вызвал рост заработной платы программистов – в Москве и Санкт-Петербурге на 11–15%, в регионах – более чем на 20%, по ряду специальностей – более чем на 30%.

### Смена зарубежных рынков

Конфликт с Западом положительно сказался на доходах российских софтверных компаний – по прогнозу РУССОФТ, по итогам 2023 г. их совокупный оборот увеличится на 26%, причем продажи на внутреннем рынке вырастут на 36%.

С экспортом ситуация сложная – зарубежные продажи упадут на 24%. Продолжается вытеснение российских компаний с рынков недружественных стран. Не помогает и маскировка российских корней.

Новый тренд – ориентация на рынки дружественных стран, причем не только ближнего, но и дальнего зарубежья.





«Импортозамещение дало хороший импульс для ускорения и роста, мы сделали за три месяца то, на что у зарубежных вендоров уходило три года. Сейчас же важно смотреть дальше: как обогнать мировых лидеров в разработке. Поэтому в прошлом году PIX Robotics вышла на дружественные зарубежные рынки, такие как Латинская Америка, Азия, Ближний Восток. Клиенты видят преимущество в том, что наши решения имеют качество мирового уровня, но стоят дешевле, чем более раскрученные бренды. А мы получаем свежий взгляд на развитие продуктов, конкурируем с западными компаниями, что помогает быстрее развивать и внедрять новые технологии для российских заказчиков», – рассказал генеральный директор PIX Robotics Сергей Ложкин.

Растет активность российских компаний на Ближнем Востоке, прежде всего в ОАЭ. Еще несколько лет назад нельзя было представить работу в Саудовской Аравии, а сейчас саудиты идут на переговоры, не опасаясь запретов из американского посольства. Перспективной выглядит и Юго-Восточная Азия.

Эксперты разошлись во мнениях относительно Латинской Америки. Положительный фактор – дружественное отношение к России – нивелируется сложной логистикой, высоким уровнем инфляции и сильными профсоюзами, препятствующими внедрению некоторых решений в сфере информационной безопасности. В странах Африки беспокоит политическая нестабильность, в частности, в ЮАР – пережесты в борьбе с последствиями апартеида. В числе наиболее перспективных для российских инвестиций стран Латинской Америки – Аргентина, Бразилия, Мексика и Колумбия, из африканских – страны северной Африки и бывшие французские колонии, обладающие более квалифицированным управленческим аппаратом.

Новый тренд – российские компании не мигрируют под иностранные, что практиковалось и практикуется даже в странах Африки, а выступают именно как российские, под брендом «Россия». «Россия должна брендироваться в том числе программным обеспечением. Если российское ПО – значит, хорошее», – заявил Л. Матвеев и посоветовал, что поддержка экспорта ИТ не входит в приоритеты российских представительств за рубежом.

Выход на новые рынки – дорогой, длительный и сложный процесс. Риски введения новых санкций, сложность трансграничных платежей, нехватка ресурсов для изучения новых рынков и проведения маркетинговых кампаний – все это ограничивает возможности российских поставщиков ПО. И хотелось бы на пути выхода на новые рынки получать поддержку от государства. **IKS**



## Энергия интеллекта

**Ведущее аналитическое агентство России и СНГ в сфере телекоммуникаций, ИТ и медиа**

- Аналитика
- Стратегии
- Бизнес-планирование
- Информационно-аналитическая поддержка
- Потребительские опросы в B2C и B2B сегментах



Минск



Системная интеграция

Дата-центры

Облачные сервисы

ИТ-инфраструктура

Офисная техника



Москва



Голосовые услуги

ШПД

Мобильный интернет

VAS

Межоператорские услуги



Ташкент



Платное ТВ

Мобильное видео

Игры

Интернет-порталы

Видео-контент



Алматы



Навигация и LBS

M2M

NFC

E-commerce

Теле-медицина

# Новые линейки и безупречный сервис. C3 Solutions – еще ближе к заказчикам



**C3 Solutions, номер два в топ-10\* вендоров инженерных решений для ЦОДов, активно наращивает производственные мощности, продуктовый портфель, экспертизу и сервис. Подробнее – Дарья Алексанкина, генеральный директор компании.**

– Давайте начнем разговор с темы производства, ведь этот ресурс – ключевая характеристика настоящего вендора. Как развиваются производственные мощности C3 Solutions? Что с заводом в Шебекино?

– Наши мощности в Шебекино, которые мы в свое время оснастили по последнему слову техники, сейчас законсервированы. Производство перенесено на площадку в Белгород, туда перевезена и большая часть оборудования. Площадка растет: в ближайшее время мы запускаем новую покрасочную линию и обновляем парк станков. Отдельно выделю наш опытно-конструкторский участок. Дело в том, что от партнеров приходит все больше запросов на изготовление продуктов по техническим заданиям конкретных заказчиков. Чтобы сократить сроки разработки и производства кастомизированных изделий, мы и создали такое подразделение. ОКР или R&D в контуре компании позволяют C3 Solutions выполнять как точечные, так и масштабные сложные проекты под ключ. Это наше ноу-хау, и здесь мы очень сильны.

Позитивная история последнего времени – заключение OEM-соглашений с тремя площадками: в Костроме, Рязани и в Московской области. Подготовлена и интегрирована вся необходимая документация, чтобы выпускать наши продукты на этих предприятиях. Это сразу позволило нам снизить нагрузку в пиковые периоды на основное производство в Белгороде. Кроме того, диверсификация производственных площадок по разным регионам снижает риски, связанные с логистикой и безопасностью.

Помимо производственных площадок расширяем и штат специалистов, занимающихся разработкой и продвижением продуктов. На 30% увеличили конструкторский отдел, в два раза – отделы R&D и продуктологии. С любовью и максимальным вниманием относимся ко всем продуктам, которые

создаем и выводим на рынок. Поэтому много инвестируем в продуктивное направление, чтобы поддерживать качество наших решений и сопровождать их на протяжении всего жизненного цикла.

– Как развиваются ваши основные продуктовые линейки?

– Недавно вывели на рынок собственную линейку ИБП. Ассортимент очень широкий. В портфеле C3 Solutions системы бесперебойного питания мощностью до 1,2 МВт, напольные и стоечные решения, моноблоки и модульные аппараты. ИБП с двойным преобразованием, высоким КПД и модульной архитектурой востребованы в сегменте ИТ и ЦОДов. Моноблочные решения с возможностью быстрой замены компонентов – идеальное решение в случае ограниченного бюджета, но высоких требований ко времени ремонта. Промышленные ИБП с защитой от жестких условий эксплуатации оптимально подойдут для промышленных площадок и объектов. На эту продукцию ощущаем высокий спрос, уже есть первые продажи.

Также обновили нашу «классику» – линейку шкафов. Требования заказчиков меняются, поэтому продуктовые предложения всегда надо совершенствовать, чтобы они максимально соответствовали этим изменениям. Мы кропотливо переработали линейки шкафов, в частности, сделали их глубже – ведь в ЦОДах всегда идет борьба за эффективность использования технологического пространства.

Одна из новинок C3 Solutions – ОСП-стойка. Продукт уже есть в нашем каталоге, но сейчас мы активно дорабатываем это решение с одной из крупнейших ИТ-компаний. Интерес к ОСП есть, надеемся, что рост спроса позволит перейти к серийному производству.

Новое дыхание получила и линейка БРП. Полтора года назад начали заниматься разработкой полностью российского продукта. И сегодня предлагаем рынку настоящий стопроцентный «импортзам» – блок распределения питания на процессоре «Байкал». Это уникальная модель с пофазным и порозеточным управлением, с воз-

\* Согласно исследованию iKS-Consulting.

возможностью управлять из мобильного приложения, с «горячей» заменой розеточных модулей. Российского аналога нет. Более того, продукт по своим характеристикам превосходит и импортные аналоги. Сейчас опытные образцы развозим по заказчикам. А с нового года стартует серийное производство.

Относительно недавно мы представили собственную линейку СКС – в этом сегменте у нас одно из самых широких предложений. Есть и медножильные, и оптические системы, в том числе высокой плотности, поддерживающие как сегодняшние, так и перспективные скорости передачи данных в ЦОДах.

В этом году также обновили набор решений для edge-вычислений: это наши микроЦОДы с возможностью кастомизации практически для любой задачи заказчика.

Предлагаем и решения для охлаждения ЦОДов. Короче говоря, у нас есть решения для всех основных систем инженерной инфраструктуры дата-центров.

**– Вы достаточно давно использовали в своих комплексных решениях ИБП и средства охлаждения сторонних вендоров.**

– Да, это так. Теперь у нас свои продукты, производимые для нас по ODM-контрактам – по нашему ТЗ, под нашим брендом. Решения тщательно проработаны нашими специалистами совместно с заводом-изготовителем.

Выводя на рынок новую продуктовую линейку, очень важно иметь соответствующую экспертизу. И мы ее нарастили, существенно вложились в персонал, о чем я уже говорила.

В связи с этим отмечу один момент: не менее важно делать упор и на сервисное обслуживание. Мы понимаем, что нельзя оставлять заказчиков один на один с вопросами, возникающими в ходе эксплуатации оборудования. Мы будем рядом с ними на протяжении всего жизненного цикла наших продуктов, будем оказывать заказчикам максимальную помощь и содействие. Близость к клиенту, понимание его проблем и сложностей – главный приоритет в компании.

**– Насколько ваш сервис близок к заказчикам?**

– Для сервиса используем площадки наших авторизованных сервисных центров, которые расположены по всей территории страны. Предлагаем различные варианты сервисных SLA. В частности, есть возможность обслуживания 24/7/4, т.е. круглосуточная поддержка с реакцией в течение 4 часов. Конечно, это недешевый вариант. Обычно им пользуются крупные заказчики, для которых простой оборудования очень критичен.

Мы предлагаем различные способы, позволяющие сократить возможное время снижения уровня резервирования или простоя объекта. Так, для ряда моделей ИБП может применяться схема advanced replacement. При возникновении проблем с работой ИБП мы его сразу заменяем на другой на время ремонта. Это наше конкурентное преимущество в сервисном обслуживании ИБП.

Наши новые линейки – ИБП и кондиционеры – требуют больше внимания в процессе эксплуатации, чем те же

шкафы и стойки. И мы понимаем необходимость дальнейшего развития сервисной модели. Сдать и забыть – это не про C3 Solutions.

**– Все понимают, что для оперативной замены важно наличие того же ИБП на складе в России. Где расположены ваш?**

– Склад находится в Белгороде, в 8 ч езды на машине от Москвы. Если говорить об ИБП, то на складе уже имеются как новые изделия, так и ЗИП. Поэтому проблем с доставкой оборудования в любую точку страны не будет, из-за границы ничего везти не надо.

**– С кардинальной сменой вендоров заказчики стали чаще жаловаться на качество продуктов. Что вы делаете, дабы избежать подобных жалоб?**

– На нашем производстве четко выстроена система контроля качества. На OEM-площадках обязательно осуществляется выходной контроль. Там постоянно присутствуют наши представители, которые проверяют и тестируют выпускаемую продукцию.

Недавно мы прошли обучение по государственной программе «Производительность 2.0». В ней много внимания уделялось организации контроля качества. После прохождения обучения часть процессов мы поменяли.

У нас есть круглосуточная линия для обращений. Внимательно обрабатываем все сообщения. Более того, периодически я сама просматриваю эту линию. Если проблема возникает по нашей вине, все всегда исправим, и неважно, сколько это будет нам стоить. Наше главное правило: «Стопроцентно довольный клиент».

**– Насколько уход зарубежных брендов ускорил рост компании C3 Solutions на ЦОДовском рынке? Как вы оцениваете ее долю?**

– С помощью доступных нам данных, в том числе статистики iKS-Consulting, мы регулярно пытаемся оценить нашу долю рынка. В сегменте шкафов – это 35%, БРП – 25–30%. После ухода зарубежных вендоров многие заказчики переключились на нас. Но замечу, что в этих сегментах и до 2022 г. наши позиции были достаточно сильными. Сейчас перед нами стоит задача быстрого роста в сегментах ИБП, СКС и систем охлаждения. Все возможности для этого у нас есть.

Так, наш высокий потенциал в сегменте СКС и ИБП показали данные исследования «Карта вендоров», недавно опубликованного iKS-Consulting. Кстати, в сегменте «ИТ-стойки» мы стали лидером, заняли высокие позиции и в сегменте «Модульные/префаб-решения». Но особенно порадовало вхождение в топ-10 вендоров инженерных решений для ЦОДов, в этом рейтинге мы – вторые. Но это только второе место, а значит, есть к чему стремиться.



# Кадровый ЭДО: навигация среди айсбергов

Окончание. Начало см. «ИКС» №3'2023, с. 18.

Дмитрий Аверьянов, независимый эксперт

**Подводная часть айсберга, с которым может столкнуться «корабль» КЭДО, отнюдь не ограничивается рассмотренными в первой части статьи проблемами формата электронной подписи и сохранения юридической значимости электронных документов при длительном хранении...**



## Видимые штампы

Электронная подпись на документе при его открытии обычными средствами просмотра файлов не видна, поэтому для подсказки, что в документе что-то написано (подписано) «невидимыми чернилами», дополнительно может (в русле здравого смысла – обязан) ставиться видимый штампик с указанием даты, данных подписанта и других реквизитов сертификата подписанта. Это напоминание о том, что кроме штатного средства просмотра нужно запустить СКЗИ и с его помощью искать в документе подпись.

Понятный и имеющий большие возможности, включая визуализацию, в том числе при множественном подписании, вариант – размещение видимых штампов вне подписываемых метаданных документа (на специальных полях), например, pdf. На данный момент нет примеров использования открепляемой подписи с множественными штампами с сопоставимыми с Adobe Acrobat Reader (AAR) возможностями для отчуждаемых документов (не в системах внешних операторов СЭД).

## Регламенты

Важная составляющая КЭДО – нормативное обеспечение, включающее как получение согласия от каждого участника на использование КЭДО, так и регламент, который в том числе определяет критерии признания ЭП, что особенно актуально для признания НЭП. Через регламенты работодатель и сотрудники признают используемые механизмы (положения) организации КЭДО. Очевидно, что они не должны противоречить законам. Кроме регламента (порядка, положения) потребуется приказ о внедрении, уведомление и согласие работника.

## Сколько стоит КЭДО?

Если КЭДО не собственный проект компании, то в его стоимость входит много компонентов. В первую очередь это развертывание

или аренда УЦ и закупка КЭП в аккредитованном УЦ или НЭП, в том числе в неаккредитованном УЦ. Затем интеграция как с учетной HR-системой, так и другими смежными системами, включая долговременный архив и личный кабинет сотрудника на корпоративном портале. Опцией может быть интеграция с порталом госуслуг или сервисом «Госключ», представляющая собой отдельную ценовую позицию. Иногда сама система КЭДО является лишь надстройкой (модулем) и требует закупки платформы, например, платформы СЭД.

Далее на стоимость КЭДО окажут влияние ответы на целый ряд вопросов. Какой требуется набор сертификатов? Например, потребуются ли исследования для встраивания СКЗИ? Входят ли лицензии на СКЗИ (CSP) в состав цены? Включены ли сами серверы (оборудование, лицензии или их аренда, стоимость сервисов), в том числе TSP, OCSP, а также лицензии на их клиентские части? Не забудем о стоимости разработки регламентов (КЭДО по требованиям Трудового кодекса, собственного УЦ при наличии), обучения, развертывания, техподдержки на этапе внедрения.

Как в целом организовано внедрение? Может оказаться, что вместо договора на «КЭДО под ключ» заказчик заключит ряд двухсторонних договоров (КЭДО, интеграция и т.п.) и в итоге получит: «к пуговицам и рукавам претензий нет» (договоры подписаны), но в целом система КЭДО неработоспособна.

Навигатор по экосистеме КЭДО приведен на рис. 2.

## Подведем итоги

Развернуть собственный (on premise) «небольшой КЭДО» технически достаточно просто. Можно начать с файлового хранилища (с ограничением доступа к папкам) кадровых документов с подписанием их в отдельном приложе-

<p><b>Локация (размещение):</b></p> <ul style="list-style-type: none"> <li>– облако, включая</li> <li>а) гособлако, «Работа в России»</li> <li>б) коммерческое облако</li> <li>– своя площадка (on-premise)</li> <li>– смешанная (гибрид)</li> </ul>	<p><b>Экосистема КЭДО и окружение:</b></p> <ul style="list-style-type: none"> <li>– КЭДО (подписание, хранение, перештамповка)</li> <li>– инфраструктура ключа (УЦ)</li> <li>– взаимодействующие системы (учетная HR-система, «Зарплаты и кадры»), гос-услуги</li> </ul>	<p><b>Номенклатура е-документов:</b></p> <ul style="list-style-type: none"> <li>– максимальная, требует КЭП работодателя, НЭП сотрудника</li> <li>– «минус 7» документов (НЭП работодателя и сотрудника)</li> <li>– документы, не требующие подписи сотрудника</li> </ul>
<p><b>Формат кадрового документа:</b></p> <ul style="list-style-type: none"> <li>– основная часть документа: PDF/A-1A</li> <li>– приложения: абсолютно любой формат, в том числе эксклюзивный</li> </ul>	<p><b>Типы подписи:</b></p> <ul style="list-style-type: none"> <li>– КЭП (аккредитованный УЦ)</li> <li>– НЭП (свой УЦ, коммерч. УЦ, госключ)</li> <li>– простая подпись (пароль – логин) – худший вариант</li> </ul>	<p><b>Варианты внедрения:</b></p> <ul style="list-style-type: none"> <li>– коробочное или конструктор</li> <li>– проприетарное (закрытое) или открытое (open source)</li> <li>– лицензии платные или free (плата за поддержку)</li> </ul>
<p><b>Форматы подписи (сумма):</b></p> <ul style="list-style-type: none"> <li>– формат № 472 (CMS, ГОСТ)</li> <li>– открепляемая подпись (sig)</li> <li>– обеспечение длит. хранения, т.е. «усовершенствование» TSP+CRL/OSPR (или CADES-A)</li> </ul>	<p><b>Штампы подписи (видимые):</b></p> <ul style="list-style-type: none"> <li>– есть, встроенные в документ</li> <li>– есть, встроенные в неподписываемые метаданные документа (множественные)</li> <li>– нет (при наличии подписи)</li> </ul>	<p><b>Проверка подписи:</b></p> <ul style="list-style-type: none"> <li>– непосредственно в КЭДО (внутри периметра)</li> <li>– online на публичном собственном или стороннем ресурсе</li> </ul>

нии, скажем, «КриптоАРМ», далее перейти на полноценную DMS с кнопкой «Подписать» и подсистемой управления задачами (маршруты, сроки, напоминания и контроль). При подписании НЭП можно использовать open source-библиотеки с поддержкой отечественной криптографии (Bouncy Castle и др.).

Можно развернуть собственный неаккредитованный УЦ. Во многие HR-системы уже добавлена кнопка «Подписать», т.е. КЭДО встроен в состав учетной кадровой системы. Разработчики классического СЭД добавляют модуль КЭДО.

Основная проблема КЭДО не в «технике», а в нечетком законодательстве. Кадровые документы – чувствительные для работников сущности, от которых может зависеть многое: налоги, дотации, расчет пенсии и т.п. Если подписанные бухгалтером отчеты в ФНС, ПФР, ФСС, ФТС и т.п. при получении проверяются регулятором и после проверки вопросы к подписи (формату, сертификату и т.п.) снимаются, то в КЭДО работодатель и сотрудник остаются один на один с ЭП и вопросы к подписи могут возникнуть в течение всего установленного законом времени хранения документа (те самые 75 лет, не говоря уже о постоянном хранении). Вопросы к подписи становятся причиной оспаривания самого ЭД.

В настоящее время нет гарантии совместимости разных подписанных ЭД (ЭП и приложений к кадровому документу). Выгрузив свой документ и предоставив его третьей стороне (государственным или коммерческим структурам, например, новому работодателю), вы можете получить ответ: «Это филькина грамота, так как мы не можем убедиться в достоверности подписи на документах и прочитать приложения».

Пока не будет единого концептуального подхода и технического формата (в первую очередь нуждается в исправлении формат, указанный в приказе Минцифры № 472) для подписания кадровых документов, пользователи КЭДО останутся заложниками законодательного тумана.

Туманом в законодательстве относительно КЭДО затянута не только протоколы и форматы, но и концепции. Это косвенно подтверждают такие заявления, как письмо Минтруда от 6.10.2022 № 14-6/ООГ-6311: «Мнение Минтруда России по вопросам, содержащимся в Вашем обращении, не является разъяснением и нормативным правовым актом». В этом письме Минтруд опубликовал собственное «не разъяснение» интригующего постановления Правительства РФ № 1192 в части правил взаимодействия КЭДО с порталом госуслуг. Станным является не только сам статус письма, но и то, что выраженная в нем позиция Минтруда (интеграция с порталом госуслуг обязательна только при использовании простой подписи) противоречит письму Роструда от 01.08.2022 № ПГ/19773-6-1 (интеграция КЭДО с госуслугами обязательна в любом случае).

На неадекватность законодательства накладывается низкая грамотность пользователей, которая в немалой степени обусловлена отказом регулятора от интуитивно понятных технологий (например, от встроенной подписи AAR, PADES) в пользу менее очевидных.



В статье изложена только часть проблем кадрового электронного документооборота. Тем не менее 22.11.2021 «Титаник КЭДО» с бортовым номером 377 под фанфары продавцов КЭДО (в ожидании новых продаж) и рукоплескания кадровых служб (для них рассмотренные проблемы – это невидимая пока часть айсберга) отчалил и в условиях густого юртумена взял курс на привлекательную цифровизацию. Одной из причин крушения «Титаника», попавшего в поле айсбергов, считается то, что телеграмма о сложной ледовой обстановке затерялась. Как бы не затерялась и настоящая статья – телеграмма с таким же предупреждением, но применительно к текущему состоянию кадрового электронного документооборота. **ИКС**

▲ Рис. 2. Навигатор по КЭДО

# Программно определяемые хранилища: наращивая функционал



Николай Носов

С точки зрения функциональных возможностей отечественные программно определяемые хранилища еще отстают от продуктов ушедших с рынка зарубежных вендоров. Но разрыв сокращается.

## Виртуальное вместо реального

Отделение логического уровня управления от физического аппаратного – подход не новый и широко используемый на практике. В частности, в программно определяемых хранилищах (Software Defined Storage, SDS) за счет создания виртуальной плоскости данных предоставление хранилища и управление им абстрагируются от базового оборудования. Это позволяет управлять отдельными пулами физических ресурсов хранения как единым логическим устройством, что повышает эффективность использования, гибкость выделения и легкость масштабирования ресурсов.

Путаницу в определении вносит термин «Programmable Storage», который тоже дословно переводят как «программно определяемое хранилище». Технология Programmable Storage использует ПО для управления и настройки в конкретных задачах физических устройств хранения данных без виртуализации и в этой статье не рассматривается.

Прообразом SDS можно считать появившиеся еще в 1987 г. RAID-массивы, объединившие диски в логические элементы, с которыми и работали операционные системы. С развитием технологий росла скорость передачи данных по сети, и в логические элементы стали объединять диски разных серверов. В дальнейшем к ним подключились дисковые массивы СХД, а в самых продвинутых решениях – и облачные хранилища.

Начала набирать популярность конвергентная инфраструктура (Converged Infrastructure, CI) – предварительно настроенное аппаратное решение, которое объединяет хранилища, вычислительные и сетевые ресурсы в общую инфраструктуру, управляемую единым программным обеспечением. Конвергентная инфраструктура часто включала SDS, что дополнительно повышало ее эффективность.

Предварительно настроенное программно-аппаратное решение – как ноутбук. Запускать и работать легко, но менять конфигурацию «железа» замучаешься. Стремление к дезинтеграции вычислительных ресурсов с целью получения оптимальной для конкретной задачи конфигурации породило концепцию компонентной инфраструктуры (Composable Infrastructure) – архитектуры центра обработки данных, в которой хранилища, вычислительные и сетевые ресурсы абстрагируются от их физического местоположения и управляются программным обеспечением через единую платформу управления. В примере с ноутбуком: нажал на кнопку – получил новые диски, нажал на другую – вернул их соседу.

Пример компонентной инфраструктуры – блейд-шасси HPE Synergy, в которое при необ-

ходимости нарастить ресурсы вставляются серверы-лезвия с корзинами для дисков. Конструктив дает возможность прямого подключения дисков без участия RAID-контроллера, что необходимо при использовании серверов в качестве компонентов SDS. Управляется блейд через Composer – мини-сервер архитектуры x86 с модифицированным ядром Linux. На нем работает обеспечивающая единое управление лезвиями всех собранных корзин программа OneView.

В качестве компонентной инфраструктуры можно рассматривать и облачную платформу, которая также дает пользователям возможность создавать «под себя» вычислительную инфраструктуру и управлять ею.

Совсем нельзя обойтись без SDS при развертывании гиперконвергентной инфраструктуры (Hyper-converged Infrastructure, HCI). Совмещение слоя хранения и слоя вычислений на горизонтально масштабируемом и относительно типовом «железе», совмещение узла SDS и гипервизора на одном физическом хосте повысило гибкость и снизило расходы на ИТ.

Преимущества SDS оценили облачные провайдеры и начали активно внедрять технологию, повышающую эффективность использования хранилищ. Развивались и технологии доступа. Приобрели популярность объектные хранилища, позволяющие загружать, получать и удалять данные по имени. Пионером стала компания AWS, в 2006 г. запустившая основанный на объектном хранилище файловый хостинг Amazon Simple Storage Service (Amazon S3). Пользователи получили возможность в любое время задействовать любой объем данных, который не привязан к физическому носителю и доступен в любой точке сети, опутавшей весь мир.

Преимущества SDS оценили облачные провайдеры и начали активно внедрять технологию, повышающую эффективность использования хранилищ. Развивались и технологии доступа. Приобрели популярность объектные хранилища, позволяющие загружать, получать и удалять данные по имени. Пионером стала компания AWS, в 2006 г. запустившая основанный на объектном хранилище файловый хостинг Amazon Simple Storage Service (Amazon S3). Пользователи получили возможность в любое время задействовать любой объем данных, который не привязан к физическому носителю и доступен в любой точке сети, опутавшей весь мир.

Преимущества SDS оценили облачные провайдеры и начали активно внедрять технологию, повышающую эффективность использования хранилищ. Развивались и технологии доступа. Приобрели популярность объектные хранилища, позволяющие загружать, получать и удалять данные по имени. Пионером стала компания AWS, в 2006 г. запустившая основанный на объектном хранилище файловый хостинг Amazon Simple Storage Service (Amazon S3). Пользователи получили возможность в любое время задействовать любой объем данных, который не привязан к физическому носителю и доступен в любой точке сети, опутавшей весь мир.

## Базовый функционал

При этом от SDS по-прежнему требуется поддерживать классический блочный доступ (интерфейс iSCSI), когда файлы разбиваются на «кусочки» одинакового размера, каждый с собственным адресом, но без метаданных (по сути, прямой доступ к жесткому диску), а также



**Антон Салов,**  
член оргкомитета,  
РССРА

интерфейс NFS файлового хранилища, имеющего древовидную структуру из файлов и вложенных папок.

В число базовых требований к SDS входит и отказоустойчивость. Важно, чтобы архитектура SDS позволяла создавать систему с любым уровнем избыточности для защиты от потери данных в случае отказа одного или нескольких узлов. Также защиту данных и доступность системы обеспечивает использование методов шифрования, резервирования и репликации данных, в частности, удаленной асинхронной репликации (remote replication) – копирования данных на удаленную, находящуюся в другой локации систему хранения с задержкой, что позволяет задействовать более медленные сетевые каналы.

Для быстрого восстановления данных удобна функция создания мгновенных снимков (snapshot) – копий состояния системы или данных в определенный момент времени.

Чтобы конфиденциальную информацию нельзя было восстановить после удаления, применяются методы гарантированного удаления данных с жестких дисков и других устройств хранения. SDS обычно использует аппаратное обеспечение для перезаписи находящейся на устройстве информации случайными данными, что делает восстановление технически невозможным.

Полезны функции линейного наращивания производительности SDS, автоматическая балансировка нагрузки между узлами и контроль качества обслуживания (QoS), позволяющий поддерживать требуемый уровень производительности для рабочих нагрузок. Низкую задержку и повышенную производительность при чтении данных обеспечивает FlashCache – встроенный кеш чтения/записи на базе флеш-памяти.

Оптимизировать использование устройств хранения помогают сжатие и дедубликация – удаление дублирующих копий данных. Применяется inline-дедубликация, при которой дубликаты удаляются непосредственно в процес-

се записи данных, и post process-дедубликация, когда удаление дубликатов происходит после записи данных.

Для эффективного и экономичного управления в SDS служит многоуровневое хранение (tiering) – группировка отдельных наборов данных по уровням их технических характеристик, типу носителя и т.д. Перенос наиболее активных наборов данных на быстродействующие носители повышает производительность SDS, а редко используемых данных на дешевые медленные носители – снижает расходы.

В настоящее время SDS применяются для оптимизации использования дисковых ресурсов СХД в традиционных системах; в работающих с общим пулом вычислительных ресурсов гиперконвергентных инфраструктурах; в конвергентных и компонуемых инфраструктурах, имеющих отдельный пул хранения; в ряде облачных платформ (например, VMware vRealize Suite или Huawei FusionSphere).

### Российский рынок до...

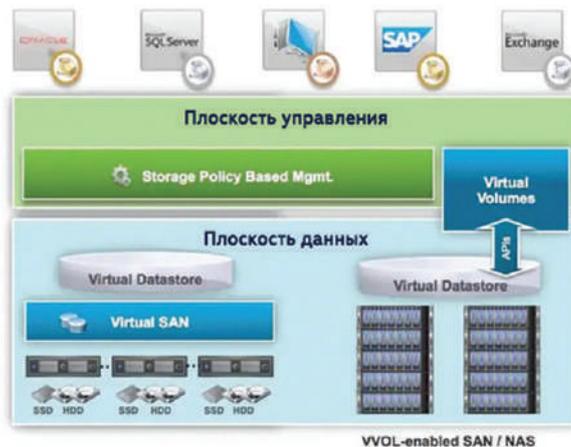
До февраля 2022 г. на российском рынке программно определяемых систем хранения присутствовали решения как отечественных компаний («Аэродиск», «Рэйдиск», «Росплатформа» – последняя изначально предлагала коробочное ПО, работающее с любыми серверами стандартной архитектуры), так и зарубежных (Datacore, Microsoft, Nexenta, Open-E). В числе классических SDS, изначально разрабатывавшихся для объединения дисковых ресурсов серверов в единый пул, активно предлагалось решение PowerFlex (ранее Dell EMC ScaleIO) компании Dell Technologies.

Крупные компании, такие как Mail.ru (ныне «VK Цифровые технологии», VK), имеющие большие команды разработчиков, использовали программно определяемые системы хранения с открытым кодом, прежде всего Ceph. Менее крупные использовали GlusterFS от Red Hat, не требующую высококвалифицированной поддержки при эксплуатации.

В области гиперконвергентных систем лидировали компания Nutanix и доминировавшая на рынке серверной виртуализации компания VMware, которая предлагала решения как для гиперконвергентных, так и для конвергентных инфраструктур. Решение VMware Virtual SAN (vSAN) позволяет объединять SSD-накопители и обычные диски, подключенные к локальным ESXi-серверам (хостам), в общее высокоустойчивое хранилище данных, к которому могут обращаться все узлы кластера vSphere самой популярной на корпоративном рынке платформы виртуализации.

На уровне управления (Control Plane) в SDS от VMware можно включать виртуальные тома

Структура программно определяемого хранилища VMware ▶



Источник: VMware

хранилищ, даже расположенных в облаке, с блочным (SAN) и файловым (NAS) доступом, что удобно для построения гибридных архитектур. При этом систему виртуализации хранилищ vSAN не надо устанавливать – она уже входит в состав гипервизора ESXi и жестко привязана к платформе виртуализации VMware vSphere.

Аналогами и конкурентами vSAN являются Nutanix DSF, PowerFlex, Datacore Hyperconverged Virtual SAN, HPE StoreVirtual, в которых на каждом хосте запускается отдельная виртуальная машина, управляющая виртуализованными ресурсами хранения хоста в Control Plane. Все эти решения совместимы не только с VMware vSphere, но и с Microsoft Hyper-V, а HPE StoreVirtual – еще и с платформами на базе гипервизора KVM.

Существуют и решения с компонентной архитектурой. Пионером стала компания Cisco с решением Cisco UCS, затем на рынке появились программно-аппаратные комплексы Dell EMC PowerEdge MX и HPE Synergy.

### ...и российский рынок после

Санкции и уход с российского рынка зарубежных вендоров ПО заставили бизнес переосмотреть стратегии развития ИТ и обратить внимание на отечественные решения, в том числе на SDS. Дополнительными стимулами к развертыванию этих систем стали:

- высокая стоимость доступных на рынке отечественных аппаратных платформ, ограничивающая возможности закупки техники;
- наличие только базовых моделей серверов общего назначения, идеально подходящих для создания конвергентных и гиперконвергентных инфраструктур;
- желание максимально использовать уже имеющиеся вычислительные ресурсы.

К уже упоминавшимся решениям компаний «Росплатформа», «Рэйдикс» и «Аэродиск» стоит добавить ряд коммерческих продуктов от компаний «Киберпротект» и «Базис». «Росплатформа» предлагает самостоятельное полноценное SDS-решение «Р-Хранилище» на базе разработок компании Parallels, «Киберпротект» – распределенное хранилище в составе своей «Кибер Инфраструктуры», SDS-продукт входит и в «Базис. ДинамиX» – платформу для DevOps.

Кроме того, SDS входят в облачные платформы, в том числе зарегистрированные в Едином реестре российских программ для ЭВМ и баз данных (ЕРРП). Как правило, в связке с платформой виртуализации используются модификации open source SDS-решений. Например, в связке с ПК СВ «Брест» и «Альт Сервер Виртуализации» применяется Serph. С доработки Serph начинала свое время и компания Mail.ru.

Компания-разработчик	Решение	Дата включения в ЕРРП, рег. номер
«Росплатформа»	«Р-Хранилище»*	03.05.2017, № 3380
НТЦ ИТ РОСА	ROSA Virtualization	10.01.2019, № 5091
«Киберпротект»	«Кибер Инфраструктура»	07.04.2020, № 6402
НИЦ «Аэродиск»	«Аэродиск Восток» vAIR	31.12.2020, № 8787 31.12.2020, № 8802
«Рэйдикс»	RAIDIX 5	04.03.2021, № 9477
«СХД Баум»	BAUM Storage AI	25.06.2021, № 10870
ITglobal.com («Итглобалком Рус»)	vStack	18.11.2021, № 11995
«Шаркс Датацентр»	SharxStorage	18.11.2021, № 12034
«VK Цифровые технологии» (VK)	VK Cloud Storage	06.06.2023, № 17861

\* В связке с «Р-Виртуализация» реализуется функционал HCI

GlusterFS используется в российских платформах виртуализации, базирующихся на open source-решениях Red Hat (система управления виртуализацией oVirt), – SpaceVM (Veil), РЕД ОС, HOSTVM, zVirt и ROSA Virtualization (НТЦ ИТ РОСА), причем РОСА предлагает и гиперконвергентное решение.

Вендоры SDS и HCI, разработавшие решения для рынка, которые включены в ЕРРП, и осуществившие известные внедрения в сторонних организациях, представлены в таблице.

Одной из первых в нашей стране стала пропагандировать использование SDS и предложила свое решение компания «Росплатформа», давно и довольно успешно конкурировавшая с Nutanix на рынке гиперконвергентных систем. До февральских событий бизнес чаще предпочитал решения американской компании, а опасавшиеся санкций организации – продукт «Росплатформы».

Компания продает неисключительные права (лицензии) без ограничения срока действия и сертификаты на техническую поддержку. «Р-Хранилище» лицензируется по объему (в те-

▲ Наиболее известные российские разработчики программно определяемых хранилищ и их решения, включенные в ЕРРП

Переход на программно определяемые СХД позволит российским предприятиям одновременно с импортозамещением старых систем решить три ключевые задачи: модернизировать ИТ-инфраструктуру, создать платформу для запуска новых цифровых сервисов и уменьшить зависимость от «черных ящиков» – аппаратных комплексов, требующих постоянной вендорской поддержки. Таким образом заказчики смогут не просто заменить один закрытый комплекс на другой, а создать новую, современную ИТ-архитектуру.



Сергей Члек,  
управляющий директор,  
«Росплатформа»



**Дмитрий Лазаренко,**  
директор бизнес-сегмента SaaS, VK

Согласно нашим тестам, гиперконвергентные системы неоптимальны для высоких нагрузок: приходится выбирать – дать меньше ресурсов либо кластеру СХД, либо клиентским виртуальным машинам. Компания решила не идти на компромисс и остановилась на конвергентной архитектуре, гарантированно предоставляя ресурсы как кластеру хранения данных, так и кластеру вычислений. Они находятся на разном оборудовании. На кластере SDS установлено управляющее ПО, отвечающее за распределение файлов, блоков и объектов, балансировку, мониторинг. К серверам кластера SDS по сети Ethernet подключаются виртуальные машины.

рабайтах) полезного пространства виртуально-го хранилища, стоимость не зависит от числа серверов или дисков в кластере.

Отказоустойчивость достигается репликацией данных между серверами. Архитектура «Р-Хранилища» рассчитана на потерю любого физического сервера или группы серверов целиком, а не только отдельного диска. Все данные хранятся в нескольких копиях, при этом система никогда не хранит более одной копии на физическом сервере/стойке/комнате.

К преимуществам «Р-Хранилища» по сравнению с западными аналогами управляющий ди-

ректор «Росплатформы» Сергей Члек отнес независимость от производителей серверного оборудования (решение устанавливается на любое Linux-совместимое оборудование), устойчивость к санкциям и круглосуточную поддержку.

Общие с «Р-Хранилищем» корни и во многом схожие характеристики имеет решение «Кибер Инфраструктура» компании «Киберпротект».

НТЦ ИТ РОСА сделала ставку на open source и выпускает SDS- и HCI-решения, очень похожие на продукты Red Hat. Плюс подхода – системы удобные, проверенные на большой базе клиентов американского гиганта. Минус – зависимость от западных разработчиков, определяющих направления развития продуктов. Перспективным выглядит использование решений в негосударственных компаниях, применявших ПО ушедших с рынка западных вендоров.

В основе SDS vStack Storage компании «Итглобалком Рус» лежит файловая система с менеджером логических томов ZFS. Слой состоит из пулов, которые включают в себя диски каждого узла. В каждый момент времени пул работает на конкретном узле кластера. Один из ключевых атрибутов кластера – избыточность, при которой в работе инфраструктуры используется больше элементов, чем требуется. Это позволяет обеспечить резервирование. Если один из узлов выйдет из строя, он будет исключен из кластера. При этом пулы потеряют по одному диску. После этого благодаря процедуре аварийного переключения пул с вышедшего из строя узла и все работавшие на нем виртуальные машины

## В чем российские SDS уступают зарубежным



**Михаил Чусавитин,**  
менеджер по развитию бизнеса по направлению серверы и СХД, Netwell

Большинство проблем, с которыми сталкиваются пользователи отечественных систем SDS и HCI, – прямое следствие начальной стадии развития продукта. Не все функции еще отточены производителями, и часто требуется «ручное» вмешательство в работу системы на нижнем уровне. Это ведет к повышению спроса на опытных специалистов с глубоким знанием продукта и систем на базе Linux.

В сравнении с решениями VMware или Nutanix российские системы проигрывают прежде всего в простоте использования и качестве интерфейсов администрирования.

Частая проблема – отсутствие тесной интеграции между двумя системами: хранилищем и виртуализацией в рамках конвергентной системы, предлагаемой российскими разработчиками. Решение иногда выглядит как пазл, собранный из отдельных продуктов, которые слабо интегрированы между собой и не настроены на вы-

сокую производительность и бесперебойную работу.

Практически полное отсутствие в отечественных решениях таких механизмов оптимизации стоимости, как полноценная компрессия, дедупликация, тонкие клоны и пр., пока не стало насущной проблемой их пользователей. Однако в скором времени из-за роста конкуренции на этом направлении и сокращения финансирования проектов перехода на «реестровое» ПО данный фактор даст о себе знать.

На текущем этапе адаптации продуктов пользователей больше волнует надежность работы системы, чем оптимальность использования имеющихся вычислительных и дисковых ресурсов, поэтому большинство администраторов предпочитают не использовать те немногочисленные функции, которые позволяют снизить стоимость владения, с тем чтобы упростить решения и уменьшить число возможных точек отказа инфраструктуры.

станут доступны на другом узле. Процедура аварийного переключения ресурсов выполняется автоматически.

Компания «Шаркс Датацентр» разработала платформу SharxStorage – распределенное, линейно масштабируемое блочное хранилище, имеющее высокую производительность и отказоустойчивость. Продукты компании используются преимущественно в решениях для транспортной отрасли федерального масштаба: в облачной платформе транспортно-логистических сервисов на базе «Транстелекома», инфраструктуре федерального оператора электронного пломбирования грузов СОПТ, для оплаты проезда и обеспечения функционирования АСУДД на ЦКАД и трассе М12 ГК «Автодор».

В рамках конвергентной инфраструктуры может использоваться созданная компанией «СХД Баум» (ранее «СК-СХД») система BAUM Storage AI. В ноябре 2022 г. компания F+ tech (головная структура «Марвел Дистрибуции») купила 49% акций ООО «СК-СХД» и собирается в перспективе занять около 30% российского рынка систем хранения данных.

Из новинок – появившееся в ЕРРП летом 2023 г. решение VK Cloud Storage. Типовой заказчик – строящий частное облако сервис-провайдер крупной корпорации. VK Cloud Storage – это коробочное решение, отчуждаемый софт, устанавливаемый в зоне клиента с оплатой за лицензии. VK предлагает зональные хранилища, ассоциированные с конкретным ЦОДом, причем разных типов – дешевые на дисках HDD и быстрые на NVMe и SSD. Клиент сам выбирает тип системы хранения и зону доступности. При этом в любой момент он может изменить решение, и VK в живом режиме перенесет его данные на другую систему хранения.

К категории SDS относятся несколько решений VK, включая блочные, файловые (базирующиеся на блочном) и объектные хранилища для платформы x86. Самое востребованное – S3-совместимое объектное хранилище, разработанное еще тогда, когда компания называлась Mail.ru. В нем используются помехоустойчивое кодирование с гарантированной избыточностью, автоматическая балансировка нагрузки между узлами, дедупликация и сжатие. Для ряда нагрузок в объектном хранилище реализован механизм FlashCache.

Среди других вендоров SDS стоит отметить компанию «Рэйдикс», которая предлагает российскую программно определяемую СХД для задач, требующих высокой производительности. В частности, СХД на базе RAIDIX использовалась в качестве хранилища для инфраструктуры НРС национального проекта по обмену академической информацией Academic

Cloud – системы из 11 отказоустойчивых кластеров в Центре вычислительных наук института RIKEN (Япония).

vAIR компании «Аэродиск» поставляется как в виде ПО, так и в виде программно-аппаратного комплекса «Аэродиск Machine-V». В ЕРРП входит и поддерживающая систему виртуализации СХД «Аэродиск Восток», реализованная на российских процессорах «Эльбрус». Среди заказчиков компании – Агентство по страхованию вкладов, Росстандарт и Росавтодор.

### Зарубежное или отечественное?

С точки зрения базовых функциональных возможностей российские решения в целом выглядят неплохо. Но у экспертов есть претензии к полноте реализации функций, простоте использования и качеству интерфейсов администрирования. Частая проблема конвергентных систем российских разработчиков – отсутствие тесной интеграции между пулами хранения и вычисления, что сказывается на производительности и надежности работы.

У технологий есть свои ограничения. Ряд экспертов считает, что HCI – это нишевый продукт для однородных легких нагрузок типа виртуальных рабочих мест (Virtual Desktop Infrastructure, VDI), когда создается большое количество одинаковых образов рабочих машин пользователей. Если шаблоны, из которых идут основные запросы на чтение, «размазаны» по хостам, так что локальная копия есть на каждом гипервизоре, то задержки минимальны и скорость чтения хранилища приемлема.

Однако для виртуализированного ЦОДа более типична ситуация работы множества разных машин с различающимися нагрузками. В этом случае лучше выделить в отдельные группы серверы (хосты) для СХД (SDS, SAN или NAS) и виртуальных машин, а такая архитектура уже не может рассматриваться как гиперконвергентная.

Применение SDS для высоконагруженных приложений не всегда успешно. В этом случае целесообразнее ограничиться виртуализацией серверов или использовать не виртуализированную инфраструктуру.

Тем не менее своя ниша у SDS, бесспорно, есть, и системы этого класса будут применяться и дальше. Российские решения, хотя и отстают от западных, в целом обеспечивают основные потребности заказчиков и могут заместить продукты ушедших с рынка зарубежных вендоров. **ИКС**

# Карта вендоров – зеркало рынка

В сентябре 2023 г. на форуме «ЦОД» в Москве агентство iKS-Consulting представило результаты очередного исследования по основным сегментам оборудования для ЦОДов.

**Александр Барсков;**  
**Дмитрий Горкавенко,**  
директор по развитию бизнеса, iKS-Consulting

Исследование «Карта вендоров» включает топ-10 производителей инженерных решений для ЦОДов и позиции вендоров в четырех продуктовых сегментах, уже ставших для карты традиционными (ИБП, системы кондиционирования и вентиляции (СКВ), СКС и стойки), а также в двух новых: ДГУ и контейнерные/модульные и префаб-ЦОДы.

Для составления «Карты вендоров» применялось углубленное анкетирование ключевых экспертов крупных российских ЦОДов, ведущих проектировщиков и интеграторов в этой области. Всего было опрошено более 50 специалистов.

Топ-10 формировался непосредственно по ответам респондентов, каждый из которых называл первую, по его мнению, десятку компаний – производителей инженерных решений для центра обработки данных в России в 2023 г.

Не удивляйтесь, что топ-10 содержит 12 компаний: результаты трех компаний оказались столь близки, что аналитики iKS-Consulting поставили их на одно (9-е) место. Всего в топ-10 вошли семь отечественных и пять зарубежных компаний. Наиболее полно представлены поставщики комплексных решений: Systeme Electric, C3 Solutions, Delta Electronics, ДКС, Huawei, EMILINK, Schneider Electric. Это компании, которые предлагают все системы инженерной инфраструктуры ЦОДов (или большую их часть): ИБП, СКВ, шкафы/стойки. Остальные – более узкоспециализированные производители. Два («Парус электро» и Kehua Tech) занимаются ИБП, два («Рефкул» и EMILINK) – СКВ и один (GreenMDC) – контейнерными/модульными ЦОДами. Впрочем, GreenMDC можно рассматривать и как поставщика комплексных решений, поскольку в составе модульных ЦОДов обычно присутствуют все основные инженерные системы.

**TOP 10**

ТОП-10 ВЕНДОРОВ инженерных решений для ЦОДов в России в 2023 году

1	Systeme Electric
2	C3 Solutions
3	Парус электро
4	Delta Electronics
5	ДКС
6	Kehua Tech
7	Huawei
8	Рефкул
9	EMILINK
9	Envicool
9	Schneider Electric
10	GreenMDC

## КРИТЕРИИ ОЦЕНКИ

1. Уровень доверия вендору
2. Способность вендора наращивать свою долю на рынке России
3. Удовлетворенность широтой линейки решений/модельного ряда вендора
4. Наличие известных инсталляций, интересных проектов в РФ
5. Признание вендора профессиональным сообществом
6. Удовлетворенность качеством систем/оборудования вендора
7. Степень уверенности в том, что вендор исполнит все обязательства, связанные с поставкой оборудования
8. Удовлетворенность расчетным сроком службы оборудования
9. Технологическое лидерство (вендор имеет собственные технологические разработки высокого уровня и реализует их в своих решениях)
10. Удовлетворенность уровнем цен вендора в конкурентном окружении
11. Степень уверенности в том, что вендор не уйдет из страны, не прекратит работу в РФ
12. Удовлетворенность сроками и условиями поставки оборудования
13. Наличие локальных складских запасов ЗИП в РФ
14. Наличие квалифицированного персонала в РФ
15. Проактивность и гибкость вендора, способность заранее адаптироваться к технологическим, экономическим и политическим изменениям
16. Технологическая открытость (заказчики знают о подводных камнях и возможных сложностях решений вендора)
17. Соответствие заявленных характеристик оборудования реальным эксплуатационным
18. Доступность сопроводительной технической документации (включая листы подбора, результаты независимого тестирования и пр.)
19. Уникальность вендора для задач конкретного заказчика (на рынке сложно найти аналоги, столь же хорошо соответствующие его потребностям)
20. Ответственность вендора перед заказчиком за исполнение обязательств на всех этапах сотрудничества
21. Стабильность, устойчивость цен, сроков и условий поставки
22. Знание вендором конкретных клиентов, их инфраструктуры и специфических особенностей
23. Авторитет сотрудников вендора, их доступность для консультаций при личном обращении или в ходе профессиональных мероприятий
24. Удовлетворенность сервисным обслуживанием
25. Затраты на эксплуатацию оборудования
26. Ремонтопригодность оборудования, включая универсальность, совместимость с запчастями других вендоров
27. Юридическая чистота и прозрачность вендора, отсутствие юридических, налоговых, финансовых или других значимых обременений.

Карты продуктовых сегментов составлялись по более сложному алгоритму. В каждой из шести категорий эксперты по 10-балльной шкале оценивали каждую из предложенных компаний по 27 критериям (см. «Критерии оценки»). Затем эти оценки использовались для расчета двух основных показателей:

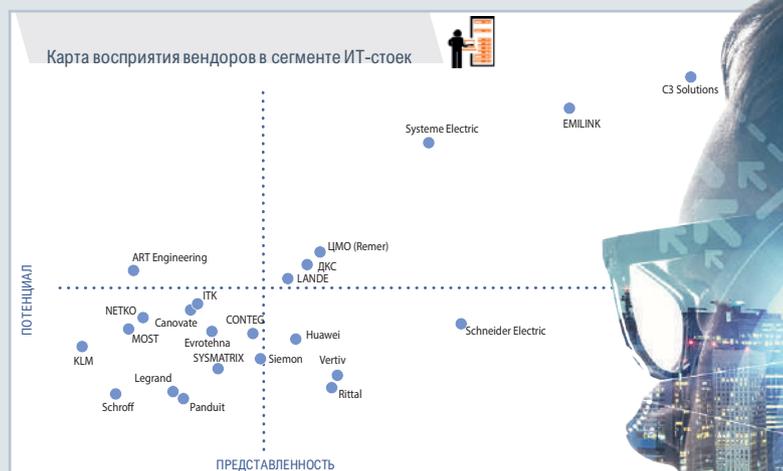
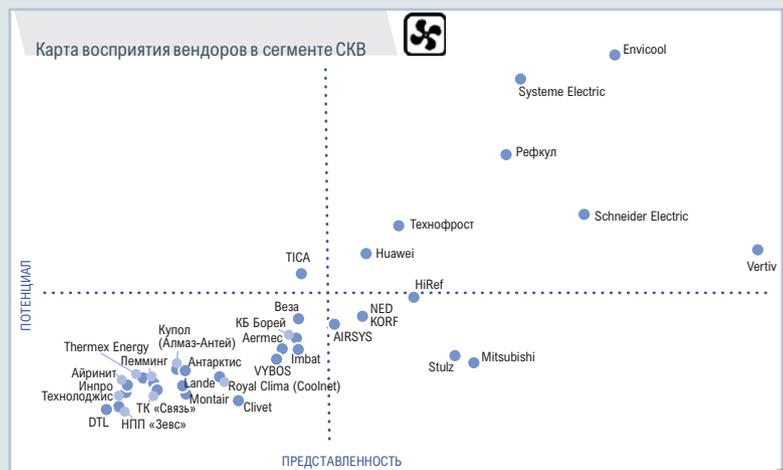
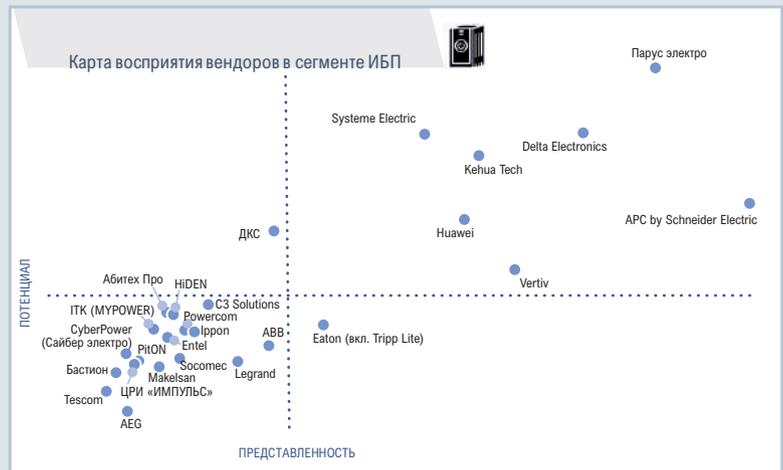
- представленности – оценки присутствия решений вендора в инфраструктуре и восприятия заказчиков с учетом отношения к нему;
- потенциала – оценки способности вендора к развитию в РФ в текущих условиях с учетом отношения к нему заказчиков.

Кроме оценок по 27 критериям в расчете учитывались вхождение вендора в топ-10, его ассоциация с конкретным продуктовым сегментом, использование его продуктов в ЦОДах заказчика за последние пять лет и планы инсталляции таких продуктов в 2023–2024 гг.

Расчеты представленности и потенциала проводились по модели, разработанной аналитиками iKS-Consulting. Оценки по каждому из критериев учитывались при расчете показателей с определенными весовыми коэффициентами. Например, критерий «Степень уверенности в том, что вендор не прекратит работу в РФ» с максимальным весом учитывался при расчете потенциала компании. А критерий «Наличие квалифицированного персонала в РФ» вносил вклад как в представленность, так и в потенциал.

В сегменте ИБП настоящим прорывом года стала компания «Парус электро». Видимо, в портфеле продуктов этого российского производителя, давно работающего в данном сегменте, нашлись решения, которые по мощности и другим показателям оказались в проектах подходящей заменой ИБП ушедших APC, Vertiv, ABB и Eaton – их продукция до 2022 г. в ЦОДах доминировала. Отсутствие таких решений, в первую очередь высокой мощности, обусловило относительно скромные позиции компаний Ippon и Powercom, которые, по данным ITResearch, лидируют на российском рынке и исторически специализировались на системах небольшой мощности. Поскольку они уже ликвидировали отставание по мощным ИБП, можно ожидать существенного улучшения их позиций в следующем году.

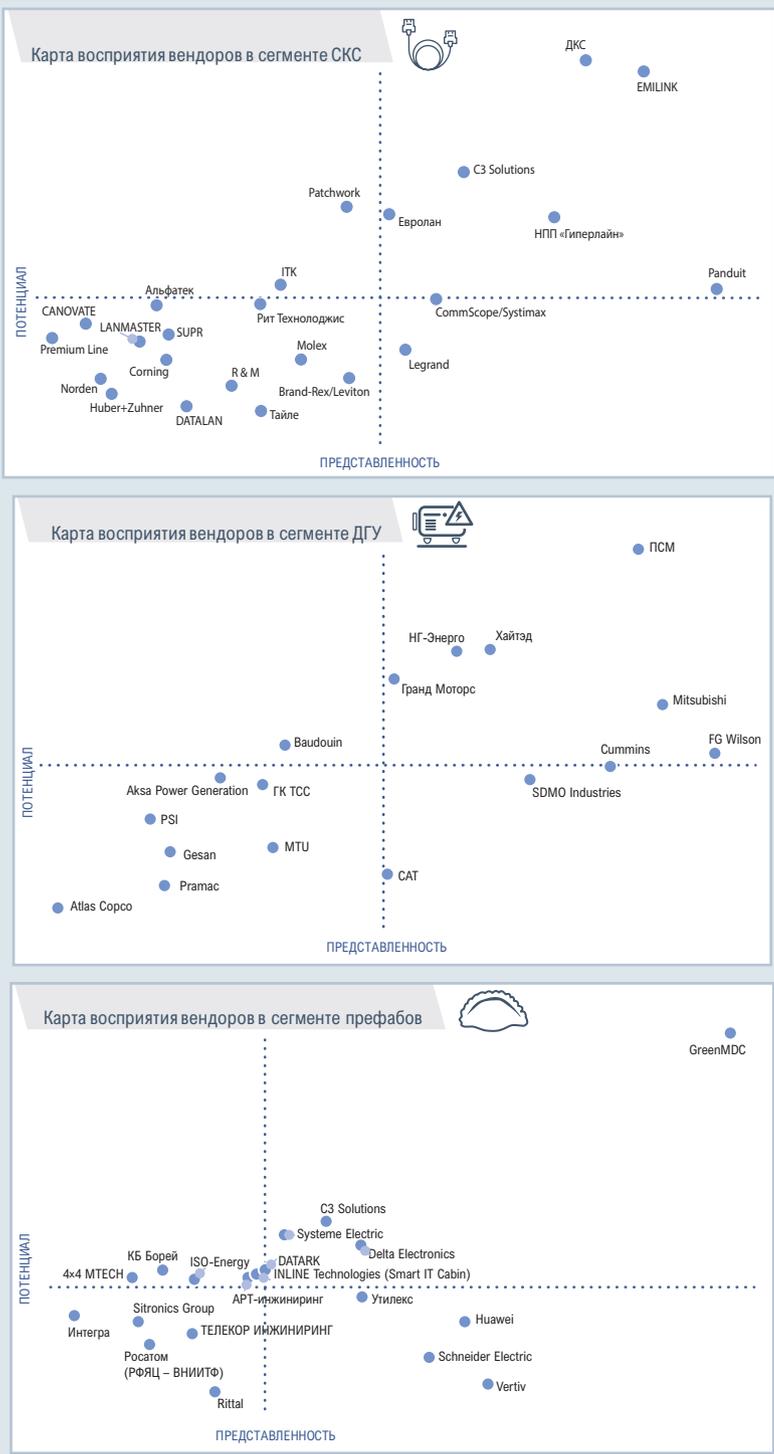
Также следует отметить высокие позиции Delta Electronics, Kehua Tech и Systeme Electric. Последняя, будучи наследницей российских активов компании Schneider Electric, много лет главенствовавшей на рынке инженерной инфраструктуры ЦОДов, заняла достойные позиции во всех сегментах, где представлена,



и стала первой в топ-10. Systeme Electric смогла сохранить самое основное – команду и экспертизу – и быстро наполнила портфель продуктов. Но ее лидерство пока, скорее, по восприятию заказчиков, а не по инсталляциям в конкретных проектах.

В сегменте СКВ явное первенство у китайской Envicool. Эта компания, одна из немногих зарубежных, имеет официальное представительство в России. Кроме того, она занимает ведущие позиции и на китайском рынке. Среди российских производителей





СКБ опережают коллег компании «Рефкул» и «Технофрост».

Замечу, что в сегментах ИБП и СКБ в правом верхнем квадранте (наибольший потенциал – наибольшая представленность) много зарубежных производителей. Дело в том, что в этих решениях есть целый ряд компонентов (компрессоры, вентиляторы, силовая электроника, автоматика) ведущих западных и японских компаний, которые официально недоступны российским производителям. А китайские вендоры применяют их в своих изде-

лиях, более того, поставляют российским заказчикам в составе ЗИП.

В сегменте ИТ-стоек весь правый верхний квадрант заняли наши производители: первая тройка – C3 Solutions, EMILINK и Systeme Electric. Это понятно: металла в стране много, резать, сваривать и красить его мы умеем, а контроллеры и силовая электроника для стоек не нужны. Можно сказать, что в этом сегменте произошло полное импортозамещение.

В верхней правой части карты по СКБ – тоже российские производители. Лидируют EMILINK и ДКС. Хочется отметить также НПП «Гиперлайн», C3 Solutions и «Евролан»: они совсем недавно представили СКБ для ЦОДов, но уже получили отличные оценки от заказчиков. Немного настораживает тот факт, что для высокопроизводительных высокоплотных СКБ используются соединители преимущественно двух компаний из недружественных стран (японской Senko и американской US Conec), но пока никто из российских сборщиков не высказывает опасений относительно возможных проблем с поставками.

В двух новых для «Карты вендоров» сегментах ситуация сложилась следующим образом. В сегменте ДГУ высокие показатели у РСМ, «Хайтед», «НГ-Энерго» и «Гранд Моторс». Переход на китайские дизели пока выглядит безоблачным, но, как и в случае с китайскими автомобилями, только время покажет, насколько они надежны. Ряд экспертов говорят о том, что китайские ДГУ запускаются и выходят в рабочий режим существенно дольше, чем лучшие западные двигатели. Это значит, что заказчикам придется потратиться на увеличение времени автономной работы от аккумуляторов. А это и деньги, и дополнительные площади.

В сегменте модульных, контейнерных и префаб-ЦОДов впереди с большим отрывом компания GreenMDC. Здесь важно уточнить, что опрашивались крупные ЦОДы, которые не очень активно используют контейнеры, поэтому в данном случае речь идет, скорее, о знании бренда. Можно предположить, что при обращении к более целевой группе заказчиков (например, из нефтегазовой отрасли) позиции других ведущих игроков, таких как DATARK и «Утилекс», были бы выше. В этом сегменте также можно отметить Sitronics: во-первых, модульные ЦОДы эта компания предлагает вместе с ИТ-оборудованием, во-вторых – по модели «ЦОД как услуга».

В целом индустрия ЦОДов с большим интересом встретила очередное исследование iKS-Consulting. «Карта вендоров» – это эффективный инструмент как для оценки «здоровья» конкретных брендов, так и для их анализа при выборе поставщика оборудования для инфраструктуры ЦОДов. **ИКС**



21 марта 2024

Москва

Формат: офлайн + онлайн



**Cloud & Connectivity** – форум для профессионалов, занимающихся внедрением сервисной модели и облачных услуг, мультиклауда и гибридных ИТ-архитектур, обеспечением непрерывности и безопасности бизнеса в облачной среде.

В числе задач Cloud & Connectivity 2024 – формирование единой позиции отрасли по актуальным вопросам рынка облачных и коммуникационных сервисов, а также обсуждение и выработка основными игроками ключевых векторов развития сервисной модели как для корпоративных, так и для государственных заказчиков.

**В фокусе Cloud & Connectivity 2024:**

- Российский рынок облачных услуг. Динамика роста
- Связность как необходимое условие доступности и надежности облаков
- Edge-облака: концепция и технические решения
- Из чего строить облака: российские платформы
- Облака и безопасность

Организаторы



Минцифры  
России



КООРДИНАЦИОННЫЙ СОВЕТ  
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ  
Автономная некоммерческая организация

При поддержке



cloudcon.ru

# Охлаждение от Systeme Electric: все, что нужно заказчикам

**Компания Systeme Electric, полностью унаследовавшая команду инженеров по системам охлаждения Schneider Electric в России, быстро наполнила свой портфель предложениями соответствующими продуктами. На наши вопросы отвечает Михаил Каширских, менеджер по развитию систем охлаждения.**



**– Настолько ли полон ваш продуктовый портфель систем охлаждения, как это было у Schneider Electric? Какие кондиционеры вы уже предлагаете?**

– Мы предлагаем все основные решения. Начну с наиболее популярного варианта – внутрирядных кондиционеров. Это линейка CoolRow. В нее входят модели шириной 300 и 600 мм, на охлажденной воде (холодопроизводительностью от 25 до 65 кВт) и на фреоне (7–70 кВт). Более того, мы не стоим на месте, продолжаем расширение ассортимента. Теперь у нас есть фреоновые модели с фрикулингом. Причем используется не косвенный фрикулинг, а перекачка жидкого фреона в холодный период года. По глубине и высоте все внутрирядные кондиционеры имеют те же размеры, что и наши стойки. Поэтому они четко встают в ряд со стойками, ничего никуда не выступает.

Периметральные кондиционеры – CoolRoom – также представлены в вариантах на фреоне (20–120 кВт) и на воде (20–250 кВт, а по запросу возможен выпуск и более мощных моделей). Также поддерживается фреоновый фрикулинг. Если у Schneider Electric размеры подобных кондиционеров были жестко зафиксированы, то мы их можем варьировать. Например, базовую глубину 995 мм – уменьшить до 900 мм. Или изменить ширину. В проектах это помогает лучше вписаться в выделенное помещение.

Все наши кондиционеры могут комплектоваться увлажнителями двух вариантов: привычными электродными или пленочными. Преимущество последних в том, что для них не нужно электричество: просто подводится вода, которая увлажняет мат. Но, как и электродные (которым требуется регулярная замена парового цилиндра), пленочные нуждаются в обслуживании – в зависимости от качества воды увлажняемый мат надо периодически очищать.

Конденсаторы для кондиционеров могут быть плоскими или V-образными (в этом еще одно отличие – раньше все конденсаторы были плоскими). Ключевой особенностью V-образных конденсаторов является значительно меньшая занимаемая площадь, что позволяет существенно экономить место. Все конденсаторы имеют зимние комплекты – их четыре варианта, конкретный вариант подбирается в зависимости от мощности устройства. Зимний комплект выполнен в отдельном блоке в своем корпусе, устанавливаемом рядом с конденсатором. В таком же виде представлен и модуль фрикулинга: бокс с фреоновым насосом и жидкостным ресивером (с подогревом). Этот блок ставится рядом с плоским конденсатором. В случае V-образного кон-

денсатора блок можно установить на его раму.

Конденсаторы, зимние комплекты и модули фрикулинга одинаковы для внутрирядных и периметральных кондиционеров. Все унифицировано, выпускается на одном заводе (ранее это было не так). Унифицированы и, конечно, русифицированы дисплеи для всех кондиционеров.

Жестко прописанных конфигураций для кондиционеров нет, все наполнение – на этапе размещения заказа. Заказчик может выбрать необходимый ему вариант увлажнителя, нагревателя, конденсатора, сетевой карты для управления (SNMP, RS-485) и пр. – как в хорошем конструкторе.

Для периметральных кондиционеров возможен выбор опции воздухораспределения (с нижней, верхней, фронтальной раздачей, с фронтальным забором и пр.), вариативность высокая, причем без дополнительных затрат. Можно выбрать и цвет (раньше окрашивание в нестандартные цвета было очень непростой задачей). По умолчанию внутрирядные кондиционеры – черные, периметральные – белые.

Еще у нас есть внутростоечные кондиционеры. Три модели – на 3, 7 и 12 кВт. Это фреоновая сплит-система, внутренний блок которой устанавливается в нижнюю часть полностью изолированной стойки. Такой блок занимает от 5 до 10 юнитов.

**– А холодильные машины, чиллеры?**

– В октябре 2023 г. представили моноблочные чиллеры (CoolFlow) воздушного охлаждения с фрикулингом. Здесь две продуктовые линейки: на базе спиральных (30–500 кВт) и винтовых компрессоров (от 300 кВт до 1,5 МВт, возможен выпуск и более мощных машин).

Все кондиционеры и чиллеры уже выставлены в нашем демозале в Москве в «Технополисе». Пожалуйста, приезжайте, изучайте, тестируйте.

**– Российские ЦОДы привыкли к высокому качеству комплектующих (насосы, вентиляторы, автоматика) мировых брендов, таких как Ebm-papst, Ziehl Abegg, Copeland, Danfoss, Siemens и пр. Что «под капотом» у ваших решений?**

– Если говорить о кондиционерах, то все установленные в них вентиляторы – электронно-коммутируемые (ЕС). Компрессоры во внутрирядных стоят инверторные, а в периметральных – по выбору: инверторные или с фиксированной частотой вращения.

Что касается производителей комплектующих, то здесь есть два варианта. Первый – установка по умолчанию.

Второй – на выбор заказчика. В этом случае цена может быть выше. Да, в предлагаемых нами решениях используются компрессоры, вентиляторы и контроллеры названных вами мировых брендов. Они же, естественно, присутствуют в ЗИПе, который заказчик может заказать вместе с оборудованием или получить отдельно с нашего склада в России. На складе будут храниться и наиболее востребованные модели оборудования.

**– Каковы сроки производства и поставки оборудования?**

– Срок изготовления заказных моделей кондиционеров – семь недель. На доставку до заказчика уходит четыре-шесть недель. Производство чиллеров занимает меньше времени: от четырех до шести недель. Логистика такая же.

**– Сегодня Systeme Electric предлагает классику охлаждения. Что вы думаете о модных технологиях: адиабатике, холодных стенах, жидкостном охлаждении?**

– Наш опыт говорит о том, что в силу разных причин – от качества воды до особенностей климата – обычные чиллеры с фрикулингом пока предпочтительнее адиабатических систем. Допустимые температуры в ЦОДах поднялись, и диапазон работы чиллеров в режиме фрикулинга сильно расширился, что повысило энергоэффективность этого варианта. Хотя я не исключаю, что мы предложим рынку и адиабатические системы. Но это дело завтрашнего дня.

Холодные стены – это, скорее, дань моде. Последние три года запросов было много (Schneider Electric даже создала отдельную производственную линию для выпуска данного нестандартного оборудования), но реализованных проектов сравнительно мало. Сейчас и запросов стало гораздо меньше. Думаю, лучше перспективы не у холодных стен с LSV, а просто у блоков на охлажденной воде большой мощности с фронтальным выдувом, которые обычно устанавливают в техническом коридоре.

Жидкостное охлаждение нужно для стоек с очень высокой нагрузкой. А львиная доля запросов сегодня приходит на стойки 7–10 кВт. Примерно 15–20% заказчиков запрашивают охлаждение для стоек до 20 кВт, на более мощные стойки запросов почти нет. Наши внутрирядники прекрасно справляются с нагрузкой до 25–30 кВт на стойку, и о жидкостном охлаждении пока речь не идет.

Чтобы жидкостное охлаждение «взлетело», нужно выработать отраслевой стандарт. Сейчас слишком много разных и несовместимых вариантов. Кроме того, важна позиция вендоров, производящих серверы. Пока все на уровне «оценки перспектив».

**– Давайте вернемся на землю. Какие сервисы, связанные с охлаждением ЦОДов, вы предлагаете? И обслуживаете ли оборудование Schneider Electric?**

– Главное, мы полностью сохранили команду инженеров и мощный набор сервисов. Это работы по обследованию объектов, моделированию воздушных потоков, пусконаладке оборудования, его регулярному обслуживанию, по сервисным контрактам. Наши SLA предполагают быстрый выезд на объект, оперативную замену оборудования. Если наш инженер присутствует в конкретном городе, то время реакции – 4 ч. Обеспечиваем и удаленный мониторинг. Наши инженеры прошли полный цикл обучения по новым

кондиционерам. Более того, уже есть опыт по монтажу и наладке. В ближайшее время подобный опыт будет получен и по новым чиллерам.

У нас есть собственный конфигуратор, программа подбора. То есть мы не просто предлагаем кондиционеры той или иной номинальной холодопроизводительности, а можем рассчитать характеристики для любых условий: температур наружного воздуха, воздуха на входе в кондиционер и пр. В ближайшее время эта программа будет доступна нашим сертифицированным партнерам.

Что касается сервиса Schneider Electric, наша компания – единственный авторизованный поставщик таких услуг для уже работающего оборудования в России и Беларуси. При этом у Systeme Electric есть компетенции и по технике других вендоров, в частности, мы обслуживаем компрессоры Turbocor.

**– Насколько заказчики могут быть уверены, что реальные характеристики при эксплуатации на объекте будут соответствовать заявленным?**

– Мы долго выбирали партнеров по производству оборудования. Тщательно проверяли технику, системы контроля качества. И уверены в тех, кого выбрали.

Так, на заводе по производству чиллеров, с которым мы активно взаимодействуем на постоянной основе, есть большая сертифицированная лаборатория. В ней можно испытывать оборудование на холодопроизводительность не только при высокой температуре, но и при температуре около 0°C, т.е. тестировать в режиме полного фрикулинга. Можно проводить FAT-тесты, если заказчик хочет посмотреть, как его чиллер будет вести себя под нагрузкой. Причем за тестом можно наблюдать удаленно.

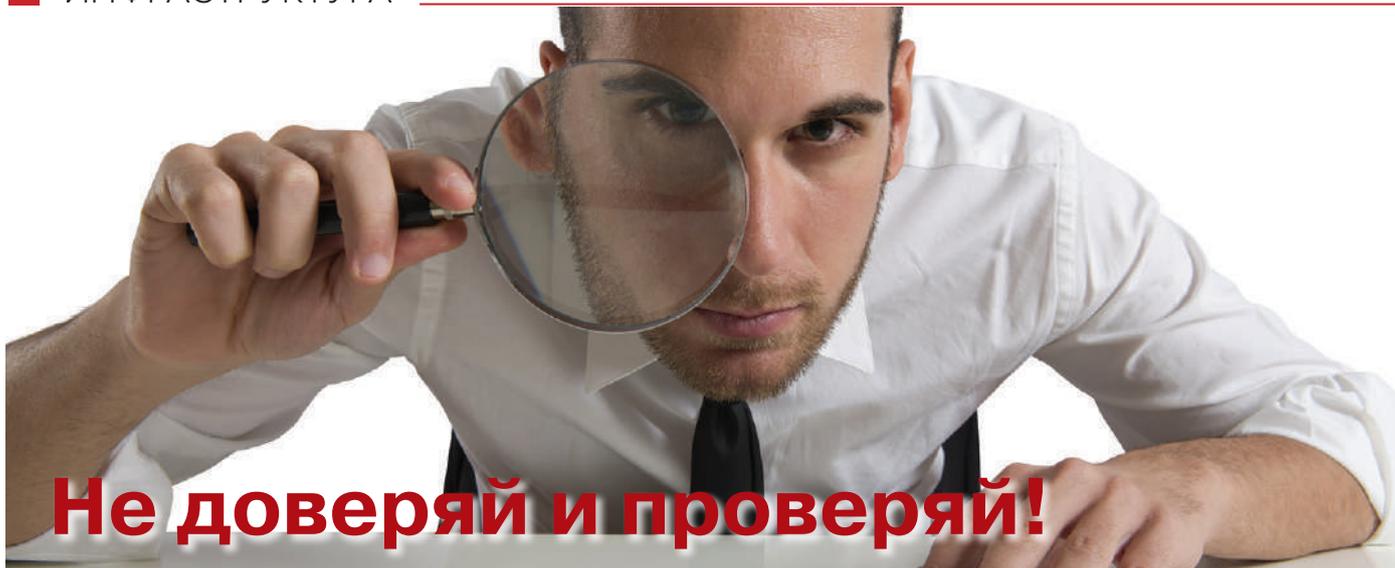
В московском демоцентре мы тщательно протестировали наши кондиционеры. И они полностью подтвердили свои характеристики. Более того, на тех площадках, где кондиционеры уже эксплуатируются, все нормально, все характеристики соответствуют заявленным, жалоб нет.

Скажу и о том, что наша стандартная годовая гарантия может быть сразу расширена до трех лет без необходимости заключения дополнительных контрактов.

**– Каковы ваши ближайшие планы?**

– На следующий год намечен выпуск сплит-систем потолочного исполнения. Такие системы устанавливаются под потолком, а потому будут востребованы на объектах, где в помещении нет свободного места на полу. Кроме того, в начале следующего года представим чиллеры с водяным охлаждением. Это будут агрегаты мощностью от 30 кВт до 2,5 МВт.

Как показало исследование «Карта вендоров», проведенное iKS-Consulting, Systeme Electric – уже в числе лидеров рынка систем охлаждения. Через год, уверен, мы укрепим эти позиции и по числу инсталляций. Полная линейка качественных продуктов, опытная команда, высокий уровень техподдержки – все, что нужно заказчикам, у нас есть.



## Не доверяй и проверяй!

Александр Барсков

**Исследование «Карта вендоров», представленное iKS-Consulting, показало серьезное продвижение китайских поставщиков на российском рынке климатического оборудования для ЦОДов. Укрепляют свои позиции и отечественные производители. Но качество продукции тех и других пока нуждается в проверке.**

### Китайское – с европейской «начинкой»

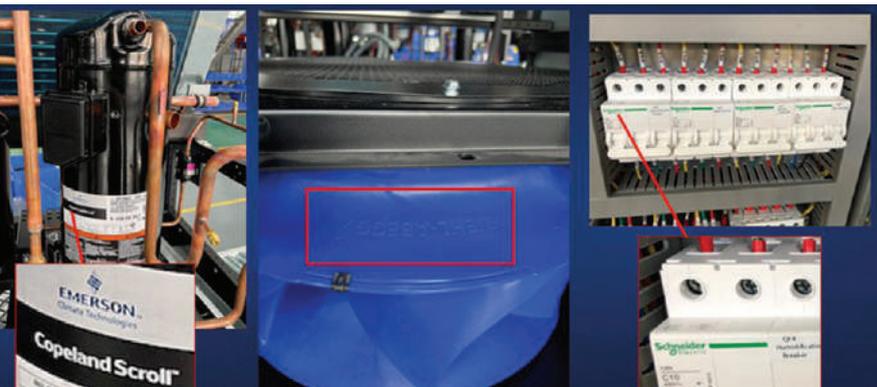
Форум «ЦОД», организованный «ИКС-Медиа», выявил рост интереса российских заказчиков к китайской климатической технике в качестве замены оборудования ушедших из России европейских производителей. Видимо, во многом это обусловлено тем, что китайские вендоры строят свои агрегаты на тех же самых европейских комплектующих, к которым привыкли российские заказчики и которые стали им (равно как и отечественным производителям) недоступны. Это, например, ЕС-вентиляторы Ebm-papst и Ziehl Abegg, компрессоры Copeland и Danfoss, контроллеры Carel, автоматика Siemens и пр.

Китайские вендоры не только поставляют в России само оборудование с европейской «начинкой», но и завозят к каждому агрегату ЗИП, в состав которого входят дефицитные комплектующие. При этом в Китае немало местных про-

изводителей комплектующих, однако ведущие поставщики климатических систем ориентируются именно на продукты мировых брендов. Константин Григорьев, технический директор компании «БРИЗ – Климатические системы», объясняет это тем, что китайские компании работают не только на внутренний рынок, и в других странах эти бренды хорошо знают, чего нельзя сказать о локальных китайских производителях. Кроме того, во всем мире есть специалисты, хорошо знакомые, например, с вентиляторами Ebm-papst, Ziehl Abegg или с компрессорами Danfoss. Владимир Шепелев, управляющий директор зарубежного отдела компании Envicool, добавляет, что китайские производители могут использовать и местные комплектующие, но для таких ответственных заказчиков, как ЦОДы, стараются этого не делать.

Ведущие поставщики климатического оборудования из Поднебесной, такие как Envicool,

В климатической технике для ЦОДов китайские производители предпочитают использовать европейские комплектующие ▼



Источник: «БРИЗ – Климатические системы»



▲ В сборочном цехе компании TICA

TICA, Airsys, предлагают полный «джентльменский набор» решений для ЦОДов: внутрирядные и шкафные кондиционеры (на воде и фреоне), а также различные чиллеры – это наиболее востребованные на российском рынке продукты. Но ими ассортимент продукции не ограничивается. Так, на конференции «ЦОД» Тимур Шабаев, руководитель отдела проектных продаж компании Engineering Solutions (российский партнер TICA), подробно рассказал о выпускаемых TICA холодных стенах и системах непрямого испарительного охлаждения.

Еще более широкий ассортимент решений представила компания Envicool, которая уже поставила в Россию более 10 тыс. единиц своей продукции. Помимо кондиционеров, чиллеров, холодных стен и систем испарительного охлаждения, она также готова предложить и пока не очень популярные в России системы прямого фреонулинга, и решения с жидкостным охлаждением. Причем, как сообщил В. Шепелев, компания производит даже теплообменники для конкретных серверов, поэтому может поставлять системы жидкостного охлаждения под ключ. В Китае уже много заказов на такие решения. Возможно, что и в России с учетом интереса к высоконагруженным стойкам, например для систем искусственного интеллекта, следует ожидать подобного.

Китайская Airsys также производит полный набор кондиционеров и чиллеры, причем, по словам Виктора Шишигина, коммерческого директора этой компании в России, 80% всех поставок идет в ЦОДы и ИТ-комплексы. Однако на форуме «ЦОД» компания решила представить свои «зеленые» технологии в виде модульной холодной стены с устройствами подачи воздуха MaxAir<sup>3</sup>. Стена строится из модулей, которые могут быть развернуты горизонтально или вертикально, чтобы адаптироваться к размеру помещения в соответствии с конкретным проектом и условиями на объекте. MaxAir<sup>3</sup> работает в составе комплексного решения PowerOne, в которое также входят чиллеры, сухие охладители и системы водопровода. По утверждению В. Шишигина, используя PowerOne, можно в любой точке мира построить ЦОД со значением PUE менее 1,2.

Компания «БРИЗ – Климатические системы», предлагающая решения под брендом ROYAL Clima, в качестве китайского партнера выбрала компанию Coolnet. По словам К. Григорьева, объездив восемь производственных площадок, российские специалисты сделали выбор в пользу именно Coolnet в частности потому, что это завод полного цикла, который «не подстраивается под поставщиков». Этот вендор предлагает полный набор прецизионных кондиционеров,

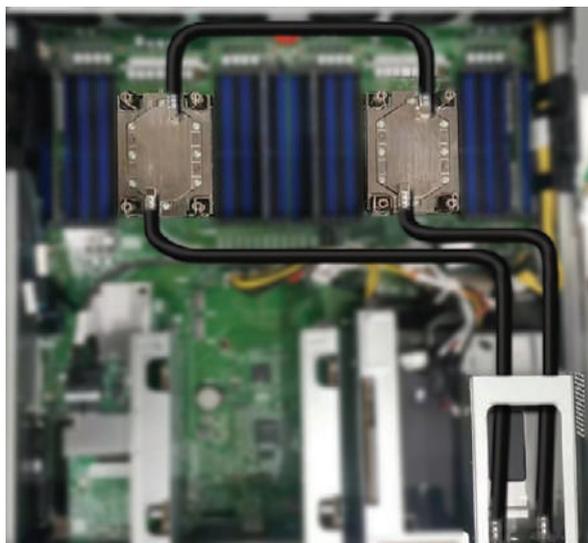
в том числе с фреоновым фрикулингом. А вот для того, чтобы обеспечить потребности заказчиков в чиллерах, «БРИЗ – Климатические системы» начала сотрудничать с турецким производителем Eгасо.

Китайские производители и их партнеры особое внимание уделили представлению современных комплексов для тестирования изготавливаемого оборудования и тщательной проверки как отдельных компонентов, так и выпускаемых систем. Но при всех плюсах китайской техники работа с вендорами из Поднебесной в сегодняшних геополитических условиях, конечно, более рискованна, чем сотрудничество со своими, российскими производителями. А что предлагают они?

### Российское – на новых компонентах

На непростую стезю производства систем охлаждения для ЦОДов (непростую в том числе потому, что ЦОДы – очень требовательные заказчики) российские компании встали разными путями. Одни (например, «Рефкул» и «КБ Борей») изначально ориентировались на этот рынок, вторые, имея большой опыт работы в области холодильного оборудования для других областей (NED, «Технофрост» и т.д.), вышли на него недавно, третьи – дополнили климатическими системами свои продуктовые портфели для обеспечения их комплексности (C3 Solutions, EMILINK) и/или благодаря хорошей «наследственности» (Systeme Electric). Кто-то оказался вынужден это сделать.

К последним относится компания HTS. Традиционно представлявшая оборудование Stulz в России, компания с уходом этого производителя оказалась в непростой ситуации, которая усугублялась тем, что многие заказчики уже заложили в свои проекты оборудование Stulz и им требовались полные аналоги – по габаритам, хо-



◀ В жидкостных системах охлаждения небольшие теплообменники устанавливаются непосредственно на платах серверов

Источник: Envicool



▲ На производстве оборудования NED

лодопроизводительности и другим характеристикам. HTS смогла реализовать импортозамещение оборудования Stulz в России, совместно с заводом «Рефкул» разработав и наладив выпуск сразу нескольких моделей кондиционеров, включая моноблочные кондиционеры внутреннего и внешнего исполнения. И это, как подчеркивает Ирина Арепина, заместитель генерального директора HTS, полноценное российское производство кондиционеров.

А вот компания NED на рынке вентиляции и кондиционирования работает уже более 25 лет и, как утверждает ее директор по маркетингу Ольга Ковальчук, может удовлетворить «все потребности в климатической технике на объекте». Согласно исследованиям Litvinchuk Marketing Agency, компания является лидером в России по выпуску (в штуках) центральных кондиционеров и чиллеров. Примечательно, что на рынок ЦОДов она вышла не просто с климатическими агрегатами (чиллерами, шкафными и внутрирядными кондиционерами, холодными стенами), а с полноценными решениями, которые включают оборудование для размещения серверов и изоляции коридоров. Это оборудование производится партнером NED – белго-

родской компанией Spectrum. Если учесть еще наличие в портфеле продуктов Spectrum модульных ИБП (до 800 кВА) и стоек распределения питания, то получается, что партнеры охватывают почти все основные инженерные системы для ЦОДов. Очень перспективный игрок на этом рынке.

Еще один производитель с большим опытом в области промышленного холодильного оборудования, который начал работу на рынке оборудования для ЦОДов, – компания «Технофrost». Как рассказал ее технический директор Александр Будкевич, в 2022 г., несмотря на все сложности, связанные с дефицитом комплектующих, «Технофrost» смог разработать решения для ЦОДов: чиллеры, прецизионные кондиционеры на заходящей воде и холодные стены. (Помог большой склад компонентов, который позволил продержаться более полугод, пока искали замену европейским комплектующим.) Первым заказчиком цодовского оборудования «Технофrost» стала компания PNC group – более 70 чиллеров и почти 250 кондиционеров были точно в срок поставлены на площадку девелопера в Медведково.

Текущие мощности завода позволяют наряду с основным холодильным оборудованием изготавливать для рынка ЦОДов до 20 чиллеров (мощностью 500–700 кВт) и до 50 прецизионных кондиционеров (100–200 кВт) в месяц. Сейчас строится новый производственный корпус, благодаря которому предприятие планирует в 2024 г. более чем в два раза увеличить выпуск этой продукции. Параллельно возводится лабораторный корпус, где можно будет проводить комплексные испытания чиллеров и кондиционеров.

Следует отметить, что российские производители не обходят вниманием и инновационные

Чиллеры для ЦОДов производства «Технофrost» ▼



энергoeffективные решения. К ним относится представленная компанией Antarcctis система адiabатического косвенного охлаждения на основе композитного трубчатого теплообменника (подробнее об этой системе – в статье «Охлаждение для ЦОДа: обойдемся без компрессоров?», «ИКС» № 3'2022, с. 30).

### Прорыв года – в сознании заказчиков

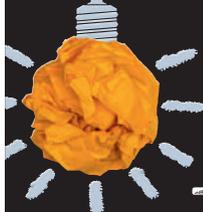
С появлением множества новых вендоров, часть из которых не имеют большого опыта работы на рынке ЦОДов, чаще стали возникать различные нестыковки и проблемы. Примерами поделилась И. Арепина из HTS. Нередко поставщики, обещая, что «все будет как в ТЗ», опускают ряд технических нюансов, которые проявляются уже в процессе строительства ЦОДа. Так, в одном из проектов компания-поставщик на этапе тендера умолчала о том, что блок АВР не помещается в корпус кондиционера. То, что его надо разместить на отдельном щите, выяснилось при монтаже – со всеми вытекающими дополнительными затратами и неудобствами.

Другой пример. Заказчику потребовался чиллер, способный работать при  $-40^{\circ}\text{C}$ . Ему предложили такое решение, но даже в характеристиках его комплектующих нижняя граница допустимой температуры составляла лишь  $-20^{\circ}\text{C}$ . Как предупреждает И. Арепина, если хоть один компонент рассчитан только до  $-20$ , значит, и весь агрегат – до  $-20$ . Чтобы чиллер нормально работал при  $-40^{\circ}\text{C}$ , все его компоненты должны быть рассчитаны на работу при этой температуре. «Мы живем в холодной стране, – продолжает она. – Поэтому даже оборудование Stulz мы поставляли не с заводскими, а с собственными низкотемпературными комплектами».

Прорывом года В. Шепелев из Envicoool считает кардинальные изменения в сознании заказчиков и интеграторов. «Раньше мировым брендам, таким как Vertiv, Stulz и другие, верили на слово, и заявленные характеристики не надо было проверять. Сейчас ситуация изменилась. Заказчик стал тщательно проверять решения. Анализировать, те ли характеристики ему предлагают, та ли температура на входе, почему расход воздуха такой маленький, достаточно ли его и т.п.»

«Выполнение таких привычных операций, как закупка запчастей и поддержание оборудования в рабочем состоянии, сегодня может потребовать много смекалки, связей и воображения. Важно понимать, где можно использовать аналог, а где обязательно нужно раздобыть оригинал», – характеризует текущий момент И. Арепина из HTS.

Сегодня надо тщательно все тестировать. Задавать поставщикам «миллион» вопросов, оговаривать все нюансы и проверять, проверять и проверять. Время нынче такое. **ИКС**



## Тренинговый центр АНО КС ЦОД

Открой новое пространство знаний о ЦОДах!

### Расписание программ на 2023/24 гг.

#### ЭКСПЛУАТАЦИЯ ЦОД

11-13 декабря 2023, Москва /  
24-26 июня 2024, Москва / 11-13 декабря 2024, Москва

#### ЭЛЕКТРИЧЕСКИЕ И МЕХАНИЧЕСКИЕ СИСТЕМЫ ЦОД

26-29 марта 2024, Москва

#### ПОСТРОЕНИЕ ЦОД

18-19 апреля 2024, Москва / 9-10 октября 2024, Алматы

#### ТЕЛЕКОММУНИКАЦИИ И СЕТИ В ЦОД

29-31 мая 2024, Москва

#### УПРАВЛЕНИЕ ПРОЕКТИРОВАНИЕМ И СТРОИТЕЛЬСТВОМ ЦОД

18-20 ноября 2024, Москва



Спецусловия при прохождении онлайн-курсов  
Подробнее уточняйте по email: [info@ano-dcc.ru](mailto:info@ano-dcc.ru)

[ano-dcc.ru](http://ano-dcc.ru)

Преподаватели курсов – эксперты отрасли ЦОДов, обладающие многолетним практическим опытом, за плечами которых создание и эксплуатация крупнейших российских объектов.

Описание и регистрация  
[ano-dcc.ru/study/](http://ano-dcc.ru/study/)



# NED: конструктор систем охлаждения для ЦОДов

**NED, компания с 25-летним опытом в области климатического оборудования, начала активно работать на рынке ЦОДов. О ее экспертизе, продукции и сервисах – Владимир Халфин, заместитель генерального директора ООО «НED-Центр».**



– **NED – относительно новое имя на российском рынке цодостроения. Представьте, пожалуйста, компанию.**

– Наша компания существует более 25 лет и за это время из небольшого продавца иностранного оборудования превратилась в крупнейшего в России производителя систем вентиляции и кондиционирования воздуха. Для решения задач вентиляции и холодоснабжения мы производим все – от небольших вентиляторов до огромных холодильных машин, от простейших блоков автоматики до серьезных систем диспетчеризации объектов. Мы можем оснастить инженерными системами любое здание любой сложности – от маленького детского сада до огромного стадиона.

В компании работает свыше 2000 сотрудников. Производство развернуто на двух заводах: в подмосковном Дзержинском и в Белгороде. У нас большое конструкторское бюро, примерно 150 человек. Все, что мы выпускаем, – это наши разработки.

В прошлом году оборот компании составил около 12 млрд руб. В этом году планируем выйти на уровень 20 млрд руб. Среди наших клиентов – представители самых разных отраслей народного хозяйства: промышленные предприятия, медицинские, спортивные, образовательные организации и т.д.

Компания имеет представительства по всей территории РФ – от Санкт-Петербурга до Южно-Сахалинска. Также есть офисы в Казахстане и Узбекистане. Стараемся быть ближе к клиентам, не только поставляя оборудование, но и предоставляя услуги проектирования, пусконаладки, сервисного обслуживания.

– **Сегодня остро стоит проблема, связанная с импортными комплектующими. Как вы ее решаете?**

– Когда стало понятно, что элементная база из Европы будет для нас по большей части недоступна, мы были готовы к такому развитию событий. Например, наш завод в Белгороде освоил производство вентиляторов и рабочих колес. А теплообменники уже много лет производим сами. Безусловно, часть комплектующих, в том числе электромоторы для тех же вентиляторов, мы закупает за границей, но по многим позициям локализация производства достигает 90%.

Наиболее сложная ситуация сложилась с компрессорами, поскольку традиционно мы ориентировались на продукты Danfoss. Когда этот производитель перестал поставлять свои изделия в Россию, пришлось переделывать всю конструкторскую документацию под те компрессоры, которые мы были в состоянии ввезти. Однако к новой ситуации адаптировались довольно быстро.

У нас хорошие связи с азиатскими странами. Например, в Китае у нас свой офис, логистика налажена.

– **Как и когда вы вышли на рынок оборудования для ЦОДов?**

– На рынке оборудования для ЦОДов мы присутствуем примерно четыре-пять лет. Началось с того, что наши клиенты, столкнувшись с ограничением поставок со стороны западных партнеров, попросили разработать внутрирядные кондиционеры. Для нас это оказалось относительно несложно, поскольку к тому времени мы уже освоили выпуск прецизионных кондиционеров и технологии были отлажены.

Сегодня поставляем для ЦОДов различные виды внутрирядных и шкафных кондиционеров. На базе широкой линейки наших чиллеров делаем серьезные холодильные центры, причем сами их и проектируем. Научились производить и интегрировать в ЦОДы крупные вентиляторные стены, в том числе с охлаждением. По всем этим продуктам наработана серьезная экспертиза.

– **Какое в целом впечатление производит на вас отрасль ЦОДов?**

– То, как развивается отрасль, вселяет оптимизм. Мы рассчитываем, что наша продукция займет на рынке оборудования для ЦОДов достойное место. Нравятся люди, которые работают в этой сфере. Приятно и интересно общаться с компетентными специалистами, которые уверены в себе и знают, как все надо делать. Я подметил, что технический директор практически любого ЦОДа уверен, что именно его техническое решение самое лучшее, готов косяками лечь, чтобы это доказать. Пока мы в дискуссии не вступаем, работаем по полученным техническим заданиям. И стараемся создать набор элементов, из которых, как из конструктора Lego, наши заказчики смогут построить нужную им систему.

В ЦОДах используются различные технические решения. Одним дата-центрам требуются внутрирядные кондиционеры с изоляцией коридоров в машзале, другим – охлаждаемые вентиляторные стены, третьим – большие вентиляторные установки. Изучая запросы наших клиентов, мы понимаем, что можем все это изготовить и стать производителем, который способен удовлетворить любые потребности заказчиков из отрасли ЦОДов.

Наращиваем компетенции, набираем специалистов и, уверен, постепенно, шаг за шагом станем незаменимыми партнерами для большинства ЦОДов. И сможем не только работать по ТЗ, но и сами разрабатывать решения для дата-центров.



– Если не ошибаюсь, NED расшифровывается как **New Engineering Discoveries**, новые инженерные открытия. Какие инновации вы используете?

– В области классической вентиляции и холодоснабжения уже все изобрели, и мы, по сути, «тасуем» существующие технические решения, оптимизируем их, в том числе с подбором оборудования, которое может быть поставлено клиенту в данный момент.

Для нас инновационная деятельность состоит в том, чтобы развивать наше производство: совершенствовать процессы, обновлять оборудование, обучать персонал, искать квалифицированные конструкторские кадры. Стараемся оснастить наши производственные площадки самыми современными станками, роботами, которые позволяли бы изготовить все, что нужно для климатических систем ЦОДов.

В ЦОДах тоже много инноваций, и это еще одна причина, почему эта отрасль столь привлекательна. Встречаясь с одними и теми же заказчиками через короткий промежуток времени, понимаешь, что необходимые им решения развиваются. И нам важно поспеть за этими изменениями.

Вместе с тем то, что некоторые ЦОДы считают инновациями, нам хорошо знакомо. Например, адиабатика. В охлаждении и вентиляции адиабатические системы применяются давно. Мы плотно ими занимаемся, умеем их рассчитывать и изготавливать. И у заказчиков, использующих наши решения, в том числе в ЦОДах, существенно снижается энергопотребление.

– На форуме «ЦОД» вы представили комплексное решение, включающее также серверные шкафы, системы изоляции коридоров и ИБП.

– Да, эти решения предлагает наш партнер, компания Spectrum. У нее большой опыт проектирования, строительства и эксплуатации ЦОДов. Ее производство тоже расположено в Белгороде, и ее продукция в высокой степени интегрирована с нашими системами.

Общая эффективность системы холодоснабжения напрямую связана с организацией машзала: как изолированы воздушные коридоры, исключены ли утечки холодного воздуха и пр. Поэтому системы размещения ИТ-оборудования и изоляции коридоров очень важны для нас и, конечно, для заказчиков.

– Для ЦОДов еще важно качество сервисного обслуживания: быстрота реакции, оперативность ремонта/

замены и пр. Как у вас выстроена система сервисной поддержки?

– У нас большая собственная сервисная служба, укомплектованная высокопрофессиональными специалистами. Мы периодически сталкиваемся с некачественной пусконаладкой своего оборудования, поэтому в момент его монтажа и запуска в эксплуатацию наши специалисты часто выезжают на объекты. Кроме того, наши бригады могут сами провести пусконаладочные работы, тем самым экономя клиентам время и деньги.

Во всех городах-миллионниках, и не только миллионниках, у нас есть или свои сервисные инженеры, или специализированные компании, которые сертифицированы нами и могут предоставить квалифицированный сервис. Поэтому время реакции минимально. Если речь идет об оборудовании, установленном в обычном здании, то наш специалист приедет в течение 24 ч. На объекты, которые должны функционировать в режиме 24/7, – гораздо быстрее. Для самых критичных объектов рекомендуем размещать ЗИП на самом объекте, обучаем персонал заказчика, чтобы он мог максимально оперативно заменить проблемные компоненты, – а потом уже разбираемся, что произошло. Наше преимущество перед зарубежными компаниями в том, что компоненты для всех изделий мы держим на складе. А дальше – логистика, доставка самолетом, поездом, машиной.

Также отмечу, что стандартная гарантия на наши продукты – три года, расширенная – пять лет. Если необходимо, даем и большую гарантию.

– Каковы планы компании на рынке инженерной инфраструктуры ЦОДов?

– Как я уже говорил, стратегия – предложить заказчику некий конструктор, из которого он мог бы собрать любую необходимую ему систему, будь то классические фреоновая или чиллерная система с внутрирядными или шкафными кондиционерами, холодная стена, система с адиабатикой, жидкостное охлаждение или любое другое перспективное решение. Причем весь продуктовый портфель для таких решений будет на 100% сделан в России. Когда выполним эту задачу, точно займем лидирующие позиции на рынке климатического оборудования для ЦОДов.

# Не все DCIM-системы одинаково хороши

**Евгений Кривоносов**, генеральный директор, «СДИ Софт»;  
**Оливер Линднер**, директор бизнес-юнита по ЦОД, FNT Software

**Эффективное управление инфраструктурой ЦОДа на фоне сокращения финансирования, ограниченности выбора решений из-за санкций, с одной стороны, и быстрого развития облачных технологий, с другой стороны, – задача нетривиальная. Чтобы с ней справиться, требуются комплексные перспективные системы.**

ЦОДы зачастую являются элементом гибридных экосистем, включающих в себя физические и виртуальные ресурсы, которые расположены частично на собственных площадках предприятий, а частично – в облаке. У гибридной инфраструктуры по сравнению с традиционной возможности шире, но из-за большего числа задействованных технологий, поставщиков услуг, мест размещения оборудования, планов тарификации и взаимозависимостей между отдельными элементами инфраструктуры управлять ею на порядок сложнее.

Традиционные системы управления инфраструктурой ЦОДов (Data Center Infrastructure Management, DCIM) все больше приближаются к пределу своих возможностей. При этом, несмотря на распространенное мнение, что все DCIM-системы более или менее одинаковы, между ними существуют фундаментальные различия: одни развились из систем учета кабельной инфраструктуры и серверов, другие – из систем управления зданием. В результате у представителей каждого из направлений своя специализация и свои индивидуальные особенности.

## Новые требования к ИТ

В перспективе программное обеспечение должно будет поддерживать ключевые процессы, возможность обмена данными в масштабах предприятия и гибкой интеграции в так называемые цепочки создания ценности. Учет энергопотребления, охлаждения и площади – безусловно значимые функции, но предоставляемые услуги не менее важны. Поэтому DCIM-решение должно охватывать все уровни ИТ-ресурсов ЦОДа. Компаниям, вставшим на путь цифровизации, нецелесообразно и дальше использовать ПО, которое не сможет поддержать такой переход. Им необходимо решение, которое поможет реализовать намеченные изменения и справиться с будущими задачами.

Все больше компаний отказываются от использования собственного (корпоративного) ЦОДа, и эта тенденция определяет направление развития современных DCIM-систем. Если вы переносите свои серверы и сети к поставщику услуг colocation, то уже не вы, а он следит за надлежащим функционированием соответствующего оборудования. А вы при наличии перспективного DCIM-решения можете уделить больше внимания увеличению добавленной стоимости своих услуг. При переходе к распределенной среде невозможно управлять процессами ее функционирования при помощи DCIM-решения, ориентированного на классическую модель ЦОДа.

Эта тенденция имеет и финансовую сторону. Возможности экономии за счет аппаратных и физических аспектов себя исчерпали. Дальнейшее ощутимое сокращение издержек может быть достигнуто только в результате комплексной оптимизации, в том числе на виртуальном и прикладном уровнях. Только гибридная DCIM-система даст прозрачную картину всей инфраструктуры и позволит управлять всем массивом данных о ней из одного места, что приведет к повышению их доступности и качества.

Такая система, поскольку она обеспечивает наличие всех необходимых данных, их достоверность, актуальность и согласованность, позволяет быстро анализировать нужные параметры. Специалисты и руководство, имея под рукой прямой доступ к необходимой информации (например, о договорах обслуживания), могут принимать более грамотные решения. Кроме того, все удаленные ИТ-подразделения через доступ к единому источнику достоверных и актуальных данных связываются в единую согласованную сеть. Все это позволит перейти от реагирования на случившееся событие к плановому упреждающему управлению инфраструктурой.

## Два подхода

Неоднократно приходилось видеть, что при выборе DCIM-решения заказчики с подачи консультантов «сравнивают яблоки с апельсинами», совершенно искренне не понимая этого. Они подробно изучают отдельные функциональные области, игнорируя фундаментальные различия между концепциями, лежащими в основе DCIM-инструментов.

Современные DCIM-системы, исходя из истории их развития и задач, для которых они изначально разрабатывались, стратегически можно разделить на две группы.

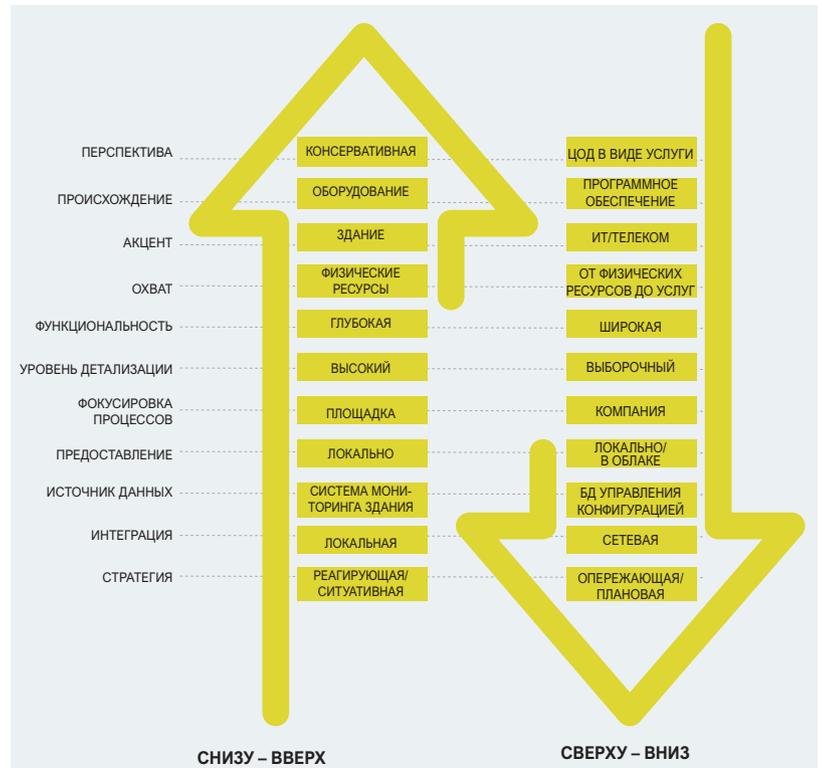
Первая группа – решения, вышедшие из систем управления зданием. Они изначально разрабатывались для управления работой систем электропитания и кондиционирования зданий. Оттуда они перешли в ИТ-сектор (так называемую белую зону) и стали использоваться для управления стоечным оборудованием. Данная группа ориентирована на работу в пределах одной площадки. В силу своей специфики в этих инструментах сильно развиты функции мониторинга и контроля. Их, как правило, устанавливали локально, и изначально они не имели сетевых функций и не предусматривали интеграцию.

Вторая группа – инструменты, которые выросли из управления серверами и кабелями и развились в комплексные решения для управления ИТ-инфраструктурой предприятия. Со временем в них появились функции управления инженерными коммуникациями (так называемой серой зоной). Инструменты этой группы в большей степени ориентированы на мониторинг объектов компании в целом и в меньшей – каждого отдельного ЦОДа. Они обладают огромными функциональными возможностями с точки зрения комплексных стандартизированных процессов. При этом в некоторых областях они несколько уступают инструментам первой группы: функции управления системами кондиционирования, например, у них не настолько детализованы, поскольку с самого начала они были ориентированы на интеграцию и сетевое взаимодействие.

Решения первой группы можно отнести к модели развития, которую условно назовем «снизу – вверх» (от управления инженерными системами к управлению ИТ-инфраструктурой), а второй группы – к модели развития «сверху – вниз» (добавление необходимой функциональности).

## Что выбрать?

Ценность ИТ для компании зависит от качества управления ЦОДом. Ценность ИТ-серви-



сов также обусловлена тем, насколько грамотно осуществляется управление ими. При этом эффективно управлять и ЦОДом, и ИТ-сервисами с помощью одного и того же инструмента невозможно.

Проблема выбора DCIM-решения связана с тем, что пользователи составляют обширный список необходимых функций, но не сообщают, какие задачи предполагается решать: одно дело – управлять инфраструктурой отдельного ЦОДа, а другое – инфраструктурой всех объектов предприятия.

При выборе также необходимо учитывать планы на будущее. Вопрос приобретения DCIM-решения, как правило, встает в контексте строительства нового ЦОДа. Соответственно требования к решению формулируются только для этого конкретного объекта. В результате внедряется система, которая оказывается негодной, когда через некоторое время возникает необходимость управлять всеми ЦОДами компании и другой важной ее ИТ-инфраструктурой. Кроме того, бывают ситуации, когда компания арендует оборудование у поставщика услуг colocation, а также создает собственную периферийную инфраструктуру на своих площадках. При выборе решения только для одного ЦОДа желательно учитывать и такие перспективные сценарии. Бэкграунд систем определяет фундаментальные различия в их применимости, которые не очевидны при простом сравнении функций.

▲ Сравнение моделей развития «снизу – вверх» и «сверху – вниз»

## Что отличает перспективное DCIM-решение

Помимо традиционных задач, связанных с электропитанием, охлаждением и использованием площадей, операторам ЦОДов сегодня зачастую приходится решать вопросы пропускной способности, выбора и внедрения аппаратных платформ, облачных решений и систем виртуализации, а также организации программно конфигурируемых сетей и сетевых фабрик. Современный ЦОД – сложная экосистема, для управления которой требуется инструмент, сочетающий в себе возможности автоматизации, планирования, эффективного управления сложными процессами и позволяющий получить как полную детализированную картину ситуации в целом, так и информацию об отдельных параметрах и элементах.

Для успешной эксплуатации ЦОДа необходимо иметь систему учета, дающую исчерпывающую информацию обо всех ресурсах и взаимосвязях между ними. Какой же должна быть такая система?

**Полнота данных.** DCIM-система должна иметь центральный репозиторий для хранения данных обо всех единицах учета – от кабелей до услуг. При централизованном учете данных разных подразделений компании обеспечивается полнота и целостность учета. Для синхронизации информации и поддержания ее качества должна проводиться автоматическая проверка совместимости (достоверности).

**Тотальный охват.** DCIM-система характеризуется не только глубиной, но и шириной функциональности. Такой подход продиктован необходимостью поддерживать, помимо прочего, общекорпоративные ИТ-процессы. В традиционных системах акцент делается на управлении отдельными зданиями. Создавать перспективную DCIM-систему лучше без привязки к ка-

кой-либо системе управления зданием. Тогда она будет способна работать с разными системами такого класса, развернутыми на разных объектах, управлять облачными ресурсами и интегрировать услуги colocation.

**Стандарты из коробки.** Современное DCIM-решение должно задавать стандарты для компании и в то же время оставаться гибким там, где это необходимо. Гибкость подразумевает не полномасштабную кастомизацию, а возможность изменения атрибутов или отдельных отчетов. Например, зачастую необходимо отразить в рабочих процессах специфические для компании детали, такие как распределение заданий между разными группами сотрудников, и эффективную интеграцию с другими установленными системами.

**Перспективная технология.** За пять лет на уровне оборудования в ЦОДах поменялось не так уж много, чего не скажешь о программном обеспечении. Только недавно появились первые трехмерные изображения, а сегодня они уже данность. Сейчас активно обсуждается использование в ЦОДах приложений дополненной/виртуальной реальности. Было успешно реализовано несколько пилотных проектов, и скоро такие приложения получат повсеместное распространение. Активно развивается машинное обучение. Пока нет практических коробочных решений для пользователей-неспециалистов, но их появление – вопрос ближайших нескольких лет. Для всех современных вариантов использования DCIM-системы требуется платформа, поставляющая необходимые данные от одного или нескольких объектов. В идеале такая платформа должна поставлять данные для других приложений, например, через интерфейсы или предварительную настройку для конкретного применения.

**Масштабируемость.** DCIM-система должна не терять своей актуальности при изменениях в жизни компании (быстрый рост, слияние, объе-



Специальные условия  
при оформлении подписки  
для корпоративных  
клиентов!



Оформляйте подписку  
в редакции – по телефону: +7 (495) 150-6424  
или по e-mail: [podpiska@iksmedia.ru](mailto:podpiska@iksmedia.ru)



динение, отделение). Поэтому нужна возможность подключить новых пользователей (например, при присоединении нового объекта). Такая же ситуация с приобретением новых лицензий: нужно учитывать финансовые последствия. Если система разворачивается в масштабе всей компании, ею будет пользоваться большое количество сотрудников. А чем больше подразделений компании используют одну программу, тем выше ее ценность для бизнеса и эффективнее взаимодействие между подразделениями.

**Независимость от производителя.** DCIM-системы от производителей сетевого и ИТ-оборудования имеют существенный недостаток: они ориентированы исключительно на продукты поставщика DCIM-системы. Однако в реальной жизни ситуация, когда ИТ-среда состоит из оборудования одного изготовителя, встречается редко. Если в библиотеке оборудования системы – только собственные решения поставщика, у заказчика возникнут проблемы в случае, например, слияния. Библиотека, включающая в себя «железо» разных производителей, – обязательное требование.

**Умная интеграция.** ИТ-среда постоянно эволюционирует, поэтому крайне важно, чтобы внедрить DCIM-систему можно было легко, надежно и недорого. В этом залог успешного управления инфраструктурой ЦОДа в долгосрочной перспективе. В отличие от специализированных решений, которые статичны и могут взаимодействовать только друг с другом, интеграция дает необходимую гибкость, позволяет использовать новые возможности. Особенно если это интеграция с ИТ-системами более высокого уровня, например, системами управления услугами.

**Активная поддержка продукта.** Жизненный цикл ИТ-продуктов существенно сократился. Всего за несколько лет ультратонкий

корпус эволюционировал в блейд, потом в конвергентные системы, а теперь и они уже начинают исчезать.

Поставщикам традиционных DCIM-систем все сложнее не отставать от развития технологий. Например, система управления кабельной инфраструктурой была недавно основательно модернизирована из-за внедрения в ЦОДах каскадной технологии. DCIM-решение должно быть способно отражать эти эволюционные изменения с минимальной задержкой – наличия современного пользовательского интерфейса уже недостаточно.



#### Готовность к будущим вызовам: контрольный список

- типовое ПО с широкими возможностями настройки;
- модульная структура;
- работа локально и в облаке (ПО как услуга);
- полный учет всех активов ЦОДа;
- процесс-ориентированная поддержка;
- качественная документация;
- функции планирования;
- интеграция данных и стандартные API-интерфейсы;
- отсутствие ограничений для добавления новых функций;
- библиотека оборудования, независимая от производителей.

Спросите себя, отвечает ли ваша DCIM-система всем перечисленным требованиям. Возможно, сейчас функционала достаточно, но рано или поздно ваши потребности изменятся. Обратите внимание: быстро найти, оценить и внедрить новое комплексное DCIM-решение практически невозможно. Поэтому лучше подготовиться заранее. Залог успеха – гибкое реагирование на изменение ситуации. Доработка устаревшего ПО – сложный, медленный процесс, который чреват торможением развития. И все равно в результате такая система не будет поддерживать сервис-ориентированные функции управления. **ИКС**

# Шкафы для любого формата

**Поддержка одним изделием сразу трех форматов (19", 21" и 23"), уникальные системы световой сигнализации и гашения вибраций – ключевые характеристики шкафов SYSMATRIX EX. Об этих и других особенностях решений SYSMATRIX рассказывают основатели и руководители компании.**

**«ИКС»:** Когда и с чего начиналась история вашей компании? Что сегодня предлагает SYSMATRIX?

**Александр Тепляков:** История SYSMATRIX началась в 2013 г. с производства наших первых изделий в Китае. В том же году мы зарегистрировали два патента на профили несущей конструкции, которые по-прежнему используются при изготовлении наших шкафов серий EX и MR.

В 2016 г. торговую марку SYSMATRIX мы зарегистрировали в России. В 2017 и 2018 гг. наши продукты были включены в перечень инновационной продукции Агентства инноваций города Москвы. Это признание стало важным рубежом для нас, подтверждая, что мы движемся в правильном направлении.

В 2019 г. было принято решение о локализации производства в России. Это позволило значительно сократить сроки поставки и устранить ограничения по объему заказов. Более того, локализация дала нам возможность гибко вносить изменения в конструкцию изделий, чтобы лучше отвечать потребностям, возникающим в конкретных проектах.

**Станислав Смолев:** 2022 г. особенно значим для нас, так как мы стали финалистами престижной Национальной премии «Бренд года в России». Это признание подтверждает, что наша команда работает на высоком уровне и создает инновационные продукты, которые по достоинству оценивают наши партнеры и клиенты.

Сегодня мы выпускаем широкий ассортимент продуктов, включающий 10 серий шкафов и стоек. Особое внимание уделяем оборудованию для дата-центров и предлагаем специализированные шкафы для размещения серверного оборудования с высокой нагрузочной способностью. Решения полностью совместимы с системами изоляции воздушных коридоров ЦОДов. Кроме того, мы производим решения для зон коммутации с высокой плотностью, а также для эффективного размещения ИБП и аккумуляторных батарей.

Активно развиваем новое направление – защиту ИТ-конструкций от воздействий вибрации, толчков и сейсмической активности. Таким образом, мы готовы предоставить надежные и эффективные решения, которые обеспечивают безопасность и сохранность ИТ-оборудования даже в условиях экстремальных воздействий.

**«ИКС»:** Насколько велика ваша зависимость от импортных комплектующих?

**А.Т.:** Импортные комплектующие составляют около 1–2% общей себестоимости изделий. Их влияние на финансовую устойчивость и производственный процесс в целом минимально. Мы активно управляем этой зависимо-

стью, стремясь минимизировать

риски, связанные с импортными компонентами, находя возможности закупки у локальных поставщиков. Наша компания стремится к более независимым и устойчивым источникам комплектующих, чтобы обеспечить стабильность производства и бизнеса в целом.

**«ИКС»:** Что представляют собой R&D-мощности компании?

**С.С.:** В рамках R&D-направления мы создали отдел SYSMATRIX LAB, который стал настоящим центром инноваций. Наши штатные специалисты – всего лишь часть наших ресурсов. Для реализации масштабных проектов мы активно привлекаем экспертов, обладающих необходимыми компетенциями. Это бизнес-аналитики, технологи в области материаловедения, инженеры по техпроцессам. Наш подход заключается в том, чтобы собрать в команду лучших специалистов для достижения результатов.

Именно в подобной синергии мы находим перспективные решения, которые помогают нам реализовывать амбициозные проекты и оставаться на переднем крае развития технологий.

**«ИКС»:** Какие решения SYSMATRIX предлагает для ЦОДов? В чем их конкурентные преимущества?

**А.Т.:** Для ЦОДов мы рекомендуем высоконагружаемые шкафы серии EX. Одно из их важных преимуществ – мультистандартность: они универсальны и поддерживают все основные форматы – 19", 21" и 23". Это значит, что конструктив шкафа обеспечивает возможность сборки с любым из указанных расстояний (19", 21" и 23") между монтажными профилями.

Переход с формата 19" на 23" приводит к увеличению площади поверхности полки на целых 20%! Например, если на 19-дюймовой полке глубиной 950 мм можно разместить четыре АКБ Delta FTS 12-100 X (12 В/100 Ач), то на 23-дюймовой – уже восемь (располагая аппараты не вдоль, а поперек). Улучшить утилизацию дорогостоящей площади ЦОДов позволяет также использование модели SYSMATRIX EX высотой 52U. Отмечу и нагрузочную способность шкафа – до 2000 кг! Три пары монтажных профилей обеспечивают равномерное распределение нагрузки, а комплект «косынок» дополнительной жесткости – надежность, даже в условиях сейсмоактивности.

Наши шкафы могут поставляться с шестью типами дверей, начиная от прочных металлических и заканчивая пер-



**Александр Тепляков,**  
генеральный директор,  
SYSMATRIX



**Станислав Смолев,**  
коммерческий директор,  
SYSMATRIX

форированными. Важно, что есть варианты, которые обеспечивают эффективную вентиляцию и при этом гарантируют защиту от физического и визуального доступа. Боковые съемные панели – двух видов: глухие металлические (максимальная защита) и перфорированные (эффективная вентиляция и охлаждение оборудования). Крыши бывают также двух видов: с пылезащищенными кабельными вводами и органайзерами (IP20) и с защитой от вертикального падения воды (IP21).

Шкафы серии EX уже в базовой комплектации оборудованы активным вентиляционным модулем, включающим пять вентиляторов диаметром 120 мм с воздухопроизводительностью 750 куб. м/ч. Это позволяет эффективно удалять избыточное тепло из корпуса шкафа и поддерживать оптимальный температурный режим.

В SYSMATRIX EX хорошо продумана система организации кабельной инфраструктуры. В стандартную комплектацию включены два кабельных органайзера на крыше и два вертикальных внутри шкафа. Это способствует упорядочению кабельной инфраструктуры, улучшению внутренней вентиляции шкафа, а также упрощению монтажа и обслуживания.

По запросу мы оснащаем наши шкафы системой световой сигнализации. Это совершенно новый способ контроля температурных условий внутри серверного шкафа – интегрированная в угловые профили корпуса световая сигнализация с использованием LED-подсветки. В нормальном режиме работы светодиодная подсветка зеленого цвета указывает на оптимальные температурные условия внутри шкафа. Если температура достигает 35°C, подсветка автоматически меняется на синюю, обозначая активацию режима интенсивной вентиляции. Однако, если температура продолжает расти и достигает 45°C, подсветка становится красной, сигнализируя о необходимости вмешательства. Это служит указанием на возможные проблемы с охлаждением.

Наконец, для предотвращения влияния вибраций на серверы мы предусмотрели возможность оснащения шкафов изоляторами (системами гашения), что уменьшает физическое воздействие на установленное в них оборудование.

**«ИКС»: Сотрудничаете ли вы с поставщиками ИБП и кондиционеров, чтобы предложить заказчикам полное решение в сфере инженерной инфраструктуры? С кем конкретно?**

**С.С.:** Мы стремимся предложить своим клиентам комплексное решение в области инженерной инфраструктуры. Когда речь идет о системах бесперебойного питания, мы гордимся нашим стратегическим партнерством с компани-

ей Powercom. По данным ITResearch, это лидер российского рынка ИБП, а значит, клиенты SYSMATRIX могут быть уверены в том, что они получают решения от компании с богатым опытом и высокими стандартами качества.

Для решения задач в области охлаждения серверных и ЦОДов мы сотрудничаем с компанией «КБ Борей», поставляющей продукцию под брендом BOREY. Это партнерство позволяет нам предлагать клиентам надежные и эффективные решения для охлаждения, которые критически важны для бесперебойной работы ИТ-оборудования.

**«ИКС»: Какие новые продукты появятся у компании в ближайшее время? Каковы ваши бизнес-планы?**

**А.Т.:** Мы уделяем особое внимание тому, чтобы выпускать продукты, которые максимально соответствуют запросам наших клиентов. Для эффективной реализации этой стратегии SYSMATRIX LAB активно взаимодействует с клиентами, принимая обратную связь, и проводит анализ рынка. Этот процесс позволяет нам выявлять ключевые

тенденции и потребности инженеров, что, в свою очередь, помогает разрабатывать продукты, наиболее полно соответствующие запросам нашей целевой аудитории.

SYSMATRIX LAB также активно анализирует конкурентное окружение, выявляя ниши, в которых наши продукты смогут дополнить существующие предложения. Это не только подтверждает ценность наших решений в глазах потенциальных клиентов, но и укрепляет позиции нашей компании на рынке.

В самых ближайших планах – вывести на рынок коммутационную стойку с уникальными характеристиками. Конструкция обеспечит высокую плотность размещения оборудования и удобство организации большого количества кабелей.

**С.С.:** Относительно бизнес-планов. Мы строим большой бизнес. Наша тактика – постоянно подтверждать свою репутацию как надежного поставщика инновационных продуктов.

Эти два фактора сходятся в стратегии, которая помогает нам в построении успешного большого бизнеса.

Мы осознаем, что поставки на ключевые объекты инфраструктуры – это не просто бизнес, это вклад в обеспечение стабильности и надежности современного мира. Мы гордимся возможностью поддерживать критически важные инфраструктурные проекты и продолжаем стремиться к сохранению высокой надежности и доступности данных и сервисов наших клиентов.



# ЕКФ целится в будущие проекты



**Продолжаем начатый в предыдущем номере «ИКС» разговор о решениях ЕКФ, предлагаемых в рамках направления «Телекоммуникационное оборудование TERACOM». Наш собеседник – Алексей Чураков, руководитель данного направления.**

**– Один из ключевых продуктовых сегментов TERACOM – это структурированные кабельные системы. Что уже предлагаете? Как развиваются эти системы?**

– Мы видим свою задачу в том, чтобы предлагать не отдельные продукты, а полноценное решение для организации слаботочных систем – от информационной розетки в офисе до порта на коммутационном поле кросс-панелей, откуда идет подключение к активному оборудованию. Начали мы с медножильных решений. В нашем ассортименте – все необходимые компоненты: кабели, коммутационные шнуры, информационные модули и розетки, патч-панели. В настоящее время производим продукты категорий 5е, 6 и 6А. В следующем году планируем расширить предложение до категории 8.1. Это высокочастотные (рабочий диапазон до 2000 МГц) высокопроизводительные кабельные системы, способные обеспечить скорость передачи данных до 40 Гбит/с.

Выпускаемые сегодня решения категории 5е и категории 6 – как неэкранированные, так и экранированные, 6А – только экранированные. Выпуск неэкранированных (УТР) компонентов категории 6А намечен на следующий год. Это будет решение, актуальное главным образом для каблирования больших серверных шкафов и стоек. Дело в том, что диаметр экранированных кабелей и шнуров категории 6А довольно велик, что затрудняет их установку и обслуживание в местах подключения большого числа портов. УТР-вариант позволит минимизировать размеры кабельных пучков, которые заводятся в серверные стойки. Это, по сути, обязательный вариант для многих проектов, реализуемых в крупных бизнес-центрах, серверных комнатах и ЦОДах.

Конечно, в подобных проектах невозможно обойтись без оптики. Соответствующие решения – в наших ближайших планах. С начала следующего года будем выводить на рынок оптические шнуры, пигтейлы, адаптеры, стоечные кроссы, а также всевозможные расходники для организации подключений, спайки, разводки на отдельные порты и пр. Эти продукты появятся в первую очередь.

Для высокоплотных оптических систем требуются более технологичные решения и жесткий контроль качества, вплоть до контроля каждого компонента. Установка некачественного компонента может привести к тому, что большой объем установки, большой сегмент сети окажется неработоспособным. Поэтому мы тщательно подходим к выбору производственной площадки и организации контроля качества этих изделий. И высокоплотные решения планируем выпустить чуть позже, после вывода базовых оптических компонентов.

**– А что из кабеленесущих систем предлагает ЕКФ?**

– Это не новая для ЕКФ продуктовая группа. Металлические и пластиковые кабель-каналы выпускаем давно. Но недавно обновили производственную площадку, установив в начале 2022 г., пожалуй, самую мощную линию по производству прокатного металлического лотка в России. Сейчас линия вышла на плановые, максимальные мощности.

Мы предлагаем лотки разного исполнения: листовые, лестничные, проволочные. Последний вариант особенно актуален для ЦОДов, поскольку обеспечивает вентиляцию прокладываемых кабелей и быстрый доступ для обслуживания кабельных трасс. Скорость изготовления листового лотка составляет 25 м/мин, что позволяет обеспечивать крупные проекты и поддерживать складской запас с минимальными сроками поставки. Многие конкуренты работают «от заказа», и заказчик вынужден ждать, пока продукт изготавливают.

В портфеле продуктов ЕКФ имеются традиционные пластиковые кабель-каналы со всеми необходимыми аксессуарами: всевозможные углы, повороты и пр. В ближайших планах – выпуск пластиковых ПВХ-лотков. Это тоже категория продуктов, которые часто используются в ЦОДах для подведения к стойкам как медных, так и оптических кабелей. Также компания предлагает огнестойкие проходки и огнестойкие короба.

**– Для подобных решений важно наличие сертификата пожарной безопасности.**

– Вы правы. Мы ответственно подходим к вопросу сертификации. Считаем, что любой добросовестный производитель должен подтверждать качество своей продукции соответствующими сертификатами. И мы, конечно, выполним соответствующие процедуры для огнестойких проходок.

Для многих объектов требования пожарной безопасности очень высокие. Например, витопарные кабели, которые прокладываются в пучках на объектах с массовым пребыванием людей, должны иметь безгалогенную оболочку нг(А)-HF. А для объектов социального назначения (больницы, детсады, школы) годятся только слаботочные кабели с оболочкой с низким содержанием токсинов при горении. Оба варианта кабелей у нас есть, сейчас занимаемся получением соответствующих сертификатов.

Считаем важным получить сертификат и на огнестойкие кабельные линии (ОКЛ). В состав таких линий входит не только кабель, но и кабеленесущие элементы. Пока для формирования ОКЛ у нас не хватает кабелей с огнестойкой оболочкой. Их выпуск также в наших планах.

**– Давайте поговорим еще об одном важном продуктом сегменте TERACOM: шкафах для размещения оборудования.**

– Мы предлагаем различные телекоммуникационные шкафы. Например, настенные – емкостью 4U, 6U, максимум 18U. Они универсальны: их можно не только повесить на стену, но и поставить на пол. Дверки у таких шкафов, как правило, обзорные, из ударопрочного каленого стекла. Напольные шкафы – от 18U до 48U. Ширина стандартная – 600 или 800 мм, глубина – от 600 до 1000 мм. У этих шкафов двери разные: глухие металлические, перфорированные, стеклянные.

Самая интересная для ваших читателей категория – серверные шкафы. Это изделие более сложное по сравнению с обычным телекоммуникационным шкафом. Серверные шкафы применяются для дорогостоящего и тяжелого активного оборудования. Они должны выдерживать высокую статическую нагрузку (до 1500 кг), обеспечивать организацию большого числа кабелей, установку блоков распределения питания (БРП, PDU), удобное обслуживание оборудования. Кроме того, это должны быть не просто отдельные шкафы, а конструктивы, которые можно смонтировать в ряды с выделением и организацией холодных и/или горячих коридоров. Сейчас мы разрабатываем решение, которое будет обладать всеми перечисленными свойствами. Планируем представить на рынок в следующем году. Причем это будет комплексное предложение, включающее не только шкафы, но и все элементы для изоляции коридоров, все необходимые аксессуары.

**– А какие решения вы можете предложить для организации систем электропитания?**

– Для этих задач служат две основные группы продуктов: ИБП и БРП. ИБП поставляются под брендом E-Power. На данный момент имеются онлайнные моноблочные ИБП мощностью до 30 кВт. До конца этого года представим источники мощностью до 100 кВт. Также в ближайших планах – модульные аппараты мощностью до 600 кВт.

В линейке БРП сейчас – горизонтальные устройства максимум на девять розеток. В следующем году появятся вертикальные БРП со значительно большим числом розеток. Они рассчитаны на большие шкафы, где много активного оборудования. Дальше будем расширять ассортимент в направлении smart-решений с дистанционным мониторингом и управлением, в том числе с возможностью подключения датчиков для контроля внутреннего состояния стойки.

Smart-БРП будут работать в связке с нашей облачной IoT-платформой EKF Connect Industry, официальный запуск которой запланирован на начало следующего года. Она позволит осуществлять удаленный мониторинг и управление не только БРП, но и другими инженерными системами дата-центров: охлаждения, вентиляции, резервного питания и др.

**– Вы основательно подходите к разработке новых продуктов. Но многие важные вещи пока в планах. Не боитесь опоздать с их выводом на рынок?**

– Согласен, эту работу нельзя вести долго. Мы не одни на рынке. Если слишком затянем, то просто останемся не у дел. Но те сроки, которые я называю, вполне оптимистичны. Судите сами, направление TERACOM существует с начала 2023 г., и уже в 2024-м мы планируем предложить современные технологичные решения для ЦОДов, включая системы изоляции коридоров, высокоплотную оптику,



мощные модульные ИБП. У некоторых конкурентов на это уходило до 10 лет.

Более быстрый вывод продуктов на рынок с высокими требованиями к надежности и отказоустойчивости влечет за собой риск запуска «сырых» решений, что скажется на репутации. Да, мы целимся в будущие проекты, тщательно прорабатывая наши продукты. Но уже сейчас стараемся попасть в вендор-листы крупных клиентов. Пока с базовым оборудованием. Но в дальнейшем, когда мы войдем в число поставщиков таких заказчиков, нам будет проще предлагать им новое оборудование.

**– Какие сервисы вы предлагаете для своих решений?**

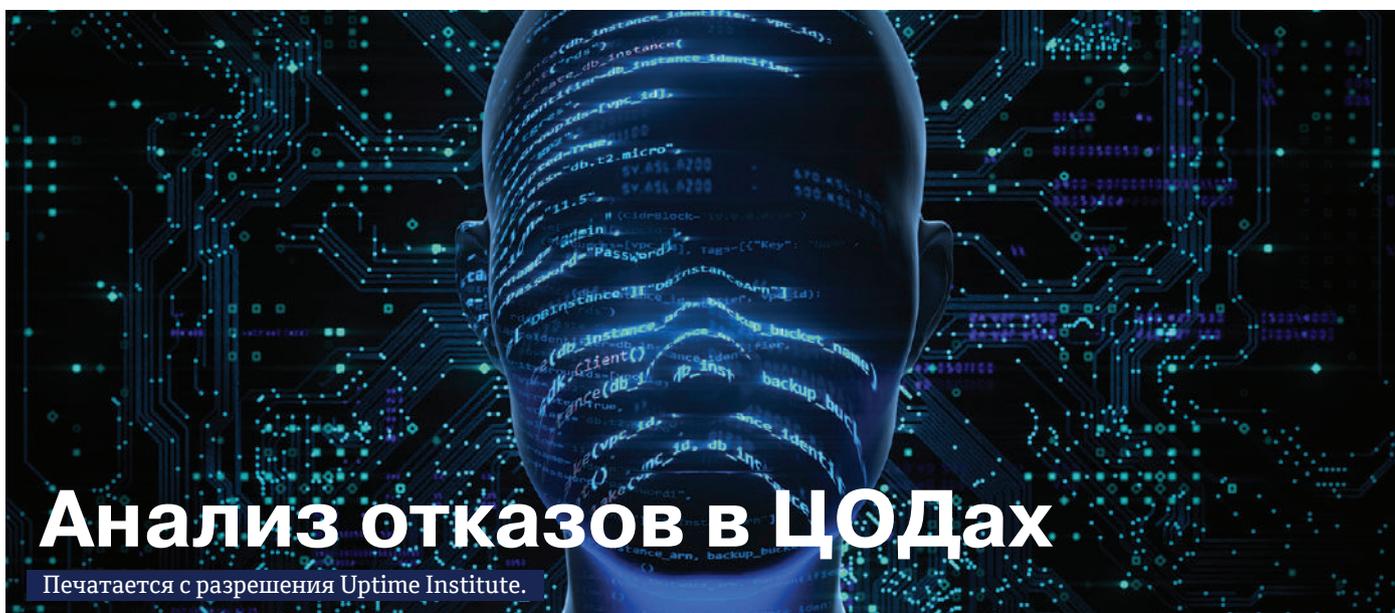
– Ни один современный продукт невозможен без сервисов, поэтому мы уделяем им особое внимание. Сервисы – это один из важных параметров, характеризующих ответственного вендора. Как правило, они требуют существенных вложений, но редко монетизируются. Поэтому сервисы запускают с перспективой на долгий срок существования продукта.

Наши сервисы касаются различных направлений. Есть, например, финансовая поддержка. Есть всевозможные логистические сервисы, связанные с повышением удобства отгрузки, доставкой товара напрямую с нашего склада (минуя склады партнеров), резервированием продуктов для крупных проектов и т.д.

Отдельно выделю сервисы, обеспечивающие удобство работы с нашими продуктами. Это в первую очередь сервисы для проектировщиков. У нас уже есть всевозможные калькуляторы, конфигураторы, сейчас готовим BIM-модели. И мы ничего не прячем, все эти инструменты будут в открытом доступе на сайте.

Не так давно в компании появился полноценный инженеринговый центр, где разрабатываются типовые решения по электроснабжению, автоматизации здания. Наша команда готова браться и за нестандартные задачи. Возможен и последующий шеф-монтаж, если клиенту это потребуется.





# Анализ отказов в ЦОДах

Печатается с разрешения Uptime Institute.

**Энди Лоуренс**, исполнительный директор по исследованиям;

**Ленни Саймон**, старший научный сотрудник, Uptime Institute

**Предотвращение сбоев в работе цифровой инфраструктуры – приоритетная задача для руководителей всех компаний, участвующих в предоставлении ИТ-услуг. Чтобы снизить вероятность повторения отказов ИТ-систем и ЦОДов, важно располагать данными об их типе, частоте и последствиях.**

## Методология и терминология

Собирать информацию об отказах – дело непростое. Одни аварии широко освещаются в СМИ, другие остаются не известными общественности. Некоторые менеджеры, сотрудники и клиенты ЦОДов могут знать о перебоях в его работе, в то время как другие не будут осведомлены об этом. Кроме того, проблемы, связанные с деградацией сервисов или перебоями в работе, могут не классифицироваться как отказы.

В этом материале использованы данные из разных источников (табл. 1), включая общедоступную информацию (например, опубликованную в СМИ и соцсетях), аналитические исследования Uptime Institute (в частности, глобальный опрос руководителей ИТ-служб и ЦОДов в 2022 г.

и исследование отказоустойчивости ЦОДов в 2023 г.), а также другие обезличенные и обобщенные данные, полученные от участников опросов и партнеров Uptime. Отказы в работе ИТ-систем и ЦОДов (далее – отказы) в зависимости от серьезности их последствий мы разделяем на пять категорий (табл. 2).

Несколько десятилетий инноваций, масштабные инвестиции и совершенствование процедур эксплуатации в ИКТ-отрасли позволили добиться того, что в целом критически важные ИТ-системы, сети и центры обработки данных стали намного более надежными, чем раньше. Впечатление, что серьезные сбои происходят чаще, обусловлено усилением зависимости экономики и общества от ИТ, а также большей прозрачностью работы ИТ-систем

**Табл. 1.** Источники информации, используемые Uptime Institute для отслеживания отказов в работе ИТ-систем и ЦОДов ▼

Источники	Точность	Методология	Ограничения
Общедоступная информация	Низкая	Мониторинг новостного потока в СМИ/соцсетях	В основном фиксируются крупные аварии и перебои в предоставлении услуг конечным потребителям
		Косвенные свидетельства отключений	Могут отсутствовать детали
		Заявления компаний	Источники могут быть ненадежными или плохо информированными
Исследования Uptime Institute	Средняя/хорошая	Отраслевые опросы Uptime Institute	Ответы могут варьироваться в зависимости от должности источника и выборки респондентов. Все ответы анонимны
База данных Uptime Abnormal Incident Report (AIRs)	Хорошая/очень хорошая	Подробные, точные данные по объекту передаются в соответствии с соглашением о неразглашении	Детализация в основном на уровне объекта/площадки. Все данные анонимны

благодаря публикациям в новостных каналах и соцсетях.

Для большинства руководителей ЦОДов и ИТ-служб небольшие перебои в обслуживании на уровне ИТ-систем – частый раздражитель и признак того, что требуются дополнительные внимание и инвестиции. Но в фокусе настоящего отчета находятся более серьезные инциденты (категорий 3, 4 и 5), которые могут иметь тяжелые последствия и требуют детального анализа первопричин, а также корректирующих действий, чтобы снизить вероятность их повторения.

Растущее в последние годы использование облачных сервисов изменило характеристики отказов. Они часто вызваны ошибками ПО или конфигурирования, и это отражает растущую сложность ИТ-систем и обслуживающих их сетей.

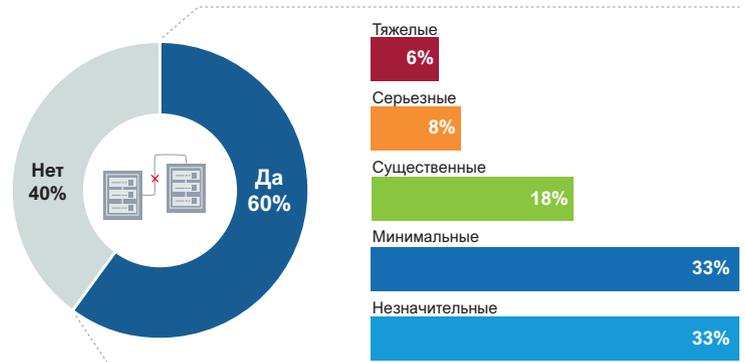
### Частота и тяжесть отказов

Насколько часто происходят отказы? Увеличивается ли их число? Ответы на эти вопросы зависят от того, кого вы спрашиваете и как ваши респонденты определяют, что такое отказ. Несмотря на эти методологические сложности, данные опросов Uptime Institute, охватывающие большие группы руководителей ЦОДов и ИТ-служб по всему миру, относительно непротиворечивы.

Они свидетельствуют о том, что количество отказов во всем мире увеличивается из года в год по мере роста отрасли. Это увеличение наряду с очевидными последствиями некоторых отключений неизбежно привлекает внимание общественности. Может создаться ложное впечатление, что частота отказов в пересчете на единицу емкости ИТ-систем растет. На самом деле это не так. Число отказов растет не так быстро, как масштабы ИТ-инфраструктуры или глобальная емкость ЦОДов.

В четырех опросах, проведенных в 2020–2022 гг., доля менеджеров ЦОДов, которые столкнулись с перебоями в работе своих объектов,

Происходили ли за последние три года в работе вашей организации сбои, вызванные отказами на вашем собственном объекте или у стороннего поставщика услуг? Если да, то классифицируйте их по тяжести от 1 (незначительный) до 5 (тяжелый) (n = 730)



Источник: Uptime Institute Global Survey of IT and Data Center Managers, 2022

колебалась от 60 до 80%. В целом частота отказов в пересчете на одну площадку (или на одного респондента опроса) устойчиво снижается. В 2022 г. из числа операторов, участвовавших в ежегодном опросе Uptime, о перебоях в работе за последние три года заявили 60%, в то время как в 2021 г. таких операторов было 69%, а в 2020 г. – 78%.

Но мы не хотели бы заявлять о прорывном улучшении ситуации по двум причинам. Во-первых, влияние пандемии COVID-19 на бизнес-климат и на работу ИТ-служб и ЦОДов затрудняет сравнение результатов исследований последних лет. Во-вторых, есть некоторые противоречивые данные (здесь они подробно не обсуждаются), которые требуют дальнейших исследований.

Есть также признаки того, что частота по крайней мере некоторых категорий отказов уменьшается. Uptime Institute классифицирует отказы по шкале от 1 до 5 (см. табл. 2), и в две наиболее серьезные категории (4 и 5) исторически попадал примерно каждый пятый отказ. Но по данным опроса, проведенного в 2022 г., доля этих отказов сократилась до 14% (рис. 1).

▲ Рис. 1. Доли различных категорий отказов за последние три года

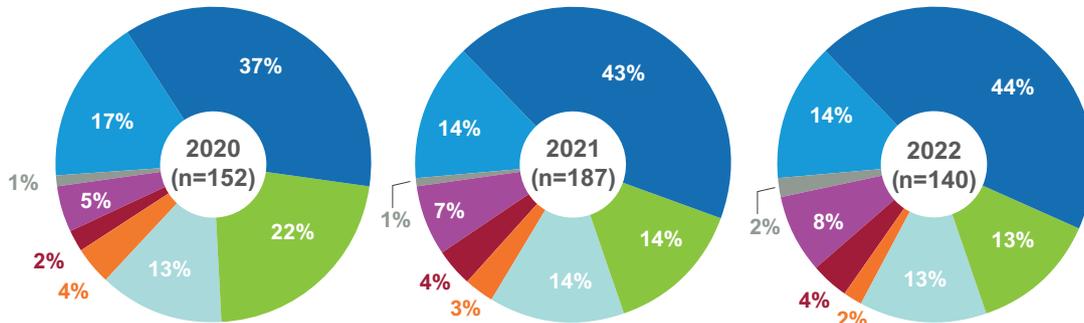
Табл. 2. Классификация отказов по серьезности их последствий ▼

Категория	Последствия	Пояснения
1	Незначительные	Сбой регистрируется, но не оказывает заметного влияния на предоставляемые ЦОДом сервисы
2	Минимальные	Предоставление сервисов нарушается, но влияние на пользователей/заказчиков/репутацию минимально
3	Существенные	Фиксируются перебои в обслуживании клиентов/пользователей, но в основном ограниченного масштаба, продолжительности или эффекта. Финансовый эффект минимален или отсутствует. Некоторое влияние на репутацию или выполнение регуляторных требований
4	Серьезные	Серьезные перебои в предоставлении сервисов и/или работе ЦОДа. Последствия включают в себя некоторые финансовые потери, нарушение регуляторных требований, ущерб репутации и, возможно, реализацию угроз безопасности. Возможна потеря клиентов
5	Тяжелые	Серьезные и разрушительные перебои в предоставлении сервисов и/или работе ЦОДа. Последствия включают в себя крупные финансовые потери и, возможно, реализацию угроз безопасности, нарушения регуляторных требований, потерю клиентов и ущерб репутации



Что послужило основной причиной последнего значимого инцидента или отказа в вашей организации?

- Система электроснабжения
- Сетевая инфраструктура
- ИТ-системы (аппаратура и ПО)
- Система охлаждения
- Пожар/система пожаротушения
- Проблемы с безопасностью
- Сторонний провайдер
- Неизвестно



Источник: Uptime Institute Global Survey of IT and Data Center Managers, 2020–2022

▲ Рис. 2. Основные причины отказов в ЦОДах

Какие выводы можно извлечь из полученных данных?

- Частота отказов относительно постоянна и высока, несмотря на усовершенствование технологий, ПО и методов физического резервирования. Обусловленные отказами финансовые и/или репутационные издержки оправдывают серьезную обеспокоенность руководителей и регулирующих органов.
- Несмотря на шумиху в СМИ, нет никаких свидетельств того, что число отказов увеличивается в сравнении с общим ростом масштабов ИТ-систем – возможно, оно даже медленно сни-

жается. (Uptime Institute проводит дальнейшие исследования по этому вопросу.)

- Частота отказов и их продолжительность убедительно свидетельствуют о том, что фактические показатели многих поставщиков не соответствуют соглашениям об уровне обслуживания (SLA). Клиентам не следует рассматривать SLA (или показатели доступности, выраженные тем или иным количеством девяток (99,9...)) в качестве надежной гарантии будущей доступности сервисов.

Анализ данных об отказах затрудняют два фактора. Первый связан с последствиями пан-

## Аварии, информация о которых становится общедоступной

В дополнение к своим регулярным исследованиям и опросам Uptime Institute отслеживает крупные (или громкие) аварии, о которых сообщают СМИ или другие общедоступные источники. Эта информация иногда отличается от данных опросов.

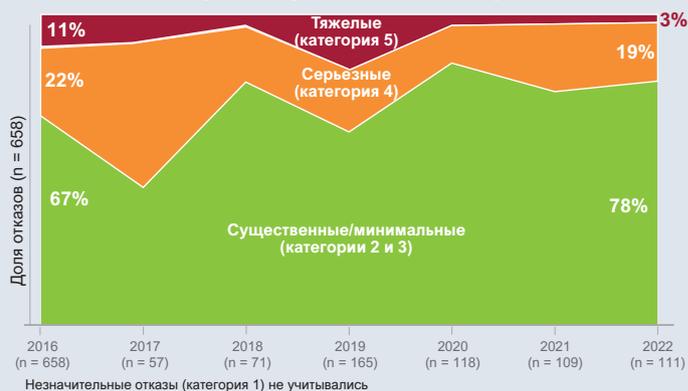
В последние годы СМИ и соцсети все чаще сообщают об отказах ЦОДов, но многие из них незначительны, а информация о них нередко неточна. Поэтому мы не учитываем сообщения о незначительных происшествиях, для которых трудно проверить детали и которые не привели к серьезным финансовым потерям, сбоям в работе или потере репутации.

Абсолютное число серьезных аварий, о которых публично сообщалось, сократилось за последние четыре года. Но неясно, вызвано это технологическими изменениями, изменениями в работе ЦОДов или другими факторами –

хотя пандемия COVID-19, может быть, ослабила последствия отказов в 2020 г.

Собранные нами данные позволяют предположить, что каждый год по всему миру, вероятно, будут происходить 10–20 серьезных аварий в области ИТ, которые приведут к крупным финансовым потерям, сбоям в работе компаний, потере репутации или даже к гибели людей.

↓ Доля различных категорий отказов (за исключением незначительных), о которых сообщалось публично



Источник: Uptime Institute Intelligence, 2023

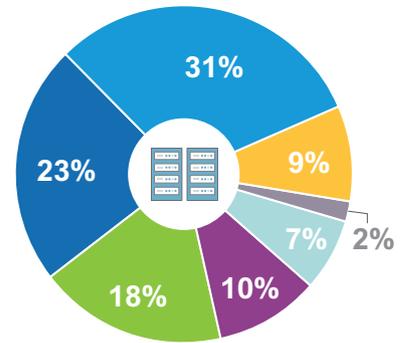
↓ Число отказов, информация о которых появилась в открытых источниках и которые учтены Uptime Institute

2016	2017	2018	2019	2020	2021	2022	Всего
27	57	71	165	118	109	111	656



Какие из перечисленных ниже проблем были наиболее распространенной причиной сбоев в работе ИТ, которые затронули вашу организацию за последние три года? (n = 406)

- Проблемы с сетью/коннективностью
- Проблемы с электроснабжением
- Проблемы с ИТ-системами/ПО
- Проблемы у провайдеров ИТ-сервисов (публичные облака, SaaS и пр.)
- Проблемы с охлаждением
- У нас не было сбоев
- Другое



Источник: Uptime Institute Data Center Resiliency Survey, 2023

демии: в то время как одни операторы ЦОДов были вынуждены сократить объем технического обслуживания, другие, наоборот, смогли проводить внеплановое дополнительное техобслуживание. Второй – со смещением акцентов с ЦОДов премиум-класса, часто имеющих одну резервную площадку, на более сложные распределенные архитектуры. Хотя последние в конечном счете могут оказаться более устойчивыми, обеспечение отказоустойчивости в больших и сложных сетях ЦОДов еще недостаточно отработано.

### Причины отказов

Знание причин отказов имеет решающее значение для их предотвращения в будущем. Большинство инцидентов имеют несколько причин, и, как мы заметили в ходе опросов, понимание

их деталей может зависеть от точки зрения конкретного специалиста.

Ежегодные глобальные опросы руководителей ИТ-служб и ЦОДов дают надежный и непротиворечивый набор данных от респондентов, которые, как правило, в деталях осведомлены о работе ЦОДов, но не всегда обладают столь же подробными знаниями обо всех аспектах работы ИТ-систем. Другие исследования Uptime, охватывающие более широкую группу респондентов, могут выявлять другое распределение причин отказов. Поэтому к подобным данным следует относиться аккуратно.

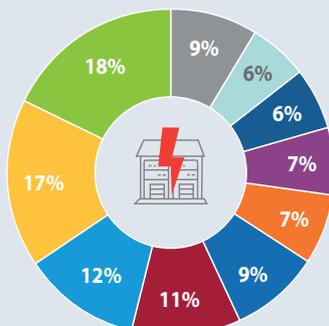
Результаты ежегодного опроса, проведенного Uptime в 2022 г., хорошо согласуются с данными предыдущих лет. Они показывают, что основной причиной отказов на большинстве объектов остаются проблемы с электроснабжением

**▲ Рис. 3.** Основные причины сбоев в работе ИТ-сервисов за последние три года

Публично зафиксированные или заявленные перебои в работе ИТ-систем имеют разные причины, но демонстрируют и некоторые закономерности. Так, за последние два года кибератаки и программы-вымогатели стали регулярной и все более частой причиной перебоев. На их долю пришлось 11% публично зарегистрированных отказов в 2022 г. (в 2021 г. – 8%) – см. рисунок ниже. Среди известных жертв были оператор ЦОДа и международная газета.

### ↓ Причины отказов, о которых сообщалось публично (2022 г.)

- ИТ (ПО/конфигурация)
  - Оптический кабель
  - Сеть (ПО/конфигурация)
  - Кибератаки/программы-вымогатели
  - Электроснабжение
  - Пожар
  - Проблемы у провайдера (партнера)
  - Нехватка ресурсов
  - Охлаждение
  - Сеть (кабельная система)
- (n=103)



Источник: Uptime Institute Intelligence, 2023

Атаки программ-вымогателей часто приводят к длительному отключению значительной части цифровой инфраструктуры организации. Из-за заражения систем и нарушения целостности данных организациям приходится перестраивать системы и базы данных. Потеря информации при таких инцидентах – обычное дело. Внедрение стандартных операционных систем для управления инженерным оборудованием ЦОДов и более широкое использование средств удаленного мониторинга значительно повышают риск нарушений безопасности в дата-центрах.

Чем больше рабочих ИТ-нагрузок передается на аутсорсинг внешним поставщикам, тем больше громких аварий приходится на их долю. Начиная с 2016 г. на провайдеров и коммерческие ЦОДы пришлось две трети (66%) всех отказов, о которых сообщалось публично. И эта доля увеличивается из года в год: в 2021 г. – 70%, а в 2022 г. – уже 81%. Причем сильнее всего выросло количество отказов из-за отключения услуг связи, в то время как число сообщений о перебоях в работе облачных сервисов сократилось. Отчасти это вызвано высокой зависимостью почти всех услуг от телекоммуникаций, но также и тем, что телеком-операторы перешли от дорогостоящих проприетарных систем к более доступным компонентам и архитектурам.

Считаете ли вы, что публичные облака достаточно устойчивы для выполнения критически важных ИТ-нагрузок вашей организации?



Источник: Uptime Institute Data Center Resiliency Survey, 2023

▲ Рис. 4. Устойчивость публичных облаков для критически важных ИТ-нагрузок

(рис. 2). Как и в предыдущие годы, все остальные причины встречаются гораздо реже. Три другие распространенные причины также неизменны: сбои в системе охлаждения, ошибки ПО/ИТ-систем и проблемы с сетевой инфраструктурой. Частота проблем у сторонних поставщиков – например, у провайдеров SaaS, хостинга и инфраструктурных облачных сервисов – растет, что отражает более интенсивное использование облаков и услуг colocation.

При опросе более широкого круга специалистов картина несколько меняется. В ежегодном исследовании отказоустойчивости ЦОДов мы также задаем вопросы о наиболее распространенных причинах комплексных сбоев в работе ИТ-служб. Ответы показывают, что проблемы, связанные с сетевой инфраструктурой и кон-

Рис. 5. Наиболее частые причины отказов из-за поставщиков ИТ-услуг ▼

Сталкивались ли за последние три года ваша организация с серьезными отказами, вызванными проблемами у поставщика ИТ-услуг (n = 186)? Если да, то каковы их наиболее распространенные причины? (Выберите не более трех вариантов)



Источник: Uptime Institute Data Center Resiliency Survey, 2023

нективностью, встречаются чаще проблем с электроснабжением (рис. 3).

### Надежность облачных сервисов

Облачные сервисы спроектированы таким образом, чтобы минимизировать вероятность отказов. Для этого крупные провайдеры (такие как Amazon Web Services, Microsoft Azure и Google Cloud) включают в свои решения специальные уровни промежуточного ПО; распределяют нагрузку по системам, сетям и ЦОДам; перенаправляют трафик в обход мест аварий и проблемных сайтов. В целом их архитектуры обеспечивают высокий уровень доступности услуг. Но ни одна архитектура не является абсолютно отказоустойчивой, и многие зарегистрированные сбои можно отнести на счет трудностей управления сложным инфраструктурами облачных провайдеров.

Надежность (и прозрачность) публичных облаков в последние годы стала предметом пристального внимания из-за некоторых громких сбоев в их работе и растущего интереса к запуску в таких облаках критически важных ИТ-сервисов. Концентрация – чрезмерная зависимость от нескольких основных сервисов и ЦОДов, на базе которых эти сервисы предоставляются, – также вызывает озабоченность.

В нашем опросе только каждый десятый респондент счел, что публичные облака достаточно устойчивы для выполнения всех рабочих ИТ-нагрузок. При этом почти каждый пятый (18%) не доверит свои ИТ-нагрузки таким облакам, а около трети (34%) готовы перенести туда только часть нагрузок (рис. 4). Это не те цифры, которые хотели бы видеть облачные провайдеры. Но они вряд ли кардинально изменятся до тех пор, пока провайдеры не смогут предложить больше гарантий прозрачности – и, возможно, новые SLA, предоставляющие критически важным заказчикам больший контроль и компенсацию в случае нарушения соглашений.

Конечно, беспокойство по поводу отказоустойчивости облаков может быть отчасти обусловлено количеством сбоев в работе облачных сервисов, которые попадают в заголовки газет. В нашем исследовании вопросов отказоустойчивости за 2023 г. 42% респондентов (рис. 5) заявили, что за последние три года их организация страдала от перебоев в работе, вызванных проблемами у провайдера, – незначительный рост по сравнению с 2022 г. (39%).

→ Окончание статьи – в следующем номере «ИКС»



# Сертификация СКС: чем и зачем?

**Российский рынок покинул основной производитель измерительного оборудования, используемого при сертификации СКС. Что делать компаниям-инсталляторам, которые хотят предоставлять качественные услуги, и на что рассчитывать заказчиком?**

**Екатерина Оганесян,** независимый эксперт, автор и ведущий преподаватель курсов по СКС в Бауманском учебном центре «Специалист»

С уходом продукции Fluke Networks из России мнения на рынке СКС разделились – от панического «все пропало» до равнодушного «раз мерить нечем, то и не надо». И дело не в том, объявляла ли компания об уходе официально или ее ресурсы стали недоступны по факту.

У всех поставщиков решений СКС, выдающих гарантии на установленные системы, есть требования к тестированию. В старших и наиболее производительных кабельных системах это обязательная сертификация СКС прибором с действующей заводской калибровкой. Так было заведено у брендов – Systimax, Panduit, Siemon, Legrand и других, ушедших с нашего рынка. Такой же подход исповедуют и отечественные производители СКС: ДКС, «Гиперлайн», ИТК и прочие. И хотя сейчас у поставщиков СКС в списках разрешенных приборов фигурирует с десятков моделей от разных изготовителей, в России за последние 15 лет львиная доля измерений выполнялась тестерами Fluke Networks: анализаторами DTX, затем приборами DSX на шасси Versiv. Ими пользовались компании-монтажники, и с ними же на объекты выезжали эксперты, если что-то было не так.

Предпочтение не только негласное, оно прослеживается документально. У ДКС в материалах 2022 г. о системной гарантии указаны только приборы Fluke DSX. У ИТК в листе требований к тестированию 2023 г. названий приборов нет, но пункты настроек и имена диагностических функций однозначно отсылают к Fluke Networks. У «Гиперлайна» в описаниях системной гарантии недавно расширился список разрешенных тестеров; в прежние же годы предпочтение в явном виде отдавалось приборам Fluke. Неудивительно, что рынок СКС был ошарашен, когда компания Fluke Networks свернула деятельность на территории нашей страны.

Между тем доминировал этот производитель в России далеко не всегда, просто знают об этом только специалисты с большим стажем. С середины 1990-х гг., когда в нашей стране начали массово устанавливать СКС и выдавать гарантии на них, сменилось не одно поколение приборов. Происходили слияния и поглощения компаний-изго-

товителей, переименовывались, а иногда даже закрывались целые линейки оборудования. И при этом рынок тестирования продолжал жить. Если вспомнить хронологию тех событий, становится понятным, что он будет жить и дальше.

## 90-е годы: начало сертификации СКС в России

Вместе со структурированными кабельными системами от западных брендов в Россию пришли и приборы для их сертификации. Монтажники старой закалки помнят семейство Pentascanner компании Microtest. Эти тестеры еще не умели проверять категорию 5e – только категорию 5; измеряемые параметры соответствовали требованиям телекоммуникационного бюллетеня TSB-67, обеспечивая поддержку до 100 Мбит/с включительно. Догигабитные времена, полудуплекс... Но модели Pentascanner 2Way+ и Pentascanner 350 были, по сути, первыми приборами, у которых измерительный функционал основного и удаленного модуля стал одинаковым. До этого основные модули были измерителями, а удаленные – инжекторами. Так было написано в англоязычных инструкциях, так их называли и монтажники. Чтобы провести полную сертификацию, сначала нужно было выполнить измерения с основным модулем на одном конце и инжектором на другом, потом поменять их местами и провести измерение во встречном направлении. Но уже тогда на приборах была большая кнопка «AUTOTEST», а для трактовки результатов применялся критерий PASS/FAIL.

Название «инжектор» осталось в ходу даже после того, как основной и удаленный модули обрели одинаковый измерительный функционал. Обозначение «2-Way Injector+» было призвано подчеркнуть, что тестирование в обоих направлениях можно провести прибором Pentascanner за один цикл измерений – большой прогресс с точки зрения затрат времени на приемосдаточные испытания.

Еще одним шагом вперед стало появление в России прибора WireScope 155 от Agilent Technologies. Дело не в расширенном до 155 МГц диапазоне частот для систем, работавших в медных

средах (прибор все равно проводил измерения только на категорию 5, не 5e), а в том, что изготовитель поставлял также многомодовые и одномодовые насадки на прибор, чтобы сертифицировать волоконно-оптические линии. Насадки Fiber SmartProbe, входящие в один комплект, были не одинаковы. Для многомодовых систем один модуль имел источник излучения на длине волны 850 нм, другой – 1300 нм; для одномодовых соответственно 1310 нм и 1550 нм. Либо приходилось мириться с тем, что одна длина волны тестировалась только в одном направлении, а вторая – только во встречном, либо монтажникам опять в ходе измерения нужно было поменять местами приборы для выполнения полной сертификации. Впрочем, и тогда, и сейчас стандарты тестирования волоконно-оптических линий считают достаточным измерение оптических потерь в одном направлении.

### 2000-е годы: категории 5e и 6, затем 6A

Стандарты TIA, вышедшие в начале двухтысячных годов, содержали три принципиальных новшества, затронувших рынок сертификационных тестеров. Первое состояло в том, что категория 5e, направленная на поддержку 1-гигабитных приложений, была заявлена как минимально допустимая в горизонтальной подсистеме. Это привело к постепенному вытеснению с рынка решений категории 5, не способных гарантировать передачу 1 Гбит/с, – а соответственно и приборов, которые категорию 5e тестировать не умели. Хотя частотный диапазон остался тем же, от 1 до 100 МГц, но для тестирования категории 5e приборы должны были замерять не только перекрестные наводки NEXT на ближнем конце по модели «пара – пара», но и

эквивалентные наводки ELFEXT на дальнем конце, а также рассчитывать интегральные параметры PowerSum NEXT и PowerSum ELFEXT. Для гигабитных приложений с их режимом полного дуплекса жизненно важно проверять наводки со стороны всех пар-соседей на паружертву как на ближнем, так и на дальнем концах. Ни модели Pentascanner, ни WireScope 155 этого обеспечить не могли.

В общем-то рассчитать интегральные наводки из парных измерений нетрудно – такую задачу можно решить обновлением софта. Можно было бы научить приборы также измерять возвратные потери (Return Loss) и детально фиксировать задержку распространения (Propagation Delay) и ее рассогласование (Delay Skew), ведь длина уже в категории 5 замерялась по разнице во времени между отправкой сигнала и получением его отражения. Но новые стандарты еще и детально регламентировали шаги по частотам, на которых нужно выполнять замеры, а главное, приняли новые требования к точности измерений. В этом состояло второе принципиальное новшество. Программно модернизировать прежние семейства приборов оказалось невозможно. Аппаратная модернизация? Производителям было проще и выгоднее выпустить новые линейки приборов.

Такому решению способствовало и третье новшество: окончательное принятие требований к категории 6. Черновики стандартов на категорию 6 выпускались неоднократно, но в 2002 г. в документах TIA (прежде всего TIA/EIA-568-B) требования приняли окончательно. Вслед за этим был опубликован и стандарт ISO/IEC 11801 с описанием класса E в диапазоне частот до 250 МГц, а также класса F в диапазоне до 600 МГц.

Производители измерительного оборудования были в курсе происходящего (и даже принимали участие в разработке стандартов), поэтому нет ничего удивительного в том, что в приборах OMNIScanner компании Microtest настройки категории 6 появились за несколько лет до окончательного принятия требований к таким системам. Некоторые специалисты по СКС могут помнить этот прибор с зеленым обрезиниванием корпуса (рис. 1) – это было еще до того, как компанию Microtest купила Fluke.

Тестер был вполне надежен, а начиная с версии ONMIScanner2 к нему стали предлагаться оптические насадки OMNIFiber для многомодовой или одномодовой волоконной оптики. В начале 2000-х гг. Microtest занимала доминирующее положение на российском рынке.

Поставки тестеров WireScope 350 от Agilent Technologies начались чуть позже. В оптических насадках явно прослеживалось сходство с моделью WireScope 155: передающие порты

Рис. 1. Прибор OMNIScanner в корпоративных цветах компании Microtest ▼



могли выдавать излучение только на одной длине волны. Конкуренты за это время ушли дальше: у насадок OMNIFiber к приборам Microtest передающие порты испускали обе длины волны: 850 нм и 1300 нм для многомодового, 1310 нм и 1550 нм для одномодового.

И хотя у основного модуля WireScope 350 уже тогда был цветной сенсорный экран (первый на рынке тестеров СКС), а интерфейс был более удобен благодаря стилусу и экранной клавиатуре, массового распространения это решение не получило. Основная проблема – не очень высокая надежность. Достаточно несильного удара или падения на стол, и основной модуль разделялся на две части – в одной оставался сенсорный экран, в другой – измерительные схемы и аккумулятор. А сервисного центра Agilent Technologies на территории России не было, и его даже не планировали открывать. Калибровать и тем более чинить приборы и оптические насадки можно было только за рубежом. Это стоило несколько тысяч долларов, а путешествие оборудования туда-обратно занимало полтора-два месяца, если не происходило никаких задержек на таможне.

У Microtest тоже не было ремонтной базы в нашей стране, и первое время приборы для ремонта и калибровки тоже отправляли за рубеж. Однако затем компания стала завозить в Россию калиброванные внутренние платы приборов, чтобы на базе одного из отечественных партнеров менять одни «внутренности» на другие. Новым платам прописывался прежний серийный номер, и клиент получал в свое распоряжение тестер со сроком калибровки, продленным еще на год. Так поступали с платами приборов для медных сред (оптические насадки по-прежнему калибровались только в зарубежном сервисном центре), но и это было большим подспорьем.

Возможно, поэтому семейство OMNIScanner стало так популярно. На это обратили внимание конкуренты, и в 2003 г. компанию Microtest со всеми ее разработками поглотила корпорация Fluke. Слияние заняло около года. После этого приборы OMNIScanner2 и OMNIScannerLT какое-то время поставлялись в фирменных желтых цветах Fluke Networks, как и собственные разработки Fluke серии DSP. Однако вскоре эти наименования сняли с производства, чтобы расчистить место новому семейству DTX. Решение было маркетинговым. Чисто технически и по точности, и по тестируемым параметрам прежние приборы можно было бы применять до выхода новых стандартов, но изготовитель перестал их калибровать и ремонтировать. Старые тестеры принимались только в зачет покупки новых анализаторов DTX. До сих пор у некоторых компаний на руках остались приборы OMNIScanner и

DSP. Как и осадок, связанный с прекращением их поддержки.

Хотя нужно отметить: анализатор DTX получился весьма удачным. Пользовательский интерфейс прибора и программа для скачивания результатов на ПК были русифицированы, в то время как у серий OMNIScanner и DSP интерфейс оставался англоязычным, а переведены были только инструкции пользователя. Расширился частотный диапазон, и теперь сертификацию на категорию 7 (точнее, класс F) можно было проводить прямыми измерениями в диапазоне до 600 МГц, а не экстраполяцией. ЖК-экран стал цветным – не сенсорным, как у приборов WireScope 350 от Agilent Technologies, но ярким и четким. Оптические модули можно было держать постоянно подключенными в тыльном отсеке прибора, переключение между оптической и медной средами выполнялось кнопкой в меню. Даже с подключенной оптикой емкости аккумулятора стало хватать на полную рабочую смену. Для улучшения точности при тестировании многомодовых линий поначалу использовались катушки-оправки, унаследованные от семейства OMNIScanner (рис. 2), а затем были разработаны шнуры по технологии Encircled Flux, у которых «катушку» сделали плоской и встроили в конструктив шнура.

Пожалуй, единственное, что вызывало даже не нарекания, а скорее, некоторое недоумение – поворотный переключатель на корпусе, доставшийся в наследство от семейства DSP (возможно, как свидетельство корпоративной приверженности Fluke своим первым изделиям – мультиметрам). По мере уточнения требований к категории 6A выходили обновления софта и новые аксессуары; прибор научили измерять даже межкабельные наводки ANEXT – для этого раз-



▲ Рис. 2. Прибор DTX-1800 с подключенными оптическими модулями DTX-MFM и многомодовыми шнурами с катушками-оправками

работали специальный комплект, хотя распространения на практике он не получил. Анализаторы DTX пользовались популярностью у монтажных компаний и заказчиков во всем мире.

На этом фоне в 2008 г. компания Agilent Technologies приняла волевое решение уйти с рынка полевых тестеров и сосредоточиться на нише лабораторных сетевых анализаторов. Для тех, у кого на руках были приборы WireScope 350 и буквально за год до того выпущенные приборы WireScope Pro, которые могли тестировать категорию 6A и межкабельные наводки, это стало настоящим ударом. Лишь на территории США власти обязали компанию Agilent предоставлять клиентам поддержку (ремонт, калибровку, продажу аксессуаров) до 2013 г. Потребители во всех остальных странах в случае поломки оставались ни с чем. И даже исправный прибор после истечения годичного периода калибровки становился бесполезен, поскольку никто не мог поручиться за достоверность его результатов.

Компания Fluke Networks не зевала и с удовольствием заняла освободившуюся нишу. Какое-то время в России она даже принимала приборы других изготовителей в зачет покупки тестеров Fluke. Это затронуло в том числе и приборы LanTEK разных поколений от IDEAL Industries, хотя их сдача была не такой повальной, как приборов WireScope от Agilent. В том числе потому, что в IDEAL Industries сделали экраны цветными и яркими даже раньше других, тоже русифицировали интерфейс, расширили частотный диапазон и научили старшие модели приборов сертифицировать категорию 6A.

На рубеже 2010 г. в России осталось два производителя приборов: Fluke Networks и IDEAL Industries. Но наработки Agilent Technologies не исчезли и оставили свой след в оборудовании других изготовителей.

### 2010-е годы: расширение списка производителей

С начала 2010-х гг. на мировом рынке сертификационных тестеров появились два новых и очень похожих прибора: WireXpert от американской компании PsiberData с производственной базой в Малайзии и Certifier40G от китайского производителя JDSU (теперь VIAVI). Приборы отличаются только названием и цветом пластиковых деталей. Это неудивительно, поскольку Certifier40G – клон своего малайзийского собрата и выпускается по лицензии. Старшие модели WireXpert 4500 (PRO) и Certifier40G отвечают потребностям ЦОДов и способны проводить измерения до категории 8 включительно. Модель Certifier10G (аналог WireXpert 500) стала выпускаться позже – ее возможности усечены до сертификации категории 6A. С 2018 г. оригиналь-

ное семейство WireXpert выпускается под маркой Softing, поскольку изготовитель провел ребрендинг.

Любой, кто хотя бы раз держал в руках прибор WireScope 350 или Pro, без труда уловит в тестерах Softing и VIAVI знакомые признаки – цветной сенсорный экран со стилусом, «двуухие» гарнитуры с оголовьем, особенности меню и управления... Разработки Agilent не пропали даром. Либо тогдашняя компания PsiberData купила документацию и технологии у Agilent, либо приютила ее инженеров. А может быть, и то и другое.

Семейства приборов WireXpert и Certifier40G/10G и сейчас существуют на рынке, но в Россию их было завезено немного, поскольку в тот период ниша была уже прочно занята продукцией Fluke Networks и в меньшей степени IDEAL Industries.

В середине 2015 г. пользователей Fluke Networks ждал неприятный сюрприз: анализаторы DTX-1800, -1200, -LT и -ELT (т.е. все существовавшие тогда модели) были сняты с производства. Их официально чинили и калибровали до середины 2018 г. (причем калибровка измерительных схем для медных сред выполнялась в Москве на специально привезенном калибраторе), но производитель уже всю продвигал следующее поколение своих приборов – измерительную платформу Versiv с модулями DSX для сертификации медных сред, модулями CertiFiber Pro для сертификации волоконной оптики и рефлектометрическими модулями OptiFiber. Прежнее семейство DTX продолжало соответствовать требованиям стандартов, но тормозило продажи линейки Versiv. Выпуск функционально ограниченной и относительно бюджетной модели DTX-1500 для России и некоторых других стран никого не утешил, тем более что в 2020 г. эти приборы тоже сняли с производства, перестали чинить и калибровать. Старые модели, как водится, некоторое время принимали в зачет покупки новых, но, как и в случае с приборами OMNIScanner от Microtest, на руках у пользователей до сих пор осталось немало приборов DTX.

В 2018 г. многие фирменные производители СКС одобрили для сертификации своих систем тестер еще одного изготовителя – TestPRO CV100 сингапурской компании AEM. Прибор основан на ОС Linux, оба модуля имеют цветной сенсорный экран (резистивные версии комплектовались стилусами; более поздним емкостным экранам стилусы не нужны). Есть варианты комплектации для сертификации медных сред до категории 8 включительно, одномодовой и многомодовой волоконной оптики. Интерфейс русифицирован; в функционале прибора про-



слеживаются наработки не только Agilent Technologies, но и других компаний – возможно, в результате конкурентной борьбы. В итоге на рубеже 2020-х в сфере сертификации СКС в мире и в России было одобрено для использования оборудование пяти ключевых игроков: Fluke Networks, IDEAL Industries (с 2021 г. TREND Networks), Softing, VIAVI и AEM (рис. 3).

### Наши дни и перспектива

Снижение бизнес-активности из-за пандемии затронуло и область тестирования СКС: снизились и продажи приборов, и интенсивность использования ранее проданных. Разумеется, повлиял и уход части зарубежных компаний с нашего рынка, последовавший позже. Но ниша никогда не остается пустой. В начале 2000-х гг. большинство измерений выполнялось приборами OMNIScanner. В последние 10–15 лет наиболее популярными были приборы Fluke. Владельцы измерительного оборудования следили за тем, чтобы вовремя его откалибровать, а уполномоченные сервисные центры оказывали такие услуги. Сейчас на руках остались приборы с истекшим сроком калибровки, поскольку деятельность сервисного центра Fluke Networks в России с декабря 2021 г. фактически свернута. С тестерами других изготовителей ситуация была несколько иной – их изначально калибровали за рубежом, а сейчас эти услуги стали недоступны.

Невозможно экономически обосновать деятельность локального сервисного центра, если продано мало приборов. Она начнет окупаться только после того, как на руках окажется определенная критическая масса оборудования. Но когда ниша занята кем-то другим, создается замкнутый круг: продано мало приборов → сервис-центр экономически невыгоден → продажи без сервиса расти не будут, клиент купит продукцию конкурента. Но сейчас, когда ушедшие компании сами освободили рынок, вопрос

только в том, кто его займет. Кто решится первым – тот и получит доминирующее положение на ближайшие 5–10 лет. Ушедшие компании – не монополисты. На нескольких мероприятиях, прошедших с начала 2023 г. в Москве и других городах, демонстрировались приборы AEM TestPRO. Возможно, мы наблюдаем появление нового лидера на российском рынке тестирования СКС. А может быть, доминирующие позиции займет какой-то другой изготовитель, чьи производственные мощности расположены в Азии. Не исключено и возвращение ушедших лидеров, хотя обрести прежние позиции им вряд ли удастся. Тот, кто сможет наладить сервисное обслуживание, получит все шансы занять рынок сертификации в России.

В любом случае сертифицировать СКС нужно – без этого невозможно убедиться в том, что компоненты кабельной системы собраны верно и обеспечивают должные характеристики передачи. Это ответ на второй вопрос в названии статьи. В 2023 г. многие заказчики от безысходности соглашались принимать результаты измерений приборами, срок калибровки которых истек, но не очень давно. Можно смириться с просрочкой на полгода, максимум год, но дальше доверять результатам таких измерений нельзя. В свое время компания Microtest пыталась увеличить период калибровки с одного года до двух. Однако показания многих приборов на втором году начинали «плыть», и от этой идеи отказались. Даже если тестер постоянно находится в лабораторных условиях и есть некая эталонная линия, на которой можно в любой момент удостовериться, что результаты воспроизводимы, все равно настоятельно рекомендуется выполнять заводскую калибровку раз в год. Если же речь идет о гарантии на установленную кабельную систему, то требовать результаты измерений калиброванным прибором – прямой интерес как поставщиков решений СКС, так и заказчиков. ИКС

▲ Рис. 3. Смена поколений приборов для сертификации СКС

# NTSS ODF PROF – компактность и сверхвысокая плотность портов

В сентябре 2023 г. на форуме «ЦОД» группа компаний EMILINK представила новинку от бренда NTSS – кроссовый шкаф высокой плотности NTSS ODF PROF.

На рынке уже присутствуют шкафы самых разных конструкций, и вы спросите, в чем же исключительность новинки? Шкаф для оптического кроссового оборудования (Optical Distribution Frame, ODF) с высокой плотностью портов от NTSS – практически единственное изделие своего класса на российском рынке, которое производится полностью на территории страны. Что это дает? Возможность быстрого изготовления, реализацию решений любой сложности по требованию заказчика, замену комплектующих в короткие сроки.

## Где нужны ODF-решения

При развертывании СКС в коммерческих зданиях нет необходимости задействовать большие кроссовые поля, но для кабельных систем современных дата-центров они актуальны. В машзалах ЦОДов можно выделить две зоны высокой концентрации коммутационных шнуров. Первая – это главная распределительная система (Main Distribution Area, MDA). Вторая, встречающаяся в ряде проектов, – это зона перекоммутации (распределения, Zone Distribution Area, ZDA), которая находится в области активного оборудования (Equipment Distribution Area, EDA). В этих местах необходимо использовать специальные конструктивы для размещения и коммутации большого количества портов. Как раз таким специальным решением является NTSS ODF PROF.

## Масштабирование кроссового поля

В выпускаемых нами системах NTSS ODF PROF можно достичь плотности 6048 волокон при использовании коннекторов LC на передней панели кроссов. Такая сверхвысокая плотность (Ultra High Density, UHD) достигается в кроссах высотой 42U с размещением 144 волокон на 1U. Изготавливаются



шкафы и других размеров, в том числе высотой до 54U, они обеспечат увеличение и без того впечатляющей емкости.

Привычный способ крепления кроссовых панелей (на 19-дюймовые профили) дает возможность выбирать кроссы по желанию заказчика. Коммутационные шнуры, как правило, идут к активному оборудованию или кроссовому полю активного оборудования в другой шкаф, а при использовании широких шкафов с двумя кроссовыми полями переход в другой шкаф не требуется.

На производстве ГК EMILINK изготавливаются кроссы нескольких конструкций с максимальной плотностью 144 волокна на 1U. Их можно использовать как в качестве кассетных кроссов в составе претерминированных решений для максимального сокращения числа входящих кабелей, так и в качестве решений под сварку для традиционной оконцовки кабеля пигтейлами.

В работе с коммутационными шнурами при столь высокой плотности возникают две проблемы: быстро заполняются органайзеры и неудобно извлекать коннекторы. В таких ситуациях рекомендуется использовать дуплексные коммутационные шнуры Uniboot, в которых два волокна находятся в одном двухмиллиметровом буфере. В кроссах, в которых дуплексные LC-разъемы расположены очень близко друг к другу, необходимо применять специальные коннекторы с системой извлечения Push-Pull Tab, которая помогает извлекать коннектор без риска прервать связь на соседних линках.

Пальцевые органайзеры во всю высоту кроссового поля позволяют отводить коммутационные шнуры от кроссов на лоток, куда они спускаются по специальным органайзерам «грибкам».



Все оптические кабели и коммутационные шнуры, так же как и кроссы с кассетами, изготавливаются на производственных площадках ГК EMILINK в Костроме.

### Универсальность и компактность

Шкафы NTSS ODF PROF полностью отвечают двум важным требованиям: универсальности применения оптических 19-дюймовых кроссов – без ограничений по высоте (числу юнитов, U), типу коннекторов и внутреннему способу подключения оптических волокон – и очень высокой плотности размещения оптических портов, причем как с точки зрения площади, занимаемой в помещении, так и с точки зрения пространства поля коммутации.

Система NTSS ODF PROF представляет собой открытую стойку из алюминиевого каркаса, внутри которой свободно располагаются зона установки 19-дюймового оборудования, зона ввода и организации кабелей, а также зона организации коммутационных шнуров. При этом расположение зон, их регулировку по емкости и глубине можно менять в широких пределах. Направляющие для установки кроссового оборудования могут быть размещены посередине или сдвинуты в одну из сторон шкафа для увеличения зоны коммутационных шнуров. В случае объединения нескольких шкафов возможно более сложное зонирование рабочих полей по назначению и размеру.

Шкаф имеет съемные распашные передние двери. Ручки оборудованы замками. Боковые двери также съемные, везде есть замки. Задняя стенка двойная, при необходимости ее также можно снять или закрыть на замок.

Шкаф имеет щеточные кабельные вводы, размещенные в крыше. Их можно установить и в пол шкафа для организации ввода кабеля снизу. Крепление вводных кабелей про-

исходит в специальном лотке. С помощью пальцевых органайзеров кабели подаются в кроссы сзади или сбоку.

### Гибкость регулировки и легкость модернизации

Специалисты дата-центров отмечают, что применять несколько типовых узкоспециализированных решений для одной категории задач чаще всего не очень удобно. Шкаф NTSS ODF PROF устраняет эту проблему, допуская гибкую регулировку в соответствии с различными требованиями и условиями, возникающими в машзале.

Заложенная в конструкцию ODF-шкафа легкость модернизации, а также наличие большого конструкторского отдела дают возможность быстро переконфигурировать NTSS ODF PROF согласно любому техническому заданию.

Особо отметим, что полная локализация производства в РФ на предприятиях ГК EMILINK позволяет в несколько раз опережать по срокам поставок все известные аналоги. Кроме того, не секрет, что абсолютное большинство предлагавшихся ранее российскими производителями продуктов не могло конкурировать с решениями мирового уровня. NTSS ODF PROF в этом плане – настоящий прорыв для российского рынка. По качеству и функционалу шкаф полностью заменяет аналоги ушедших западных вендоров, при этом его стоимость намного приятнее для заказчика.

Мы всегда стремимся стать лучше – с нами реализуются лучшие решения!



# Дрон на охране картошки, или Цифровизация в агрокомплексе

Николай Носов

Цифровые технологии все активнее проникают в сельское хозяйство. Но недостаток квалифицированных кадров, отсутствие единых стандартов в отрасли, консерватизм фермеров и проблемы импортозамещения тормозят их внедрение.

## Коровник как ЦОД

«Что общего у коровника и ЦОДа?», – вызвал недоумение доклад Systeme Electric в программе онлайн-форума «СМАРТ АГРО. Автоматизированные системы управления агрокомплексом». Какое отношение компания, давно и успешно поставляющая решения для промышленности и ЦОДов, имеет к одной из наименее автоматизированных отраслей российской экономики? Руководитель продуктового маркетинга направления «Автоматизация» Systeme Electric Антон Становских дал ответ – контроллеры и преобразователи частоты Schneider Electric, на основе российского подразделения которой создана носящая созвучное название компания, используются в российском агропромышленном комплексе и поддерживаются Systeme Electric. Да и сама российская компания заинтересована в этом рынке, предлагая для него системы электроснабжения.

В эксплуатации современной животноводческой фермы и ЦОДа немало общего. Одинаково важно поддерживать оптимальный микроклимат, обеспечивать безопасность, без электричества не будут работать средства автоматизации и интернета вещей (рис. 1).

Конечно, на ферме не обязательно дублировать инженерные системы, не так критичны кратковременные перебои с электричеством, но так же используются ИБП, системы мониторинга, кондиционеры и СКУД. Операторы отслеживают показания датчиков температуры, давления и влажности. Есть и своя специфика – животные выделяют газы, в результате разложения мочи и кала в свинарниках накапливает-

ся вредный аммиак, а в ЦОДах датчики концентрации углекислого газа и аммиака не нужны.

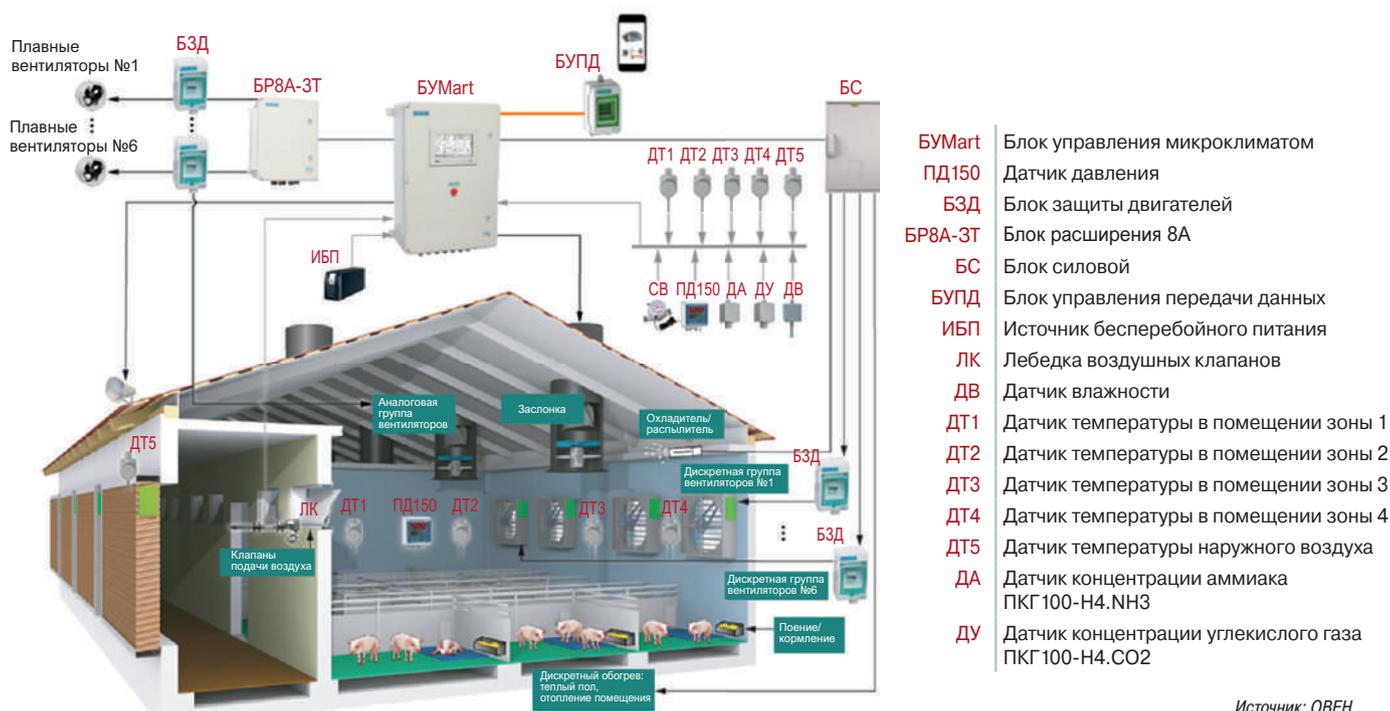
Как и в дата-центре, на ферме стараются минимизировать ручные операции, и успехи есть. Так, максимально автоматизированы процессы на запущенном в первых числах августа в Воронежской области свиноводческом комплексе «Осетровский» компании АГРОЭКО. Современные системы кормления и микроклимата улучшают состояние, поведение и здоровье животных и, соответственно, приносят прибыль.

Для удаленного мониторинга в сельском хозяйстве используются облачные сервисы, например, облачная платформа OwenCloud, разработанная компанией ОВЕН. По словам руководителя направления «Животноводство» компании Константина Кутковского, в облако на одном из российских тепличных комбинатов передаются данные о работе оборудования, через облако меняются его настройки и корректируется температура в помещениях.

## Вторая «зеленая» революция

Эксперты Goldman Sachs считают, что аналоговый период в сельском хозяйстве закончился, отрасль вошла в цифровую эру. Зарождается вторая «зеленая» революция (началом первой считают 1943 г., когда Фонд Рокфеллера запустил программу селекции растений), которая за счет применения цифровых технологий, точного земледелия и интернета вещей способна к 2050 г. увеличить производительность мирового сельского хозяйства на 70%. И это с учетом отсталых экономик третьего мира. Исследователи J'son & Partners Consulting утверждают,

Рис. 1. Система управления микроклиматом в свиноводческом комплексе ▼



Источник: ОВЕН



что инвесторы вкладывают в новый сегмент AgriTech больше, чем в модные FinTech и CleanTech (экологически чистые технологии). Лидируют США, на которые приходится 40% мирового «умного» сельского хозяйства.

Россия отстает, но AgriTech развивается и у нас. На российских фермах уже используются устройства, которые ведут мониторинг температуры тела животных и в случае отклонения от нормы отправляют уведомление на мобильный телефон отвечающего за него работника. IoT-устройства контролируют, сколько корма потребляет свинья или корова, помогают анализировать данные для оптимизации рациона питания, дают возможность отслеживать местоположение скота на пастбищах.

Устройства интернета вещей применяются для мониторинга качества воздуха и воды на фермах. Автоматическое управление инкубаторами позволяет поддерживать внутри заданные температуру и влажность.

### Автоматизация агрокомплекса

В структуру агрокомплекса входят не только мясо-молочные и птицефермы, но и поля, теплицы, производственные цеха, склады, ма-

шинно-транспортные станции, системы энергоснабжения и полива (рис. 2).

И это тоже объекты цифровизации, которая оптимизирует их работу. Современные системы автоматизации собирают информацию с датчиков, счетчиков, видеокamer и дронов и передают на уровень локальной автоматизации – обрабатывающих первичную информацию контроллеров. Далее обработанная первичная информация поступает на уровень диспетчеризации и затем на верхний уровень, где уже работают системы аналитики и ERP.

Данные в центральную диспетчерскую должны оперативно поступать из любой точки этого распределенного по большой площади объекта. Тут не обойтись без технологий беспроводной связи – Wi-Fi, 3G, LTE, LoRa, NB-IoT.

Каждый объект агрокомплекса имеет свою специфику. Так, для тепличного хозяйства и посевов генеральный директор «Дельта Контролс» Михаил Трифонов выделил следующие задачи автоматизации:

- контроль влажности почвы и автоматический полив;
- контроль температуры, влажности и освещенности в теплицах;

Рис. 2. ► Структура агрокомплекса



Источник: «Дельта Контролс»



- учет и оптимизация потребления электроэнергии, воды и тепла;
- контроль сохранности урожая.

СКУД уменьшат кражи помидоров из теплиц, а с помощью дронов диспетчеры выявят и передадут в полицию данные о нарушителях, выкапывающих на поле картошку.

### Каждой ферме – искусственный интеллект

В сельское хозяйство стали внедряться системы с искусственным интеллектом (ИИ). Так, еще в ноябре 2020 г. Сбер сообщил, что разработанная компанией Cognitive Pilot («дочка» Сбера и Cognitive Technologies) система автономного управления сельскохозяйственной техникой с применением ИИ Cognitive Agro Pilot промышленно используется в 35 регионах России. Во время уборки урожая в 2020 г. комбайны с ИИ собрали 590 тыс. т зерновых культур (пшеница, соя, ячмень, овес, гречиха) на площади 130 тыс. га, а также около 130 тыс. т рядковых и валковых культур (кукуруза, подсолнечник) на 30 тыс. га.

В апреле 2023 г. Cognitive Pilot разработала для агроботов технологию нового класса R2D (Robot-to-Driver, взаимодействие робота с водителем), повышающую, по оценкам компании, эффективность уборки на 20–25%.

В 2023 г. Минэкономразвития внесло сельское хозяйство в перечень приоритетных отраслей экономики России для внедрения искусственного интеллекта. По оценкам Национального центра развития искусственного интеллекта при Правительстве России, в условиях массового внедрения ИИ может обеспечить прирост валовой добавленной стоимости к 2025 г. на 25% в растениеводстве и на 13% в животноводстве.

### Проблемы и решения

Отвечая на вопрос нашего издания, К. Кутковский отметил, что по функциональным возможностям отставание российских систем автоматизации для сельского хозяйства от решений ушедших с рынка западных вендоров было, но

его удалось ликвидировать. Более того, эксперт считает, что по некоторым позициям наши аналоги даже впереди. Но вот с элементной базой беда. Даже до СВО российские чипы до сельского хозяйства не доходили, а теперь, в условиях жестких санкций, тем более. Так что полностью зависимость от импортных комплектующих наши вендоры преодолеть не могут.

Среди других проблем цифровизации сельского хозяйства – недостаток квалифицированных кадров, недоступность высокоскоростного интернета в регионах, а также отсутствие стандартизации и координации в отрасли.

Санкции сильно ударили по сельскохозяйственной технике, использующей западные решения с привязкой к сигналу GPS. В марте 2022 г. зарубежные разработчики систем агронавигации объявили об уходе с российского рынка и прекращении обслуживания своих дилерских и клиентских центров. На помощь пришли российские компании. Так, к концу 2022 г. МТС оперативно разработала корректирующее оборудование, повышающее точность позиционирования 190 сельхозмашин в агрохолдинге «Степь» до 2,5 см, что позволило им двигаться по полю на автопилоте. Устройства, установленные на тракторы, посевные комплексы и опрыскиватели, успешно заменили импортные аналоги. Теперь процесс выращивания пшеницы, от сева до уборки, полностью автоматизирован.

Радует, что российские проекты доводятся до стадии промышленной эксплуатации. Ключевая проблема агро-робототехники в мире – коммерциализация результатов исследований и разработок, а также масштабирование проектов. До недавнего времени до 90% участников рынка и стартапов не могли преодолеть эти барьеры.

Многие фермеры не видят необходимости внедрения компьютерных технологий, не готовы тратить деньги на их приобретение и обучение персонала. Инертность людей в отрасли, которая и так очень консервативна, – большая проблема. Но тут уже многое зависит от разъяснительной работы, в том числе в СМИ. **ИКС**

# Сильный, но легкий: K3s – упрощенная версия Kubernetes

**Денис Афанасьев**,  
руководитель  
направления  
облачных  
решений,  
CorpSoft24

**Контейнерный формат разработки и развертывания приложений – стандарт нового времени. Все знают о системе управления контейнерами K8s (Kubernetes), однако существует и K3s – облегченный вариант ее исполнения. В чем различия, преимущества и возможности для пользователей?**

## K8s и K3s: найди 10 различий

K8s (или Kubernetes) и K3s – это инструменты для управления контейнерами, т.е. легковесными автономными ИТ-средами, которые содержат в себе приложение, его зависимости и все необходимые для работы библиотеки и файлы.

Kubernetes (обычно сокращается до K8s, где 8 – количество букв, пропущенных между K и s) – платформа с открытым исходным кодом для автоматизации развертывания, масштабирования и управления контейнеризированными приложениями. K8s – один из наиболее широко используемых оркестраторов контейнеров. Он создан и поддерживается сообществом разработчиков из Google.

Основные особенности Kubernetes:

- позволяет настраивать и расширять функциональность с помощью API и плагинов;
- может масштабировать приложения горизонтально, добавляя или удаляя экземпляры контейнеров на основе нагрузки;
- обеспечивает автоматическое восстановление при сбоях;
- позволяет безопасно хранить конфигурационные данные и секреты и управлять ими.

K3s – упрощенная версия Kubernetes, предназначенная для запуска на ресурсоограниченных окружениях, например, небольших серверах, встраиваемых системах, виртуальных машинах или даже на одноплатном компьютере Raspberry Pi. Она создана проектом Rancher Labs и является легковесной альтернативой полноценному Kubernetes.

Особенности K3s:

- использует меньше системных ресурсов и имеет меньший размер по сравнению с полноценным Kubernetes, поэтому подходит для сред с невысокой производительностью;
- отличается простотой установки и настройки;

- включает в себя легковесный сервер баз данных SQLite, заменяющий отдельную базу данных.

В целом главная разница между двумя K связана с упрощенной структурой и минималистичным подходом K3s к наиболее важным компонентам и функциям. Однако ключевые концепции и возможности Kubernetes в K3s сохранены.

Важная ремарка: общая «легковесность» K3s не означает, что эту версию нельзя использовать в высоконагруженных проектах – вовсе нет, ее можно масштабировать примерно до 20 тыс. хостов. K3s – это тот же оркестратор K8s, из которого «выпилили» все условно ненужное, но основные возможности работают так же.

## Особенности выбора

При выборе между K3s и полной версией Kubernetes важно учесть специфику проекта, доступные ресурсы и предполагаемые сценарии использования. Если вам нужна легкая и удобная платформа для управления контейнеризированными приложениями, но у вас ограниченные ИТ-ресурсы, выбор в пользу K3s будет оптимальным.

K3s подходит для следующих ситуаций:

- развертывание на IoT-устройствах или встроенных системах, где ресурсы процессора и памяти ограничены;
- развертывание контейнеров в локальных средах разработки и тестирования для эффективного распределения ресурсов;
- запуск приложений в облачной или виртуальной среде с ограниченными ресурсами для минимизации операционных затрат.

Говоря о конкретных сценариях, можно выделить следующие:

1. Среда CI/CD. Конвейеры непрерывной интеграции/непрерывного развертывания (CI/CD) часто требуют наличия кластеров Kubernetes

для тестирования и развертывания приложений. K3s можно использовать для создания временных или изолированных кластеров специально для процессов CI/CD.

**2. Одноузловые (one node) развертывания.** K3s можно использовать для запуска Kubernetes на одном узле, в частности, для сценариев, в которых требуется организовать управление контейнерами на одной машине без сложностей, связанных с многоузловым кластером Kubernetes.

**3. Малогабаритные производственные развертывания.** Для небольших приложений или проектов с ограниченными ресурсами K3s может служить экономически эффективным и простым вариантом запуска Kubernetes в производство.

**4. Образовательные цели.** K3s – отличный инструмент для изучения и преподавания концепций Kubernetes, поскольку упрощает процесс развертывания и снижает накладные расходы, связанные с полным кластером Kubernetes.

**5. Удаленные и несоединенные среды.** В сценариях, где сетевое соединение прерывисто или недоступно, K3s можно использовать для создания кластеров Kubernetes на отключенных узлах или в удаленных местах.

**6. Тестирование и эксперименты с Kubernetes.** Если вы хотите поэкспериментировать с различными конфигурациями Kubernetes или протестировать определенные функции, K3s может стать легкой и одноразовой игровой площадкой для тестирования.

### Пример из жизни

Рассмотрим пример использования K3s для реальной бизнес-задачи. У вас есть интернет-магазин, и вы хотите оптимизировать его инфраструктуру, чтобы быстро масштабировать сервисы в ответ на изменения нагрузки, обеспечивая высокую доступность.

Решение: развертывание K3s для оркестрации контейнеров, запускающих микросервисы, на которых работает ваш магазин.

Шаги:

- 1. Подготовка инфраструктуры и установка K3s:**
  - приобретите или арендуйте несколько серверов (или виртуальных машин);
  - установите K3s.
- 2. Настройка кластера:**
  - используйте `kubectl` для создания и развертывания манифестов, которые описывают ваши микросервисы (например, фронтенд, бэкенд, базу данных).
- 3. Мониторинг и логирование:**
  - разверните Prometheus и Grafana для мониторинга метрик;

- разверните Loki или ELK-стек для логирования.

#### 4. CI/CD:

- интегрируйте K3s с вашим CI/CD, чтобы автоматически развертывать новые версии микросервисов при каждом обновлении кода.

#### 5. Масштабирование:

- настройте автоматическое масштабирование подов (групп контейнеров) на основе CPU или других метрик.

#### 6. Бэкапы и обновления:

- создайте стратегию резервного копирования для ваших данных;
- протестируйте обновления K3s и вашего приложения на стенде перед применением в рабочей среде.

#### 7. Тестирование:

- проведите нагрузочное и стресс-тестирование, чтобы убедиться в надежности решения.

#### 8. Пуск в производство:

- после успешного тестирования переведите ваш K3s-кластер в рабочий режим.

Конечные показатели производительности зависят от множества факторов: текущего состояния инфраструктуры, характеристик серверного оборудования, спецификации вашего веб-приложения и т.д. Однако в целом переход на микросервисную архитектуру с использованием K3s может дать следующие результаты:

**Ускорение загрузки страниц.** Улучшенное распределение нагрузки и оптимизация ресурсов ускорят загрузку страниц, ввод данных и проч.

**Увеличение конверсии.** Уменьшение времени простоя и повышение скорости работы сайта могут положительно сказаться на пользовательском опыте, что, в свою очередь, увеличит конверсию.

Конечно, эти плюсы появятся не сами собой, они требуют грамотной настройки и управления. Но в среднесрочной и долгосрочной перспективе переход на такую архитектуру может значительно улучшить производительность и надежность веб-магазина.



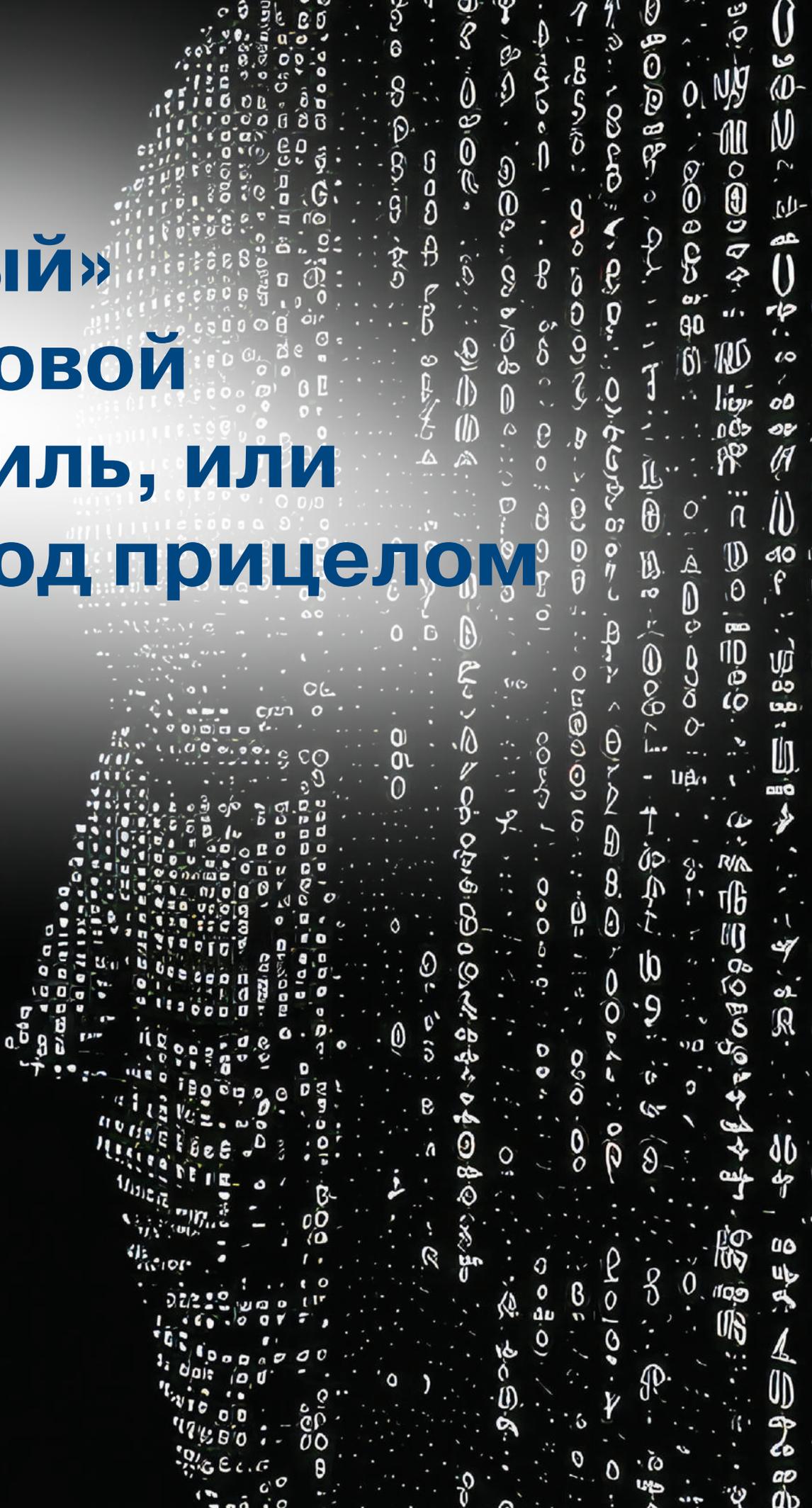
В целом K3s лучше всего подходит для тех случаев, когда важны эффективность использования ресурсов, простота и быстрота развертывания при сохранении мощи и гибкости оркестровки Kubernetes.

Если же у вас большой кластер или вы используете продвинутые функции Kubernetes, то более уместной может оказаться полная версия K8s. Она предлагает широкий спектр функций и развитую экосистему инструментов, которые могут быть полезны в сложных и масштабируемых средах. [ИКС](#)

# «Серый» цифровой профиль, или Все под прицелом

Николай  
Носов

Количество скомпрометированных записей данных в России уже вчетверо превышает ее население. Переломить ситуацию предлагается путем введения института профессиональных операторов персональных данных.



### Число утечек растет

Проникающая во все сферы деятельности человека цифровизация сопровождается лавинообразным ростом числа данных, в том числе представляющих интерес для злоумышленников. За последние полгода число утечек в мире выросло в 2,4 раза и, согласно отчету «Утечки информации ограниченного доступа в мире и России, I полугодие 2023 г.», опубликованному компанией InfoWatch, достигло 5532 (рис. 1). Лидерство по количеству утечек удерживают США – в первой половине 2023 г. экспертно-аналитический центр InfoWatch зарегистрировал 1957 случаев компрометации данных из коммерческих компаний и государственных организаций этой страны. По темпам роста утечек информации впереди Индонезия – там случаев кражи и потери данных стало больше почти в 7 раз. Для сравнения: в государствах Европы и Северной Америки случаев компрометации данных стало больше в 2,5–3 раза.

Лучше дела обстоят в России, которая выдержала первый шквал атак, связанный с началом СВО, и приняла меры по защите государства и бизнеса от киберугроз. По сравнению с I полугодием 2022 г. инцидентов, приведших к компрометации данных, стало меньше на 17,5%. «Не знаю, как это трактовать. То ли все уже украли, то ли мы научились успешно бороться с инцидентами», – прокомментировала полученные оценки президент группы компаний InfoWatch Наталья Касперская.

Основная масса утечек связана с персональными данными (ПДн): сегодня их доля в мире составляет 56,6%, в России – 73,6% (рис. 2). Хотя



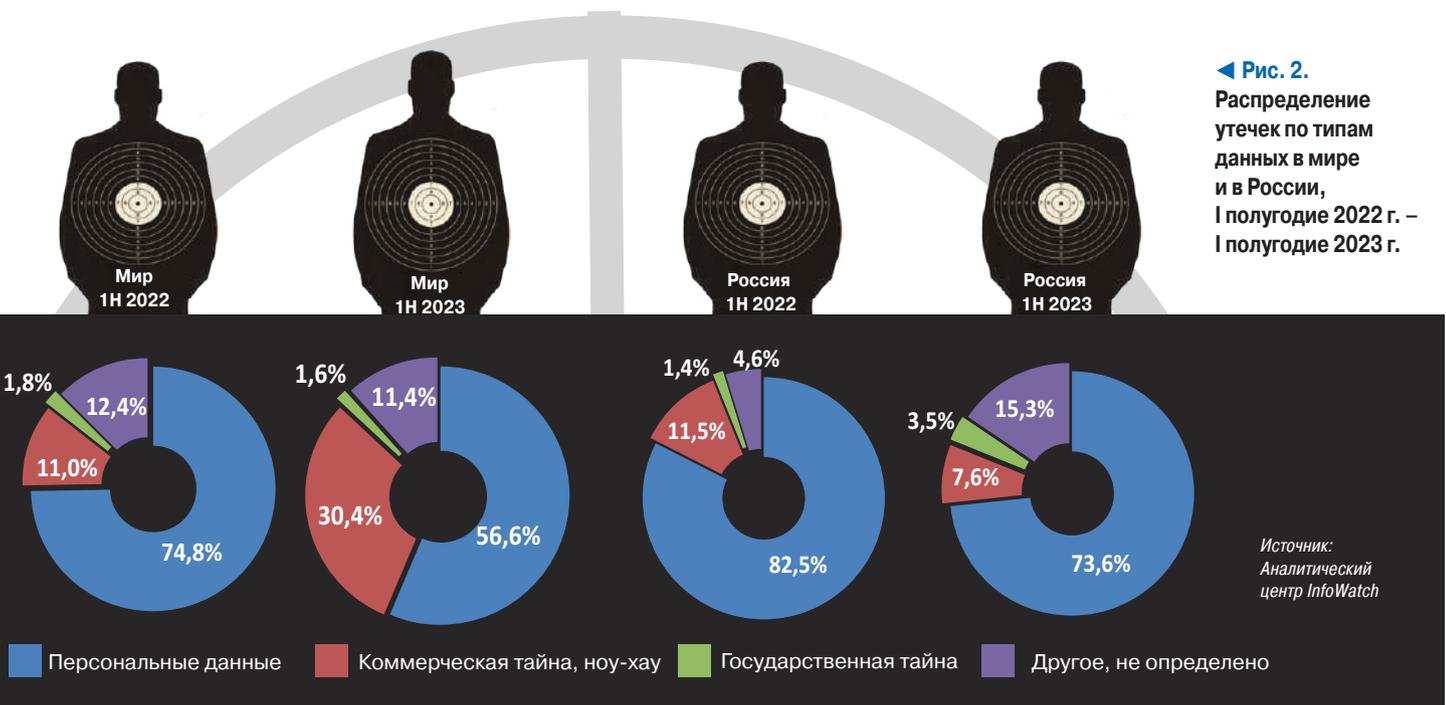
доля утечек ПДн за год уменьшилась (в I полугодии 2022 г. в нашей стране она достигала 82,5%), но утечки стали более масштабными – в I полугодии 2023 г. на одну утечку приходилось компрометация 2,45 млн записей против 1,05 млн записей годом ранее.

▲ Рис. 1. Количество утечек данных в мире и в России

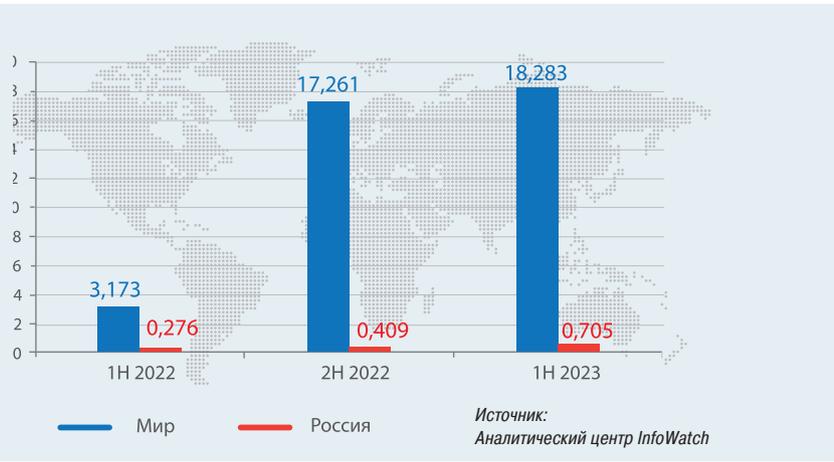
### Нужна ли защита?

В целом количество скомпрометированных записей в России выросло до 705 млн (рис. 3), что более чем вчетверо превышает число жителей страны. Возникает вопрос – стоит ли дальше вкладываться в защиту ПДн, если про нас и так уже знают всё?

Стоит, считают эксперты. «Каждая новая информация обогащает уже существующие базы знаний. Каждая новая утечка дополняет серый цифровой профиль человека», – отметил на конференции BIS Summit 2023 Милош Вагнер, заместитель руководителя Роскомнадзора.



◀ Рис. 2. Распределение утечек по типам данных в мире и в России, I полугодие 2022 г. – I полугодие 2023 г.



**Рис. 3.** ▶  
Количество  
скомпрометиро-  
ванных записей  
ПДн в мире  
и в России, млрд

Преступники используют технологии обработки больших данных для получения подробной информации о потенциальной жертве. Даже опытный специалист по информационной безопасности может попасться на проработанную целевую атаку с помощью фишинга или социальной инженерии, если злоумышленник получит его детализированный профиль.

Заместитель директора ФСТЭК России Виталий Лютиков считает, что значимость утечек преуменьшают в первую очередь операторы персональных данных, которые не видят для себя никаких рисков. Если дело дойдет до штрафов, то они маленькие, а в суд, как правило, никто не подает. А вот для частных лиц риски существенны. Например, из-за утечки паспортных данных злоумышленники смогли убедить близкого В. Лютикову человека перевести деньги. Причем психологическая обработка основывалась на разнообразной информации – паспортных данных, месте жительства, родственниках. Явление стало массовым, мало кто не вспомнит аналогичную историю, происшедшую с родственниками и знакомыми. Особенно беззащитными оказываются представители старшего поколения, привыкшие доверять людям.

По сведениям Центра противодействия киберугрозам Innostage CyberART, в I полугодии 2023 г. большая часть утечек персональных данных сотрудников произошла в компаниях из сферы информационных технологий и ритейла. Кроме того, в открытом доступе оказались персональные данные работников организаций из сферы финансов, страхования, транспорта, ЖКХ, недвижимости, образования, здравоохранения, искусства и госсектора.

«С началом СВО появился и политический аспект. Публикации об утечках проводятся для дестабилизации обстановки в стране», – отметил заместитель министра цифрового развития, связи и массовых коммуникаций Александр Шойтов. При этом часто реальной утечки не происходит, а публикуемые сведения собираются из ранее произошедших утечек и насыщаются данными, которые на самом деле не утекли.

«В России общество активно пользуется информационными ресурсами. Вводятся цифровые паспорта, утечек будет больше, защищаться придется», – подчеркнул Илья Массух, директор Центра компетенций по импортозамещению в сфере ИКТ.

### Изменения в законодательстве

Необходимость ужесточения законодательства в области защиты персональных данных обсуждается в Государственной Думе. По словам председателя комитета Госдумы по информполитике Александра Хинштейна, проект поправок в Кодекс РФ об административных правонарушениях, увеличивающих ответственность за утечки ПДн, уже направлен в Правительство и в заинтересованные ведомства для получения официального отзыва. Разрабатываются и поправки в Уголовный кодекс о наказании за использование утечек персональных данных. Позже стало известно, что правительство проект поправок в КоАП поддержало.

Сейчас максимальная ответственность за утечки ПДн для юридических лиц – штраф до

Мы должны бороться с обесцениванием персональных данных. Говорят о повышении ответственности за утечки персональных данных, но пока это только разговоры. Нужно вводить оборотные штрафы, проводить разбирательства фактов утечек. И главное – выделить персональные данные, разглашение которых действительно наносит ущерб человеку. При текущем состоянии технологий и цифровых сервисов не сможем защитить все.



**Виталий Лютиков,**  
заместитель дирек-  
тора ФСТЭК России

100 тыс. руб. Механизм проведения проверок крайне затруднен. Правительство хотя и сняло мораторий на проверки по утечкам персональных данных, но не в полном объеме.

В новой редакции КоАП ответственность будет варьироваться в зависимости от нанесенного ущерба. Если у юридического лица подверглись утечке до 10 тыс. записей субъектов персональных данных, штраф составит от 3 до 5 млн руб., если 10–100 тыс. записей – 5–10 млн руб., более 100 тыс. записей – 10–15 млн руб.

В случае повторного нарушения предлагает накладывать оборотные штрафы в зависимости от масштабов утечки: минимально – 0,1% выручки за предыдущий год (но не менее 15 млн руб.), максимально – 3% (но не более 500 млн руб.). А. Хинштейн высказал надежду, что законопроект будет рассмотрен уже во время осенней сессии.

Минцифры в рамках закона об оборотных штрафах выдвинуло инициативу о компенсации пострадавшим от утечек персональных данных: если компания, которая допустила утечку, обеспечит финансовое возмещение нанесенного пользователю вреда, это будет признаваться смягчающим обстоятельством. В этом случае к ней будут применяться пониженные оборотные штрафы. Правительство инициативу Минцифры поддержало. Кроме того, в правительстве уверены, что ответственность должна дифференцироваться в зависимости от характера подвергшихся утечке данных и степени нанесенного ею общественного вреда.

С 1 сентября 2022 г. действует положение о том, что оператор, допустивший утечку персональных данных, обязан в течение 24 ч сообщить об этом в Роскомнадзор, а в течение 72 ч предоставить в ведомство результаты внутреннего расследования инцидента с указанием причины и виновных лиц. На сайте Роскомнадзора доступны формы для подачи уведомлений от операторов ПДн. За неупоминание об утечке оператор будет нести административную ответственность.

### Причины утечек

По данным Innostage CyberART, в 32% случаев к утечкам данных приводили халатность и невнимательность работников. Нередко виновни-



**Мы каждый день даем согласие на обработку персональных данных, не понимая, как данные будут сохраняться. Нужно подумать об институте профессиональных операторов персональных данных. Не хранить всем, а передавать на хранение профессиональным операторам хранения персональных данных, чья работа – защитить данные от утечки.**



**Александр Хинштейн,** председатель комитета Госдумы по информполитике

ками утечек становились сами ИТ-специалисты, допустившие, например, ошибки в настройках баз данных. В 12% случаев утечки данных происходили в результате «слива» информации сотрудниками. Еще в 8% случаев причиной утечек данных послужили уязвимости в ИТ-инфраструктуре компаний. Своевременно обнаружить их не удалось из-за недостаточного внимания к вопросам управления уязвимостями и недостаточного уровня защищенности.

При правильно выстроенной системе информационной безопасности защититься от утечек можно. В качестве примера приведем непрерывно атакуемый, но, по словам генерального директора ГК «Солар» Игоря Ляпунова, так и не взломанный портал «Госуслуги». Правда, трудно ожидать, что мелким операторам персональных данных, скажем, гостиницам, поликлиникам или небольшим охранным предприятиям, чьи сотрудники дежурят на проходных, хватит ресурсов для построения аналогичной защиты. А таких организаций много – в настоящее время в реестре Роскомнадзора содержится информация о 920 527 операторах ПДн.

А. Хинштейн выступил с предложением о введении института профессиональных хранителей персональных данных, которые будут предоставлять услугу хранения мелким игрокам по сервисной модели. Если гостинице нужно в соответствии с законодательством зарегистрировать клиента, то пусть передает по защищенному каналу данные профессиональному оператору, который будет нести за них ответственность. И иметь доступ гостиница должна только к записям о своих клиентах: портье в Новосибирске не нужно знать адрес и номер телефона клиента отеля той же сети, но в Москве.

Только тогда защита станет не профанацией, сводящейся к заполнению бумаги о согласии на обработку персональных данных, а реальной мерой, и клиент может быть уверен, что его персональные данные не будут использованы для получения мошенниками кредита или «разводки» его родственников. **ИКС**

# Небезопасные мессенджеры

Николай Носов

**Общение онлайн уверенно вошло в практику современного бизнеса. Но не стоит забывать, что использование мессенджеров и систем видеоконференцсвязи небезопасно и требует применения средств защиты.**

## Шпион в кармане

По мессенджеру позвонила знакомая. Сказала, что нашла в родословной еврейскую бабушку и переехала жить в Израиль. Я опешил: не мог и подумать, что у голубоглазой блондинки есть что-то общее с богоизбранным народом. Высказал надежду, что скоро передумает и вернется, не выдержит жаркого климата и напряжения жизни в постоянно воюющей стране. После окончания разговора стал получать на имеющиеся выход в интернет устройства рекламу с предложением найти еврейские корни для эмиграции в Израиль.

Никогда не интересовался темой эмиграции, в том числе в Израиль. Явно кто-то «слил» разговор рекламным компаниям. Технически это мог сделать оператор связи, хранящий трафик согласно «закону Яровой». Однако в то, что представители большой четверки или спецслужбы по мелочи продают содержание звонков рекламщикам, поверить трудно.

Может «сливать» информацию смартфон, но вендору выгоднее продавать сам продукт, чем подвергать бизнес риску, продавая данные клиента. Поэтому главный подозреваемый – прикладное ПО, прежде всего обеспечивающий общение в онлайн мессенджер. Надо же как-то монетизировать бесплатный продукт. Скорее всего, информация собирается просто по ключевым словам, без глубокого анализа разговора – я же не изъявлял желания перебраться к знакомой.

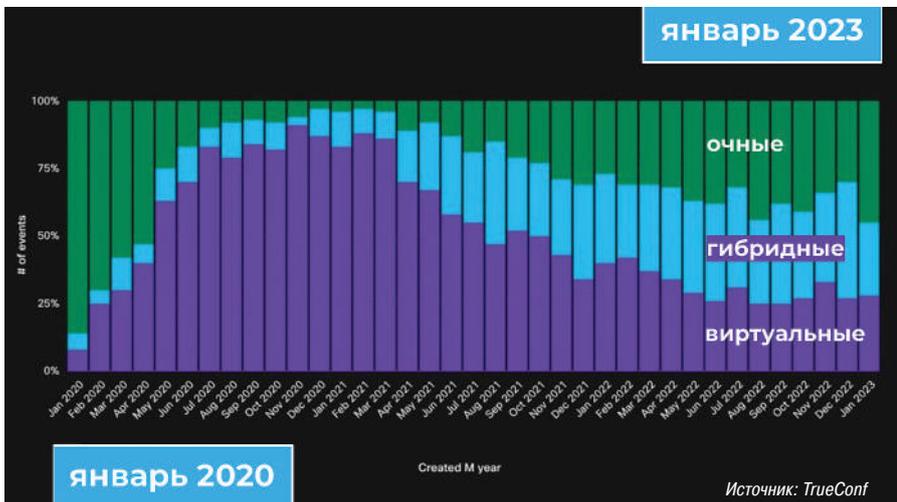
## Все в онлайн

Пандемия привела к буму общения через интернет. Компании экстренно переводили сотрудников на удаленную работу, стоимость акций Zoom взлетела до небес, лишённые возможности личного общения люди начали массово использовать мессенджеры. Удобно и дешево, особенно если принять в расчет стоимость звонков за рубеж. Конференции и совещания тоже перешли в онлайн.

После окончания пандемии, по данным, которые привел директор по развитию компании TrueConf Дмитрий Одинцов, очный формат мероприятий отчасти восстановился, но его доля остается меньше половины. Зато почти треть мероприятий стала проводиться в гибридном формате (рис. 1). В качестве примера можно привести конференции «ИКС-Медиа», которые в разы увеличили число участников за счет подключения онлайн-слушателей. Да и само мероприятие «Видео + Конференции 2023», на котором обсуждались текущие проблемы видеоконференцсвязи (ВКС), прошло в гибридном формате.

Компании и сотрудники оценили преимущества удаленной работы и не спешат с ними расстаться. Опрос менеджеров крупных западных компаний, проведенный Infosys, показал, что 59% менеджеров работают в гибридном или удаленном формате. Перевел сотрудников на гибридный формат работы «Яндекс». По данным портала SuperJob, если потребовать выхода сотрудников в офис, то 40% скорее всего уволятся, а 23% – попросят прибавки к зарплате.

Рис. 1. Формат мероприятий в последние три года ▼



## Опасности ВКС

Удаленная работа несет с собой не только преимущества, но и дополнительные риски, в том числе в области информационной безопасности. По данным Solar, в 2022 г. мессенджеры и системы ВКС стали самыми часто используемыми каналами утечки данных, на них пришлось 33,3% всех утечек.

Риски, связанные с бесплатными зарубежными мессенджерами, можно купировать, перейдя на российские продукты. К этому подталкивает и государство. Роскомнадзор опубликовал список ино-

странных мессенджеров, которые банкам и госкомпаниям запрещено использовать для передачи персональных данных, платежных документов, сведений о счетах и вкладах. Рекомендовано применять отечественные решения.

Но все же две трети утечек происходят из-за человеческого фактора – небрежности или злого умысла сотрудников. И тут импортозамещение не спасет.

Среди рисков – случайная отправка документов не в тот чат или не тому адресату, «слив» информации бывшими сотрудниками, не исключенными после увольнения из корпоративных чатов, намеренная передача конфиденциальной информации сообщнику.

### Организационные и технические меры

Для борьбы с утечками конфиденциальных данных через мессенджеры и системы ВКС целесообразно принять технические и организационные меры: разработать политики безопасности для защиты персональных данных и конфиденциальной информации, положения, регламенты и инструкции. Не просто дать под роспись ознакомиться с требованиями по информационной безопасности, а провести учения и разбор конкретных опасных ситуаций. Это уменьшит количество утечек из-за небрежности и риски атак с использованием средств социальной инженерии. Не стоит забывать о разграничении доступа к конфиденциальной информации, причем с актуальными обновлениями в связи с увольнениями или перемещениями по карьерной лестнице.

Программные и аппаратные средства защиты включают широкий спектр решений – от СКУД до систем защиты информации от несанкционированного доступа и DLP. Современные DLP-системы интегрируются с ВКС, позволяют анализировать видео и звук, фиксировать нажатие клавиш, выявлять нарушения политик безопасности и в режиме реального времени информировать о них администратора. Самые продвинутые интегрируются с системами видеонаблюдения и фиксируют случаи фотографирования экрана на смартфон пользователя.

Старший аналитик Центра продуктов «Дозор» ГК «Солар» Михаил Моисеев рассказал о случае, когда с помощью DLP-системы в трафике мессенджера выявили подозрительные сообщения, а потом установили, что сотрудник компании передавал конкурентам важную информацию о тендере. В результате действий инсайдера конкурент победил. В планах была еще одна такая «акция», которую благодаря контролю утечек удалось предотвратить.

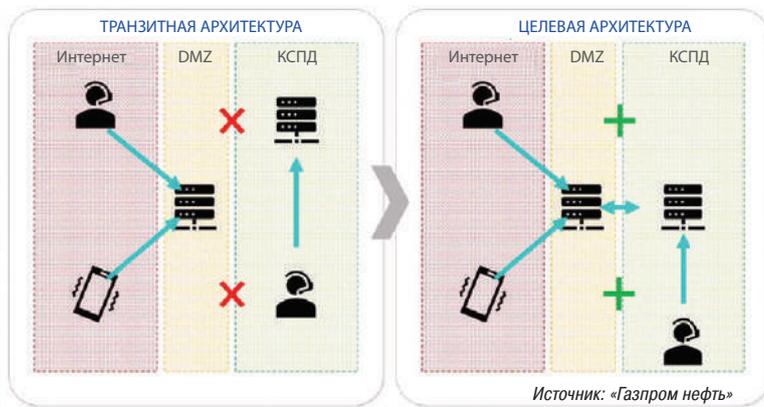
ВКС следует защищать и от внешних воздействий. «В определенных случаях возможны реа-

лизация рисков отказа в обслуживании (DDoS), перехват информации (атака «человек посередине»), утечка чувствительной информации, несанкционированное подключение к конференции, компрометация всего внутреннего сегмента сети», – предостерег сооснователь и ИБ-директор компании Awillix Александр Герасимов. Среди возможных технологических недостатков решений ВКС эксперт выделил следующие: отсутствие сквозного шифрования; отсутствие подтверждения входа в конференцию от организатора; недостаточная фильтрация входящего трафика к внутренним сервисам сервера STUN (Session Traversal Utilities for NAT) в сегменте DMZ и далее от STUN-сервера во внутреннюю сеть. Слабая энтропия уникальной ссылки на конференцию позволяет нарушителю подобрать ее простым перебором, а попавшие в даркнет пароли от других систем – использовать аналогичные для входа в систему ВКС, если она не предусматривает многофакторной аутентификации. В решении должна быть защита и от DDoS-атак.

А. Герасимов привел пример пентеста, проведенного для крупной ИТ-компании, в котором белые хакеры, подобрав перебором ID конференции на одной российской ВКС-платформе, получили доступ к тестовой комнате, обнаружили неправильно сконфигурированный STUN-сервер, проникли во внутреннюю сеть организации и закрепились в ней.

Для обеспечения безопасности системы ВКС эксперт рекомендует использовать стойкие пароли, двухфакторную аутентификацию, функцию «зал ожидания» и по максимуму ограничить возможности гостей. На уровне сервера следует ограничить доступ к внутренним сервисам STUN-сервера и убедиться, что трафик от него идет только в нужные сети, а не попадает, например, в бухгалтерию, которая не использует сервис ВКС. Целесообразно также использовать проху-серверы, балансировщики нагрузки, устанавливать WAF перед доступной через интернет веб-частью системы ВКС. Стоит ограничить доступ к ВКС по геолокации, например, допускать на конференцию только участников с IP-адресами из стран СНГ. Стандартная рекомендация – не забывать своевременно обновлять ПО.

Внедрение ВКС в корпоративную сеть передачи данных (КСПД) стоит проводить постепенно. Например, в компании «Газпром нефть», по словам руководителя портфеля проектов импортозамещения Алексея Нефедова, сначала запустили транзитную архитектуру (рис. 2), не предусматривающую связь с пользователями в КСПД. Только внешние пользователи могли общаться через ВКС. И лишь после проработки всех вопросов обеспечения безопасности стали



▲Рис. 2. Целевая и транзитная архитектуры

переходить на целевую архитектуру, связывающую внешних и внутренних пользователей.

Открытие нового канала между КСПД и сегментом DMZ вызвало опасения ИБ-служб и потребовало тонкой настройки. Были приняты следующие меры: поскольку трафик от расположенного в сегменте DMZ STUN-сервера передается по определенному протоколу, любой другой блокируется. Кроме того, трафик должен идти строго в пользовательский сегмент сети – сотрудникам, использующим ВКС. Такие меры можно рекомендовать для всех подобных случаев.

Также хорошей практикой будет использование пограничного контроллера сессий (Session Border Controller, SBC). SBC устанавливается на границе сети и является единой точкой входа-выхода в домашнюю сеть, благодаря чему скрывается ее топология.

### Защита мобильных устройств

Не стоит забывать о защите удаленных устройств, с которых пользователи подключаются к видеоконференции. Риски снижает переход на российские операционные системы. Выбор ОС для настольных компьютеров широкий – давно и успешно развиваются Astra Linux, ROSA, РЕД ОС, семейство ОС «Альт».

С российскими мобильными операционными системами ситуация хуже, но и она стала исправляться. В 2016 г. Sailfish Mobile OS RUS, созданная компанией «Открытая мобильная платформа» (купленной впоследствии «Ростелекомом») на базе ОС Sailfish финской компании Jolla, прошла сертификацию в ФСБ. В 2019 г. тогда еще единственная российская мобильная операционная система получила русскоязычное название «Аврора». В августе 2022 г. ГК «Астра» представила доработанную ОС Astra Linux Special Edition для мобильных устройств, в том числе планшетов и смартфонов с процессорами на архитектурах ARM, «Эльбрус» и x86-64.

На основе собственного Linux-дистрибутива НТЦ ИТ РОСА разрабатывает мобильную опе-

рационную систему. Выпуск телефонов на базе Rosa Mobile наладят в Зеленограде на производственной линии «Рутек». В продаже российские смартфоны должны появиться уже в конце 2023 г. В июле 2023 г. о планах выпуска собственной операционной системы для компьютеров и смартфонов заявила «Лаборатория Касперского».

Для создания безопасной национальной мобильной платформы нужна не только доверенная мобильная ОС, но и доверенная аппаратная платформа. С российскими процессорами «Эльбрус» и «Байкал» после присоединения Тайваня к антироссийским санкциям ситуация сложная, но остается вариант с микропроцессорами из КНР или стран Юго-Восточной Азии. Главное – наладить их контроль, приемку и сертификацию.

### Хакер – искусственный интеллект

Один из трендов развития ВКС, выделенных Д. Одинцовым, – использование генеративного искусственного интеллекта. В отличие от традиционного ИИ, генеративный может создавать новый контент, включая разговоры, истории, изображения и видео. Генеративный ИИ уже используется в ВКС для создания текста с наиболее важными тезисами проведенной конференции и принятыми решениями.

Новые технологии несут новые риски. В августе нынешнего года Zoom Video Communications обновила условия использования сервиса Zoom, которые требуют от пользователей согласия на предоставление данных для обучения моделей искусственного интеллекта. Компания сможет изменять, распространять, обрабатывать, поддерживать данные, а также делиться ими «для любых целей». Впоследствии в компании уточнили, что данные не будут включать пользовательский контент, но верится в это с трудом.

Аналогичным образом поступают и многие другие онлайн-сервисы ВКС, например, Google Meet. Общая тенденция – анализ содержания разговоров станет более глубоким и рекомендации рекламодателям будут более точными, не только на базе ключевых слов.

Генеративные ИИ могут использовать и злоумышленники: например, на базе собранных данных строить цифровой профиль для проведения целевой фишинговой атаки, в том числе через видеоконференцию, подделывая голос, а то и видеоизображение собеседника. Смогут ли главбух отказать в срочном переводе денег президенту компании, если услышит его голос? А если при этом еще и увидит его на экране?

Без мессенджеров и видеоконференций в современном мире не обойтись. Но надо понимать существующие риски и принимать меры по их минимизации. ИКС

# Защита данных в сети

**Злоумышленники расширяют теневой бизнес, проводят атаки с использованием скомпрометированной информации о пользователях, полученной в результате утечек. Рассмотрим наиболее распространенные угрозы и меры противодействия им.**

имен пользователей на сотни различных сайтов. При этом используется человеческая привычка использовать один и тот же пароль для нескольких учетных записей.

**DDoS.** Распределенные атаки типа «отказ в обслуживании» забивают сервер организации большим количеством запросов, чем он может обработать. Перегружая сервер, атака может увеличить время загрузки веб-страниц и полностью вывести из строя целые веб-сайты, сделать службы приложения недоступными.

## Как организации защититься от сетевых атак

Действия злоумышленников могут привести к реализации недопустимых для организации событий, поэтому прежде всего необходимо оценить, какие бизнес-процессы зависят от работоспособности веб-приложений и как атака на веб-ресурсы может повлиять на деятельность организации и ее клиентов. Мы рекомендуем каждой организации принимать следующие меры защиты.

**Регулярный анализ защищенности приложений и обновление ПО** в соответствии с сообщениями вендоров. Также разумным будет использовать межсетевой экран уровня приложений и внедрить процесс безопасной разработки веб-приложений.

**Использование антивирусного ПО** надежных вендоров, своевременное обновление его. Все подозрительные файлы следует проверять в песочнице – изолированной среде, предназначенной для анализа поведения файлов и выявления вредоносной активности.

**Применение инструментов мониторинга событий ИБ** для обеспечения безопасности целевых и ключевых систем, а также контроль внешних ресурсов – потенциальных точек проникновения.

**Защита личных устройств сотрудников**, если гаджеты используются для подключения к корпоративным ресурсам. Важно своевременно

**Антон Грецкий**, директор по информационной безопасности, ГК ActiveCloud

Общая напряженность в киберпространстве и рынок киберпреступности в 2023–24 гг. продолжат расти. Наибольшее число атак будет направлено на компании, которые предоставляют онлайн-услуги и собирают большие объемы данных о клиентах.

## Самые распространенные атаки на веб-приложения

Есть основания прогнозировать, что в ближайшем будущем общее число кибератак на организации увеличится минимум на 50%. Самыми популярными на данный момент являются четыре типа атак.

**Межсайтовый скриптинг (или XSS).** Злоумышленник внедряет вредоносный код на доверенный веб-сайт, отправляя его пользователю. Предполагая, что код отправителя заслуживает доверия, браузер получателя выполняет его, не проверив, и тем самым предоставляет хакеру доступ к любым записям, которые хранятся в браузере.

**Межсайтовый скриптинг при наличии SQL-инъекции.** Чтобы выполнить запрос пользователя, приложения должны запрашивать свою базу данных контента. Злоумышленник вставляет собственный SQL-запрос на веб-страницу, эффективно заменяя безобидный входной запрос вредоносным. Результат такой атаки – подделка личности, изменение данных, уничтожение данных.

**Заполнение учетных данных** – одна из наиболее распространенных техник захвата учетных записей пользователей. Включает в себя автоматическое внедрение утекших паролей и

информировать сотрудников о новых техниках атак злоумышленников, проводить учения для поддержания осведомленности в вопросах ИБ.

### Что должен делать для защиты от атак каждый сотрудник

Каждый сотрудник компании может внести свой вклад в информационную безопасность организации, обращая внимание на следующие моменты.

**Поведение в социальных сетях и мессенджерах.** Не стоит переходить по подозрительным ссылкам и сообщать собеседнику личную информацию, если нет уверенности в надежности адресата. При загрузке приложения следует проверять информацию о разработчике, внимательно изучать отзывы других пользователей.

**Защита личных данных** достигается применением сетевого экрана, многофакторной аутентификации и мессенджера паролей, своевременным обновлением на устройствах программы безопасности, внимательным отношением к выбору браузера.

**Защита электронной почты** – это прежде всего маркирование и удаление спама, осторожность при использовании адреса электронной почты, соблюдение настроек конфиденциальности email-провайдеров. Не лишними будут и сторонние спам-фильтры.

**Обеспечение сетевой безопасности личных устройств** достигается корректной настройкой безопасности Wi-Fi-роутера, использованием VPN в общедоступной сети Wi-Fi, а также своевременной заботой о сетевой безопасности интернета вещей.

**Безопасность мобильных устройств в интернете** – еще одна важная задача. Каждому сотруднику мы рекомендуем убедиться, что его телефон не прослушивается, отвечать на звонки только с известных номеров, регулярно искать и удалять шпионские приложения, запустить блокировщик вредоносной рекламы. Для повышения конфиденциальности можно заблокировать доступ к веб-камере.

### Безопасный онлайн-банкинг и онлайн-шопинг

Злоумышленники могут встраивать в уязвимые сайты вредоносный код для перехвата данных платежных карт.

**При онлайн-шопинге** убедитесь, что вы совершаете транзакции на защищенном веб-сайте. Его веб-адрес должен начинаться с `https://`, а не с `http://`. Буква «s» означает «безопасный» и указывает на наличие у сайта сертификата безопасности. Слева от адресной строки должен отображаться значок замка. Обращайте внимание на веб-адрес сайта: злоумышленники

часто меняют в веб-адресе несколько букв. Еще одно несложное правило – избегать предоставления финансовой информации при нахождении в публичных сетях Wi-Fi.

**При онлайн-банкинге** используйте надежные пароли и регулярно меняйте их. По возможности используйте многофакторную аутентификацию. Чтобы не стать жертвой фишингового мошенничества, вводите веб-адрес банка напрямую или используйте банковское приложение, но не переходите по ссылкам в сообщениях электронной почты. Регулярно проверяйте выписки по банковским счетам, чтобы выявить непонятные транзакции.

### Что делать, если бизнес все же подвергся кибератаке

Действуйте быстро! Главная цель на данном этапе – остановить атаку и минимизировать ущерб.

**Мобилизуйте команду.** В первую очередь необходимо задействовать сотрудников, которые отвечают за кибербезопасность вашей организации. В идеале члены команды должны обладать необходимыми знаниями и навыками противодействия кибератакам.

**Определите тип кибератаки.** Так вы поймете, на чем сосредоточиться и как лучше нейтрализовать угрозу, чтобы восстановить работу организации. Кроме этого, важно определить наиболее вероятный источник атаки.

**Локализируйте атаку.** Независимо от типа кибератаки рекомендуем незамедлительно отключить зараженную сеть от интернета, отключить удаленный доступ к сети, перенаправить сетевой трафик и сменить все уязвимые пароли.

**Оцените и устраните ущерб.** После локализации атаки необходимо определить, были ли скомпрометированы важные для бизнеса функции, оценить, какие данные могла затронуть атака и к каким системам злоумышленники получили доступ, а также выявить все оставшиеся точки несанкционированного доступа.

**Сообщите об атаке.** В зависимости от вашей юрисдикции может потребоваться уведомить об атаке соответствующие инстанции.

**Уведомите клиентов.** Необходимо сообщить об атаке клиентам, особенно если были затронуты пользовательские данные. Честность и прозрачность помогут компании сохранить доверие клиентов и общественности.

**Выполните работу над ошибками.** После атаки важно провести расследование и определить, что следует улучшить в системах и процессах, чтобы минимизировать риск повторных атак. Воспользуйтесь инцидентом, чтобы повысить уровень кибербезопасности вашей компании. **ИКС**



## Онлайн-ИБП с LiFePO<sub>4</sub>-батареями

Компания «МИКсистем» выпустила ИБП R26C9 двойного преобразования мощностью 1–3 кВА (800 Вт – 2,4 кВт), имеющий универсальную конструкцию для стоечной и напольной установки.

Особенность ИБП R26C9 – использование LiFePO<sub>4</sub>-батарей, которые отличаются почти вдвое большим сроком службы, чем традиционные свинцово-кислотные, устойчивы к протеканию и перегреву и обладают высокой энергетической плотностью, что позволяет сделать ИБП более компактными, чем аналогичные модели с VRLA-аккумуляторами, или увеличить время автономной работы при тех же размерах. Емкость батарейной сборки в R26C9 – до 30 А·ч, ток заряда – 2 А.

ИБП R26C9 обеспечивает защиту от перенапряжения на входе и на выходе, от пониженного напряжения, перегрузки, перегрева, короткого замыкания и низкого напряжения на выходе.

Коэффициент мощности ИБП – 0,8. Диапазон входного напряжения 172–268 В. Коэффициент нелинейных искажений (THD) при линейной нагрузке меньше 3%, при нелинейной – меньше 8%.

Время переключения из режима работы от сети в батарейный режим – 0 мс. Время переключения инвертер – байпас менее 4 мс. Перегрузочная способность в течение не менее 20 с в режиме питания от сети – 130%, в аккумуляторном режиме – 120%.

Интерфейс мониторинга и управления представлен разъемом DB9 с интерфейсом RS-232 и смарт-слотом с поддержкой различных карт расширения, что позволяет использовать интерфейс RS-485, SNMP и другие карты расширения.

[metalkomp.ru](http://metalkomp.ru)



Бизнес-партнер

## Стойка ОСР для высокоэффективного ЦОДа

В рамках развития линейки телекоммуникационных и серверных шкафов, предназначенных для эксплуатации в ЦОДах, компания ДКС разработала и начала поставки на российский рынок серверных стоек, соответствующих стандартам и рекомендациям сообщества ОСР.

При разработке конструкции инженеры ДКС руководствовались требованиями к условиям эксплуатации серверного оборудования в современных энергоэффективных ЦОДах. При этом учитывалась работа систем охлаждения размещаемого в стойках оборудования. В результате получилась оригинальная конструкция, объединившая в себе высокое качество изготовления и эксплуатационные характеристики, удовлетворяющие запросам самой взыскательной службы эксплуатации ЦОДа.

Стойки используются в составе коридоров изоляции холодного воздуха, устанавливаются в ряды с применением систем охлаждения типа free cooling, а также подходят для автономной установки. Стойка позволяет разместить до 48 серверов высотой в один ОСР-юнит.



Предусмотрена возможность энергопитания серверов как постоянным, так и переменным током, в том числе с помощью шинпровода. Конструкция допускает «горячую» замену как блоков питания установленного оборудования, так и самого оборудования, что полностью соответствует требованиям ОСР.

Самое пристальное внимание при разработке было уделено деталям конструкции, их согласованности между собой, технологичности изготовления и сборки. Производство стоек ОСР локализовано на собственном заводе ДКС в Твери. Здесь осуществляется полный цикл производства, сборки и упаковки стойки. Компания ДКС уверена, что новый продукт привлечет внимание владельцев существующих и строящихся дата-центров.

**DKS**  
dkc.ru

**ДКС**  
Тел.: (495) 916-5262  
Факс: (495) 916-5208  
E-mail: info@dkc.ru  
www.dkc.ru ..... с. 79

**НЕД-ЦЕНТР**  
Тел.: (800) 555-8448  
E-mail: ned@air-ned.com  
www.air-ned.com ..... с. 42-43

**СВОБОДНЫЕ ТЕХНОЛОГИИ  
ИНЖИНИРИНГ**  
Тел.: (495) 120-2866  
E-mail: info@sv-tech.ru  
www.sv-tech.ru ..... с. 15, 16-17

**C3 SOLUTIONS**  
Тел.: (495) 133-1717  
E-mail: info@c3solutions.ru  
www.c3solutions.ru ..... 1-я обл.,  
..... с. 22-23

**EKF**  
Тел.: (800) 333-8815  
E-mail: info@ekf.su  
https://ekfgroup.com/..... с. 50-51

**EMILINK GROUP**  
Тел.: (800) 777-1300  
E-mail: info@emilink.ru  
www.emilink.ru ..... с. 62-63

**KEY POINT**  
Тел.: (800) 600-3557  
E-mail: info@dc-keypoint.ru  
www.dc-keypoint.ru ..... 4-я обл.

**SYSMATRIX**  
Тел.: (800) 707-5289  
www.sysmatrix.ru ..... с. 48-49

**SYSTEME ELECTRIC**  
Тел.: (495) 777-9990  
E-mail: ru.ccc@se.com  
www.systeme.ru ..... с. 36-37

## Указатель фирм и организаций

3data . . . . .	4, 12	iKS-Consulting . . . . .	1, 4, 7, 8, 12,	TrueConf . . . . .	74	Минцифры России . . . . .	6, 19, 25, 73
3data HyperScale . . . . .	5	InfoSyst . . . . .	32, 33, 34, 37, 38	Uptime Institute . . . . .	9, 12, 13,	Минэкономразвития . . . . .	67
#CloudMTS . . . . .	14	InfoWatch . . . . .	71	US Conec . . . . .	52, 53, 54, 56	МТС . . . . .	14, 67
ABB . . . . .	33	Innostage CyberART . . . . .	72, 73	Uzinfocom . . . . .	8	МЦРИАП РК . . . . .	11, 12
ГК ActiveCloud . . . . .	77	ITGlobal.com . . . . .	13, 29	Vertiv . . . . .	33, 41	НАГ . . . . .	9
AEM . . . . .	61	ITK . . . . .	9, 10, 57	VIAVI . . . . .	60, 61	Национальный банк	
Agilent Technologies . . . . .	57, 59, 60	ITResearch . . . . .	49	VK . . . . .	28, 30, 31	Казахстана . . . . .	13
Airsys . . . . .	39	IXcellerate . . . . .	6	VMware . . . . .	13, 28, 30	Национальный центр развития	
Akashi . . . . .	13	JDSU . . . . .	60	Wildberries . . . . .	14	искусственного интеллекта при	
Alias Group . . . . .	5	J'son & Partners Consulting . . . . .	65	Ziehl Abegg . . . . .	36, 38	Правительстве России . . . . .	67
Amazon . . . . .	11	Kehua Tech . . . . .	32, 33	Zoom Video Communications . . . . .	74, 76	«НГ-Энерго» . . . . .	34
Amazon Web Services . . . . .	27, 56	Key Point . . . . .	5, 14, 16	ГК «Автодор» . . . . .	31	«Нубес» . . . . .	14
Antarctis . . . . .	41	Legrand . . . . .	57	Агентство инноваций города		ОВЕН . . . . .	65
APC . . . . .	33	Litvinchuk Marketing Agency . . . . .	40	Москвы . . . . .	48	ООО «НЕД-Центр» . . . . .	42
Astergo . . . . .	9, 10	Mail.ru . . . . .	28, 29, 31	Агентство по страхованию		«Открытая мобильная	
Awillix . . . . .	75	Mastercard . . . . .	11	вкладов . . . . .	31	платформа» . . . . .	76
Axiom JDK . . . . .	19	Microsoft . . . . .	28, 29	Агентство регионального развития		«Парус электро» . . . . .	7, 32, 33
C3 Solutions . . . . .	5, 7, 22, 32, 34, 39	Microsoft Azure . . . . .	56	Архангельской области . . . . .	14	ПСМ . . . . .	34
Carel . . . . .	38	Microtest . . . . .	57, 58, 59, 61	АГРОЭКО . . . . .	65	«Рефкул» . . . . .	32, 34, 39, 40
Cisco . . . . .	29	NED . . . . .	39, 40, 43	«Албимак Металл» . . . . .	7	НТЦ ИТ РОСА . . . . .	29, 30, 76
Citigroup . . . . .	11	NetApp . . . . .	10	«Ассоциация операторов ЦОД		Росавтодор . . . . .	31
Cloupard . . . . .	19	Netsystems . . . . .	10	и облачных сервисов РК . . . . .	11, 12	«Росатом» . . . . .	14
Cognitive Pilot . . . . .	67	Netwell . . . . .	30	ГК «Астра» . . . . .	76	Роскомнадзор . . . . .	71, 73, 74
Cognitive Technologies . . . . .	67	Nexenta . . . . .	28	«Атомдата» . . . . .	14	«Росплатформа» . . . . .	28, 29, 30
Coolnet . . . . .	39	Nutanix . . . . .	28, 29, 30	«Атомдата-Иннополис» . . . . .	14	Росстандарт . . . . .	31
Copeland . . . . .	36, 38	Open-E . . . . .	28	«Аэродиск» . . . . .	28, 29, 31	«Ростелеком» . . . . .	76
CorpSoft24 . . . . .	68	Parallels . . . . .	29	«Базис» . . . . .	29	«Ростелеком – ЦОД» . . . . .	5
Danfoss . . . . .	36, 38, 42	PIX Robotics . . . . .	21	Бауманский учебный центр		Роструд . . . . .	25
Datacore . . . . .	28, 29	PNK group . . . . .	4, 5, 40	«Специалист» . . . . .	57	«Росэнергоатом» . . . . .	14
DATARK . . . . .	34	Powercom . . . . .	49	«БРИЗ – Климатические		РУССОФТ . . . . .	20
Dell Technologies . . . . .	28	PS Cloud Services . . . . .	12	системы» . . . . .	38	«Рутек» . . . . .	76
Delta Electronics . . . . .	9, 10, 32, 33	PsiberData . . . . .	60	«БК Цифровые технологии» . . . . .	28, 29	«Рэйдикс» . . . . .	28, 29, 31
DSS . . . . .	8	Rancher Labs . . . . .	68	«Газпром нефть» . . . . .	75, 76	Сбер . . . . .	67
East Telecom . . . . .	8	RCCPA . . . . .	27	НПП «Гиперлайн» . . . . .	34, 57	«Свободные Технологии	
Eaton . . . . .	33	Red Hat . . . . .	28, 29, 30	«Гранд Моторс» . . . . .	34	Инжиниринг» . . . . .	7, 12, 13, 16
Ebm-papst . . . . .	36, 38	RIKEN . . . . .	31	«Дельта Контролс» . . . . .	66	«СДИ Софт» . . . . .	44
EKF . . . . .	50, 51	Schneider Electric . . . . .	7, 9, 10, 12,	ДКС . . . . .	6, 32, 34, 57, 79	«СёрчИнформ» . . . . .	20
ГК EMILINK . . . . .	32, 34, 39, 62, 63	Senko . . . . .	32, 33, 36, 37, 65	«Евролан» . . . . .	34	«СК-СХД» . . . . .	31
ENERGON . . . . .	10	Siemens . . . . .	36, 38	«ИКС-Медиа» . . . . .	4, 8, 11, 38, 74	ГК «Солар» . . . . .	73, 74, 75
Engineering Solutions . . . . .	39	Siemon . . . . .	10, 57	«Итглобалком Рус» . . . . .	13, 29, 30	СОПТ . . . . .	31
Envicool . . . . .	32, 33, 38, 39, 41	Softing . . . . .	60, 61	«Казтелепорт» . . . . .	13	«СХД Баум» . . . . .	29, 31
Fluke Networks . . . . .	57, 58, 59, 60, 61	Soffline . . . . .	19	«КБ Борей» . . . . .	39, 49	«Технофрост» . . . . .	34, 39, 40
FNT Software . . . . .	44	Spectrum . . . . .	40, 43	«Киберпротект» . . . . .	29	«Транстелеком» . . . . .	31
Goldman Sachs . . . . .	65	Stulz . . . . .	39, 40, 41	АНО «Координационный совет		«Узбектелеком» . . . . .	8
Google . . . . .	11, 68	SuperJob . . . . .	74	по ЦОДам и облачным		Университет Инха . . . . .	8
Google Cloud . . . . .	56	SYSMATRIX . . . . .	48, 49	технологиям» . . . . .	14	«Утилекс» . . . . .	9, 34
GreenMDC . . . . .	9, 32	Systeme Electric . . . . .	7, 32, 33,	«Лаборатория Касперского» . . . . .	76	ФСБ . . . . .	76
H3C . . . . .	10	Systemax . . . . .	34, 36, 37, 39, 65	«Марвел Дистрибуция» . . . . .	31	ФСТЭК России . . . . .	72
HPE . . . . .	27, 29	TIA . . . . .	58	«МИКсистем» . . . . .	79	«Хайтед» . . . . .	34
HTS . . . . .	39, 40, 41	TICA . . . . .	39	Министерство экономического		Центр компетенций по импорто-	
Huawei . . . . .	7, 28, 32	TREND Networks . . . . .	61	развития, промышленности и		замещению в сфере ИКТ . . . . .	19, 72
IBS . . . . .	20			науки . . . . .	14	«Шаркс Датацентр» . . . . .	29, 31
IDEAL Industries . . . . .	60, 61			Минтруд . . . . .	25	«Яндекс» . . . . .	6, 74
ГК IEK . . . . .	9						

Учредитель журнала «ИнформКурьер-Связь»:

**ООО «ИКС-МЕДИА»:**

105082, г. Москва, 2-й Ирининский пер, д. 3.;  
Тел.: (495) 150-6424; E-mail: iks@iksmmedia.ru.

# ЦОДЫ, ОФИСЫ, ОБЩЕСТВЕННЫЕ ПРОСТРАНСТВА

9 апреля 2024 ⇄ Москва

**ИКС**  
МЕДИА



СТРУКТУРИРОВАННЫЕ  
КАБЕЛЬНЫЕ  
СИСТЕМЫ



Реклама / 16+

Конференция для профессионалов, занимающихся проектированием, построением и эксплуатацией кабельных систем.

Основная задача конференции – обмен знаниями и наилучшим опытом в области проектирования, построения и эксплуатации кабельных систем. Предполагается рассмотреть основные тенденции в области СКС, новые технологии и технические решения, актуальные вопросы выбора продуктов.

#### В фокусе форума СКС-2024:

- ↳ Российский рынок СКС
- ↳ Основные тенденции в области СКС
- ↳ Особенности кабельных систем для ЦОДов
- ↳ Миграция на высокоскоростные протоколы
- ↳ Эксплуатация кабельных систем

При поддержке



КООРДИНАЦИОННЫЙ СОВЕТ  
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ  
Автономная некоммерческая организация



[cable.iksmedia.ru](http://cable.iksmedia.ru)

# KEY POINT GROUP

## РЕГИОНАЛЬНАЯ СЕТЬ ЦОД ВАЖЕН КАЖДЫЙ!



📍 ВЛАДИВОСТОК	I очередь	<b>440</b> стоек	введен в эксплуатацию - февраль 2023
📍 ВЛАДИВОСТОК	II очередь	<b>440</b> стоек	ввод в эксплуатацию - 1 квартал 2024
📍 НОВОСИБИРСК		<b>880</b> стоек	ввод в эксплуатацию - декабрь 2023
📍 ЕКАТЕРИНБУРГ		<b>300</b> стоек	ввод в эксплуатацию - 1 квартал 2024



keypoint-group.ru