COMNEWS
Цифровая трансформация, ИТ, коммуникации, контент

стандарт

№4-5 (195-196)
апрель-май 2019

Ладонь вместо паспорта

Технологии автоматизированной идентификации личности на основе индивидуальных биологических признаков получают в России все более широкое применение для решения государственных и коммерческих задач

стр. 14

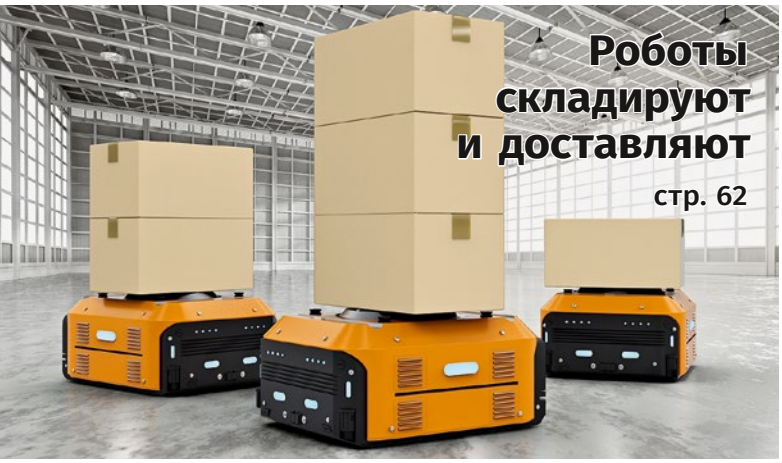
Денис Яклаков, «Сбербанк Лизинг»:

«В вопросах внедрения новых технологий мы исходим из интересов бизнеса»

стр. 18

Персональные данные становятся уязвимее

стр. 70



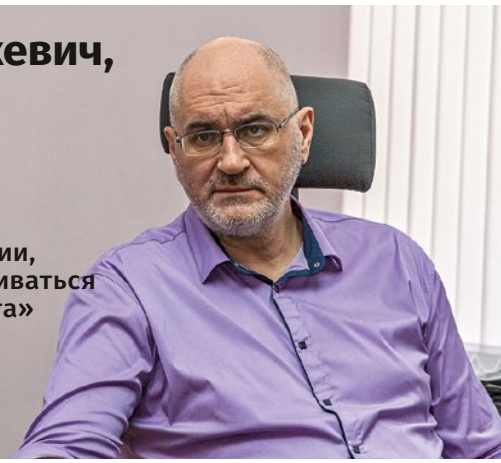
Роботы складируют и доставляют

стр. 62

Игорь Мацкевич, «Итеранет Холдинг»:

«Мы быстрее, чем государственные и крупные компании, способны подстраиваться под задачи клиента»

стр. 42



ISSN 1819-5393
9 771819 539777

Загрузите в App Store

ДОСТУПНО В Google Play

Аналитические карты:

Ключевые коммерческие дата-центры в России

5G: практика

Группа компаний “ГВАРДИЯ-ПЛЮС”

Группа компаний «Гвардия-плюс» основана в 1992 году в Москве. В группу компаний «Гвардия-плюс» входят: ООО «Гвардия-плюс тлк», ООО «Гвардия-плюс телеком», ООО «Порра», ООО «Неоком плюс Гвардия», ООО «Гвардия-плюс инк», ТОО «Гвардия-плюс тлк» (Казахстан).

Компания занимается инжинирингом, проектированием, поставкой, монтажом систем радиосвязи цифровых стандартов TETRA, DMR, GSM-R и LTE, научно-исследовательской и опытно-конструкторской деятельностью. Разработкой и производством радиосредств.

ООО «Гвардия-плюс тлк» с 1996 года является официальным сертифицированным партнером компании Motorola Solutions.

К 2019 году Компания установила более 400 систем разного назначения.

Компания предоставляет услуги подвижной радиосвязи на территории Москвы и Московской области, Санкт-Петербурга, Ленинградской области, Казани и Республики Татарстан, услуги системной интеграции в области широкополосных беспроводных сетей передачи данных. На сегодняшний день в наших операторских сетях более 5000 абонентов в пяти субъектах РФ.

Компания имеет свидетельства НПСРО «Объединение строительных организаций транспортного комплекса» на осуществление изыскательских, проектных и строительных работ объектов связи на всей территории РФ.

Компания выполняет работы на всех этапах проектирования, строительства и эксплуатации систем: от консалтинговых услуг в части получения разрешительной документации на использование радиочастот, разработки, проектирования систем радиосвязи до строительства и сдачи в эксплуатацию, а также гарантийное, послегарантийное обслуживание и сопровождение проектов.

Сервисный центр компании «Гвардия-плюс тлк» сертифицирован компанией Motorola Solutions.

Председатель Совета Директоров
Одинский Александр Леонидович

MOTOROLA SOLUTIONS

Москва, 17-й проезд Марьиной рощи, д. 4, стр. 1, офис 929

Тел.: (495) 618-43-70, (495) 618-42-96

E-mail: info@radios.ru

www.radios.ru www.motovoice.ru

«Умный» город на городские деньги

Фото: СТАНДАРТ

Поднявшаяся было в 2018 году на федеральном уровне тема «умных» городов в России в итоге оставила городские и региональные власти один на один с планированием этих проектов и, главное, с поиском источников финансирования для них.

2 ноября 2018 года стартовал ведомственный проект Минстроя России «Умный город», который возглавил заместитель министра строительства и жилищно-коммунального хозяйства Андрей Чибис. В конце января 2019 года при поддержке «Ростеха», «Росатома» и «Ростелекома» был создан Центр компетенций проекта «Умный город». Его руководителем стала Оксана Демченко, до этого – директор Департамента городской среды Минстроя. А 4 марта 2019 года Андрей Чибис своей подписью утвердил стандарт «Умный город». Журнал «Стандарт» еще в №2/193 в редколонке высказывал сомнения в том, что ведомственный документ на семи страницах может претендовать на статус стандарта, а также отмечал: «Превращение маркетингового термина «умный город» в стандарт грозит сужением круга возможных проектов и их участников, а также формальным исполнением требований нового стандарта вместо решения реальных проблем конкретного города».

В середине марта 2019 года Минстрой с помпой провел в Калуге двухдневный форум «Умный» город. Инструкция по применению», с трибуны которого глава этого министерства Владимир Якушев отрапортовал, что соглашения о реализации проектов «Умный город» подписали 19 городов. Одним из основных обязательств, которые приняли на себя эти пилотные города в рамках соглашений, стало досрочное выполнение стандарта «умного» города, утвержденного Минстроем.

Но не прошло и недели после калужского форума, как 21 марта Андрей Чибис указом президента РФ неожиданно был назначен врио губернатора Мурманской области. Спустя еще неделю, 29 марта, – первым вице-губернатором Мурманской области стала Оксана Демченко. Ведомственный проект и Центр компетенций «Умный город» оказались обезглавленными, и в конце мая продолжают находиться в таком состоянии.

Интерес регионов и муниципалитетов к проекту «Умный город» был связан с надеждой на федеральное финансирование. Хотя внимательные участники рынка еще в середине ноября прошлого года поняли тщетность этой надежды. 18 ноября 2018 года Минстрой опубликовал методические рекомендации по подготовке регионального проекта «Умные города». В разделе «Ресурсное обеспечение проекта» этого документа о возможных федеральных деньгах говорится: «Для финансирования ряда мероприятий проекта привлекаются средства фондов и корпораций развития, включая средства венчурных фондов, фондов развития и научных грантов». О мероприятиях городских администраций четко сказано, что финансовым источником для них должны быть местные бюджеты, а также возможно «привлечение софинансирования со стороны субъекта РФ». Совсем уж издевательски для регионалов звучит следующий совет методических рекомендаций: «Дополнительным источником финансирования могут являться сэкономленные при помощи внедряемых решений и сервисов «Умного города» средства регионального и местного бюджетов». И наконец, следует ключевая фраза: «В целях эффективного расходования бюджетных средств рекомендуется приоритетное привлечение внебюджетных источников финансирования».

Местные бюджеты большинства регионов и городов не позволяют выделять значимые объемы средств на «умные» проекты. При этом все больше муниципалитетов понимают, что цифровые технологии способны повысить эффективность работы властей, комфорт и безопасность горожан, что в свою очередь поможет выиграть глобальную конкуренцию с другими городами за «лучших» жителей – молодых, профессиональных, амбициозных. Поэтому местные чиновники проявляют интерес к механизмам государственно-частного партнерства (ГЧП), но не знают, что может привлечь в проекты «умного» города частных инвесторов и, опять-таки, не готовы расплачиваться с ними из казны.

Но, как сказал еще в 2006 году британский математик Клайв Хамби, «данные – это новая нефть», и города вполне могут расплачиваться с бизнесом муниципальными данными. Это не фантазии: бизнес уже охотно платит за данные. Например, Facebook более трех лет предлагает пользователям по $20 в месяц за установку на смартфон VPN-сервиса Facebook Research, который позволяет отслеживать их активность и привычки. Сбербанк в мае 2019 года предложил упростить для разработчиков технологий искусственного интеллекта доступ к городским данным.

Новые возможности дают и поправки в 224-ФЗ о ГЧП, которые приняли 29 июня 2018 года: дополнительный, 19-й пункт 7-й статьи сделал возможными объектами соглашений о ГЧП программные продукты, оборудование и любые иные объекты ИТ, без необходимости возведения каких-либо зданий и сооружений (прежняя редакция закона абсурдно требовала, чтобы частью ИТ-проекта непременно был объект недвижимости).

Городам не нужно ждать указаний федерального центра и тем более его финансирования для элементов проекта «Умный город». Имея волю и здравый смысл, уже сейчас в любом городе и регионе можно сформулировать проблемы, волнующие жителей и сами власти, найти квалифицированных исполнителей и начать сотрудничество с ними по схеме ГЧП.

Леонид Коник,
главный редактор изданий
группы компаний ComNews

COMNEWS

Содержание

№4-5 (195-196) апрель-май 2019

Анонсы

ЧИТАЙТЕ В ИЮНЬСКОМ ВЫПУСКЕ ЖУРНАЛА «СТАНДАРТ»

- Как идет подготовка дорожных карт по развитию сквозных цифровых технологий
- Что требуется для того, чтобы обеспечить IIoT-системы необходимыми промышленными данными
- В каких областях производства наиболее перспективно использование цифровых двойников
- Каковы перспективы развития рынка промышленной робототехники в России
- Насколько востребована в России услуга по страхованию киберрисков

*Специально для журнала «Стандарт». Авторы колонок выражают личное мнение, которое может не совпадать с редакционным

«ВымпелКом» готов к 5G

ПАО «ВымпелКом» (бренд «Билайн») готово ввести в эксплуатацию новейшую сеть связи 5G-ready в Москве и Московской области в 2020 году. Первая фаза проекта по модернизации сетевой инфраструктуры, которая включает в себя замену всех базовых станций в столице, завершится уже в сентябре этого года. Обновление сети оператора в Москве станет самой масштабной реконструкцией инфраструктуры за всю историю компании.

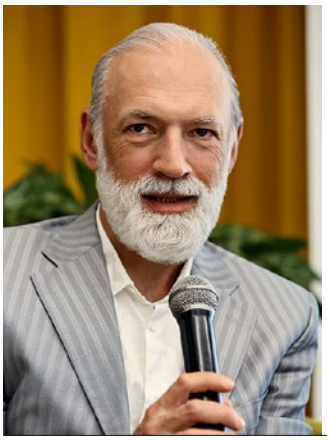


Фото: «ВымпелКом»

Генеральный директор ПАО «ВымпелКом» Василь Лацанич отметил, что оператор реализует в столице программу «Суперсити», важная часть которой – создание качественной, прогрессивной и готовой к внедрению 5G-сети

Как сообщили представители «ВымпелКома», в результате модернизации емкость сети увеличится, а скорость мобильного Интернета вырастет в три раза. Инвестиции компании в обновление столичной сети на первой фазе составляют 5 млрд рублей. Примерно столько же оператор намерен потратить на вторую фазу проекта, завершить которую планируется в 2020 году. На втором этапе предполагается провести финальную доработку сети и подготовку инфраструктуры к внедрению мобильной связи пятого поколения.

В рамках модернизации на всех базовых станциях в диапазонах 1,8 ГГц, 2,1 ГГц и 2,6 ГГц будет реализован режим MIMO 4×4, что значительно улучшит качество покрытия сети, а также увеличит проникновение сигнала и скорость передачи данных. В компании заверяют, что работы по переключению базовых станций будут проходить в ночное время – чтобы минимизировать негативное влияние на абонентов.

По словам генерального директора ПАО «ВымпелКом» Василя Лацанича, оператор поменяет все базовые станции в столице к концу лета. Он рассказал, что сеть 5G в Москве и Московской области готова на 85%. Масштабная работа по ее созданию началась в 2018 году. «Мы долго готовились – тщательно подбирали партнера и модель того, как это сделать, прорабатывали план. Во многом незаметно для клиентов мы уже сменили более 80% наших базовых станций», – говорит глава «ВымпелКома».

Технологическим партнером проекта по модернизации сети оператора выступила компания Huawei. «В Москве мы предложили «ВымпелКому» новейшие технологии, которые помогут оператору создать самую совершенную сеть на российском рынке. Использовав свой международный опыт и мощные локальные ресурсы для интеграции оборудования, Huawei удалось сократить время реализации проекта с трех до полутора лет. Это один из лучших результатов в отрасли», – сказал генеральный директор Huawei в регионе Евразия Эйден У.

В прошлом году «ВымпелКом» совместно с Huawei продемонстрировали возможности сетей пятого поколения: партнеры совершили голографический звонок в сети 5G. Демонстрационная зона была развернута в выставочном зале Музея Москвы. Звонок был совершен в диапазоне частот 26,6-27,2 ГГц с применением очков смешанной реальности (Mixed Reality, MR). Для технического обеспечения звонка использовались базовая станция 5G (gNodeB) Huawei с активной антенной решеткой (HAAU 5213) MIMO 64×64 и абонентский терминал 5G CPE на базе чипсета Huawei Balong 5G01.

Отрасль против инфраструктурного оператора 5G

Рабочая группа «Информационная инфраструктура» АНО «Цифровая экономика» не подала ни одного голоса «за» при голосовании по концепции создания и развития сетей 5G/IMT-2020 в России, подготовленной ФГУП «Научно-исследовательский институт радио» (НИИР) по заказу Министерства цифрового развития, связи и массовых коммуникаций РФ (Минкомсвязи). Ключевая идея документа – создание единого инфраструктурного оператора 5G в диапазоне 3,4-3,8 ГГц.

Голосование по концепции развития сетей пятого поколения (5G) от НИИР, подготовленной по заказу Минкомсвязи РФ, прошло на площадке АНО «Цифровая экономика». Директор по направлению «Информационная инфраструктура» АНО «Цифровая экономика» Дмитрий Марков и пресс-секретарь Минкомсвязи РФ Евгений Новиков подтвердили, что рабочая группа действительно не поддержала предложенную версию концепции.

В концепции рассматривается три сценария развития 5G: преимущественно самостоятельное развитие сетей телекоммуникационными операторами (10-15% совместного использования сетевой инфраструктуры), интенсивное совместное использование активной сетевой инфраструктуры мобильными операторами (50-70% совместного использования сетевой инфраструктуры) и развитие единой национальной сети (единого инфраструктурного оператора). НИИР отдает предпочтение третьему варианту и предлагает его в качестве базового для развертывания сетей 5G в России. В числе преимуществ институт называет экономию капитальных и эксплуатационных затрат и возможность развернуть сеть в кратчайшие сроки.

Источник, близкий к рабочей группе, сообщил, что к позиции НИИР было много подробных замечаний, которые, к сожалению, не были учтены и исправлены. «Сценарий развития сетей 5G, зафиксированный в шестой главе концепции от НИИР, не соответствовал планам и видению рынка, поэтому рабочая группа была категорически против», – говорит источник. Дмитрий Марков пояснил, что к тексту есть два замечания: рабочая группа не согласна с низкой оценкой перспектив диапазона 3,4-3,8 ГГц и с представленной финансовой экономической моделью.

В шестой главе концепции развития сети от НИИР содержится финансовый анализ развертывания сетей связи 5G/IMT-2020. Исходя из практики создания опытных зон, а также из результатов аукционов, наиболее перспективными частотными диапазонами для сетей 5G в концепции названы 3,4-3,8 ГГц и 24,25-29,5 ГГц. Доступными радиочастотными ресурсами для каждого мобильного оператора являются по 50 МГц в диапазоне 3,4-3,8 ГГц и по 400 МГц в диапазоне 24,25-29,5 ГГц (из расчета на минимум четырех операторов). Тогда как оператор единой национальной сети может обеспечить в два раза большую пропускную способность сети радиодоступа (100 МГц) в диапазоне 3,4-3,8 ГГц по сравнению с мобильным оператором.

По оценке НИИР, затраты всей отрасли на развертывание сетей 5G в городах-миллионниках к 2024 году составят 163 млрд рублей при самостоятельном строительстве сети каждым оператором, 114 млрд рублей – в случае совместного использования инфраструктуры и 72 млрд рублей – при создании единого инфраструктурного оператора.

Проведенный институтом анализ показал, что развертывание сетей 5G в России по второму (интенсивное совместное использование активной сетевой инфраструктуры мобильными операторами) и третьему (развитие единой национальной сети) сценариям позволяет сократить общие затраты отрасли на 30-55% по сравнению с первым вариантом (преимущественно самостоятельное развитие сетей телеком-операторами).

Отвечая на вопрос о дальнейшей судьбе концепции, Дмитрий Марков сообщил, что рабочая группа подготовила предложения и надеется, что эти замечания будут учтены. «Мы бы хотели, чтобы представленная НИИР концепция была доработана, и подготовили предложения в третью и шестую главы, – пояснил представитель АНО «Цифровая экономика». – Если они будут приняты, то концепция будет согласована со стороны бизнеса». В третьей главе концепции проведен анализ возможного использования диапазонов радиочастот в полосах 694-790 МГц, 3,4-3,8 ГГц, 4,4-4,99 ГГц, 5,9 ГГц, 24,25-29,5 ГГц, 30-55 ГГц, 66-76 ГГц, 81-86 ГГц при внедрении 5G в России с учетом международных тенденций развития телекоммуникационного рынка.

Ссылаясь на положения о системе управления нацпрограммой «Цифровая экономика РФ», Евгений Новиков сказал, что далее Минкомсвязи проведет согласительное совещание. «Неурегулированные разногласия оформим протоколом, приложим таблицу разногласий и направим все это в президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности», – пояснил он. Президиум комиссии, по словам представителя Минкомсвязи, может вернуть концепцию на доработку. В таком случае ведомство будет дорабатывать ее совместно с НИИР.

Минкомсвязи утвердило концепцию IoT

Министерство цифрового развития, связи и массовых коммуникаций РФ утвердило концепцию по построению узкополосных беспроводных сетей связи Интернета вещей на территории РФ. Концепция разработана в рамках направления «Информационная инфраструктура» нацпрограммы «Цифровая экономика РФ».

Согласно концепции, узкополосные беспроводные сети IoT будут применяться в ЖКХ, логистике, транспорте и промышленности. В лицензируемых полосах радиочастот они представлены тремя стандартами – EC-GSM (900 МГц, 1,8 ГГц), eMTC (также называется LTE-eMTC, диапазоны LTE) и NB-IoT (диапазоны LTE, в том числе 450 МГц, 800 МГц, 900 МГц, 1,8 ГГц, 2,1 ГГц, 2,6 ГГц – FDD). Фактически все три технологии не являются самостоятельными стандартами, а представляют собой развитие существующих стандартов сотовой подвижной связи, которые будут доработаны для удовлетворения потребностей в подключении маломощных устройств.

Согласно концепции, стандарты узкополосных беспроводных сетей связи IoT в нелицензируемых полосах частот можно разделить на две группы. С одной стороны, это набор сверхузкополосных технологий отечественной разработки «Стриж», АО «ГЛОНАСС», NB-Fi, а также технология компании «Альтоника». Они во многом схожи с более распространенной в других странах технологией Sigfox. С другой стороны, это узкополосная технология LoRa (радиоинтерфейс) или LoRaWAN (включает описание протоколов более высоких уровней).

Для приведенных стандартов наиболее востребованными диапазонами радиочастот являются 863-876 МГц и 915-921 МГц. Как указано в документе, с точки зрения радиочастотного обеспечения все технологии за исключением ГЛОНАСС рассматриваются только для безлицензионного использования. Из текста концепции следует, что для АО «ГЛОНАСС» рассматривается гибридная схема, где полосы радиочастот закрепляются за оператором или доверенными операторами в системе «ГЛОНАСС», но их использование данными операторами осуществляется без получения соответствующих разрешений.

Сверхузкополосные технологии во многом ориентированы на бизнес-модель, в которой разработчик реализует функционал агрегатора информации и предоставление сервисов для организаций, которые развернули сеть радиодоступа. При этом сверхузкополосные технологии ориентированы преимущественно на сбор телеметрии с некритических объектов.

Концепцию по заказу Минкомсвязи разработало ООО «Спектрум Менеджмент». «Услуги, которые связаны с Интернетом вещей, подлежат обязательному лицензированию в соответствии с законодательством РФ. Один из определяющих аспектов концепции заключается в том, что сети Интернета вещей должны быть объектом системы СОРМ. Это необходимо для того, чтобы обеспечить их информационную безопасность и управляемость, а также для идентификации физических объектов и процессов», – прокомментировал генеральный директор ООО «Спектрум Менеджмент» Игорь Гурьянов. По его словам, в качестве одного из возможных методов идентификации IoT-устройств предложено рассматривать систему идентификации Digital Object Architecture (DOA), однако окончательное решение о применении того или иного метода должно приниматься на уровне регулятора.

«Цифровая промышленность» обретает контуры

Министерство промышленности и торговли РФ презентовало ведомственный проект «Цифровая промышленность». Министерство собирается поддержать разработчиков цифровых платформ и программных продуктов обрабатывающих отраслей промышленности. Ведомственный проект был представлен на конференции «Цифровая индустрия промышленной России» (ЦИПР-2019), которая проходила в Иннополисе.

Согласно представленной информации, цифровая трансформация промышленности будет иметь три направления. Первое предусматривает создание регуляторной среды. Минпромторг рассчитывает развивать законодательную и нормативно-техническую базы в сфере цифровых технологий и информационные меры господдержки, а также создать программы переподготовки и повышения квалификации для каждой отрасли обрабатывающей промышленности.

Ко второму направлению относятся создание, интеграция и развитие платформ государственной информационной системы промышленности (ГИСП). Предполагается, что в этой системе будет шесть разных платформ: платформа эффективного инвестирования в промышленность, платформа по созданию и развитию производства

6

промышленных предприятий, платформа подбора комплекса мер господдержки, их получения и контроля, платформа обеспечения производства и продвижения промышленной продукции на внутреннем рынке, платформа продвижения продукции на внешнем рынке и увеличения объемов экспорта, платформа анализа и прогноза развития производства на базе объективных статистических данных.

В рамках третьего направления Минпромторг уделит внимание непосредственно цифровой трансформации обрабатывающих отраслей промышленности. Ведомство собирается сформировать центр компетенций, оценить уровень цифровой трансформации обрабатывающей промышленности и выявить проблемы, а также подготовить меры господдержки для стимулирования разработки цифровых платформ, программных продуктов, базовых технологий производства приоритетных электронных компонентов и радиоэлектронной аппаратуры.

На поддержку разработки цифровых платформ и программных продуктов планируют выделить из федерального бюджета 6 млрд рублей в течение трех лет (по 2 млрд рублей ежегодно, начиная с 2019 года). Разработанные цифровые платформы и программные продукты должны функционировать с использованием сквозных цифровых технологий, включенных в состав федерального проекта «Цифровые технологии» национальной программы «Цифровая экономика РФ». Создателям соответствующих решений могут возместить до 50% затрат на разработку при условии их рыночной востребованности у индустриальных заказчиков. При этом срок реализации проекта не должен превышать двух лет. Как сообщил директор Департамента информационных технологий Минпромторга РФ Владимир Дождев, уже летом этого года ведомство планирует запустить первый пробный отбор таких проектов.

Также в презентации «Цифровой промышленности» обозначены меры поддержки проектов, направленных на внедрение цифровых и технологических решений, призванных оптимизировать производственные процессы на предприятии. Распределять субсидии будет Фонд развития промышленности. Владимир Дождев уточнил, что льготное заемное финансирование для таких организаций будет в размере 1% годовых. Размер поддержки будет варьироваться от 20 млн до 500 млн рублей. «Эти деньги пойдут не на разработку, а на внедрение ПАК, комплексов, связанных с 3D- и 4D-печатью, роботизированных комплексов, инженерного ПО», – пояснил представитель Минпромторга. Он добавил, что уже одобрены первые заявки в области машиностроения, двигателестроения, легкой промышленности, индустрии детских товаров.

После того как проект пройдет обсуждение в рабочей группе по цифровой промышленности, летом этого года он будет представлен на рассмотрение в правительство РФ. «Сейчас мы уже реализуем отдельные фрагменты, не дожидаясь финального утверждения проекта. Думаю, что август 2019 года – это точка, когда он обретет полную юридическую силу», – сообщил Владимир Дождев.

В результате реализации данной инициативы Минпромторг рассчитывает увеличить объем выручки проектов на основе сквозных цифровых технологий со 100% в 2020 году до 250% в 2024 году. Кроме того, количество средних и крупных предприятий обрабатывающих отраслей промышленности, прошедших оценку уровня цифровой трансформации (получивших «цифровые паспорта») и подключенных к сервисам ГИСП, должно вырасти с 3,7 тыс. в 2020 году до 14,4 тыс. в 2024 году.

Директор по корпоративным коммуникациям и взаимодействию с органами власти Clover Group Наталия Самойлова предостерегла, что разрозненность платформенных решений может привести к бесполезности собираемых данных. Компания уже ведет работу с Минпромторгом по совершенствованию ГИСП. Наталия Самойлова уверена, что для будущей цифровой трансформации промышленности нужна стандартизация. Заместитель генерального директора корпорации «Галактика» Игорь Целиков полагает, что должны создаваться консорциумы, которые объединят вендоров, разработчиков и заказчиков для закрытия существующих потребностей сторон.

«Газпром нефть» обзавелась «Капитаном»

ПАО «Газпром нефть» запустило цифровую систему управления арктической логистикой. В компании утверждают, что это первая в мире подобная система. Платформа «Капитан» позволяет следить за эффективностью вывоза нефти, которую холдинг добывает на Новопортовском и Приразломном месторождениях.

Фото: «Газпром нефть»

Председатель правления ПАО «Газпром нефть» Александр Дюков подчеркнул, что применение цифровых технологий позволило холдингу повысить эффективность работы в Арктике

Решение дает возможность анализировать информацию об объемах добычи нефти, заполненности хранилищ, местоположении и параметрах движения. Все это позволяет «Газпром нефти» оптимизировать транспортные расходы.

Платформа «Капитан» разработана специалистами «Газпром нефти». Решение функционирует в трех режимах: долгосрочное и оперативное планирование, диспетчеризация арктического флота и аналитика с использованием искусственного интеллекта. Как сообщает пресс-служба холдинга, система значительно сократила сроки планирования и согласования операций по отгрузке нефти.

«Вопрос бесперебойной и эффективной логистики особенно важен для арктических месторождений «Газпром нефти», которые находятся далеко от инфраструктуры. Объемы добычи целиком зависят от своевременного вывоза углеводородов. В результате опытно-промышленной эксплуатации системы «Газпром нефть» добилась снижения затрат на 10%. В перспективе «Капитан» может стать частью комплексного плана по модернизации и расширению магистральной инфраструктуры для увеличения грузопотока по Северному морскому пути», – говорит председатель правления ПАО «Газпром нефть» Александр Дюков.

Функционал «Капитана» позволяет в режиме реального времени анализировать эффективность эксплуатации флота, оценивать скорость движения судов на маршруте, расход топлива, объем загрузки транспорта и предлагать капитанам наиболее безопасные маршруты. Ежедневно система обрабатывает около 7 тыс. параметров и выдает оптимальные логистические решения с горизонтом до трех лет, просчитывая более 1 млн возможных вариантов.

Опыт использования **Siklu EtherHaul 1200** в сети оператора связи

Василий Сипаткин, инженер АО «Кредо-Телеком»

Система передачи данных Siklu EtherHaul 1200 получила широкое распространение среди российских операторов связи как недорогое и высокопроизводительное радиооборудование. Оно используется, как правило, для организации «последней мили» клиенту, подключающему услугу высокоскоростного доступа в Интернет со скоростями от 200 Мбит/с и выше.

Кроме того, мы используем это оборудование для подключения базовых станций 3G/4G к сетям сотовых операторов связи. Очевидно, что данные скоростные радиоканалы используются для передачи трафика интернет-пользователей, а не телефонного трафика.

Также иногда мы используем данное радиооборудование для подключения собственных базовых станций к сети связи «Кредо-Телеком». Это позволяет быстро и недорого организовать ретранслятор для временного подключения клиента к широкополосному Интернету. Пока к объекту прокладывается кабель связи, данное оборудование не имеет себе равных.

Характеристики Siklu EtherHaul 1200

- Диапазон радиочастот: 70-80 ГГц;
- вес: 1ft — 4 кг, 2ft — 9,4 кг;
- размеры: 1ft — 32×22 см, 2ft — 73×46 см;
- энергопотребление: 26 Вт;
- рабочие температуры: от −45°C до +55 °C;
- степень защиты: IP67.

Конструктивно Siklu EtherHaul 1200 представляет собой единый радиомодуль с интегрированной антенной. Такая конфигурация значительно упрощает монтаж.

Существует два типа антенн для Siklu EtherHaul 1200:

— Siklu EtherHaul 1200 1 Ft (31 см) с усилением 43 dBi. Рекомендованное расстояние — до 1,5 тыс. м.

— Siklu EtherHaul 1200 2 Ft (65 см) с усилением 50 dBi. Рекомендованное расстояние — до 4 тыс. м.

Оборудование Siklu EtherHaul 1200 работает в диапазонах радиочастот, не требующих оформления частотных присвоений (решение ГКРЧ №10-07-04-01/10-07-04-02 от 15 июня 2010 года). Это значительно повышает эффективность использования данного вида радиооборудования, особенно для организации каналов связи на ограниченный срок (пока не проложили ВОЛС), что весьма ценно для операторов связи, занимающихся предоставлением высокоскоростного беспроводного доступа в Интернет.

Оборудование Siklu EtherHaul 1200 хорошо зарекомендовало себя не только за городом, но и в плотной городской застройке. Благодаря узконаправленному лучу излучения антенны Siklu EtherHaul 1200 практически не подвержена воздействию помех других радиосистем. Таким образом, на одной базовой станции оператор связи может разместить несколько Siklu, не опасаясь, что они будут мешать друг другу. Для операторов, предоставляющих услуги по радиоканалу, это дает отличную возможность организовать для клиентов высокоскоростной доступ в Интернет (до 400 Мбит/с) за сравнительно небольшую абонентскую плату.

Siklu EtherHaul 1200 имеет два комбопорта и отдельный порт для электропитания. Оборудование поддерживает технологию POE.

Мы пробовали использовать подключение электропитания по технологии POE, но получали нестабильность в работе радиооборудования. Поэтому для более качественной работы линии связи мы подключаем радиооборудование только отдельным кабелем питания.

Блоки питания Siklu EtherHaul 1200 поставляются отдельно от радиооборудования. Поскольку подключение электропитания по POE плохо себя зарекомендовало, мы не покупаем эти блоки питания. Вместо них мы используем блоки питания собственного производства (WOCCOM Systems).

Для передачи данных мы используем оба комбо-порта: один — в режиме UTP, второй — в режиме SFP. Линия UTP выступает как резервная и задействуется для оперативного ремонта.

Справка

До 2008 года российская компания «Вокком Системз» (WOCCOM Systems) занималась производством сначала аналоговых, а потом и цифровых радиорелейных станций WOCCOM DGM. Эти среднескоростные РРС широко использовались провайдерами Интернета для организации магистральных каналов связи, а также для организации «последней мили» для крупных клиентов, подключающих услугу доступа в Интернет. Эти РРС работали в сети связи компании «Кредо-Телеком» вплоть до 2016 года.

В настоящее время WOCCOM Systems производит блоки питания для некоторых видов радиооборудования передачи данных, а также внешние электронные байпасы — устройства для переключения оборудования с ИБП на прямое питание из электросети. Электронные байпасы нужны как в случае поломки ИБП, так и при регламентной замене батарей ИБП. Электронные байпасы, как правило, являются встроенным элементом довольно дорогих ИБП.

На российском рынке представлены только внешние механические байпасы, которые позволяют переключать электропитание оборудования с ИБП на местную электросеть только вручную. Таким образом, при поломке ИБП внешний механический байпас не обеспечивает автоматическое переключение оборудования на питание напрямую из электросети. А электронный байпас позволяет это сделать.

Принимая во внимание отсутствие на российском рынке внешних электронных байпасов, WOCCOM Systems в 2019 году начала производство таких устройств. Оператор, имеющий распределенную сеть связи, может использовать электронные байпасы WOCCOM Systems вместе с бюджетными ИБП. Это позволит существенно сократить время перебоев связи у абонентов.

Место силы

Ксения ПРУДНИКОВА, Яков ШПУНТ

23-26 апреля в столичном «ЭкспоЦентре» прошла Российская неделя высоких технологий (РНВТ), традиционно объединившая несколько выставок, форумов и конференций в сфере информационных технологий, телекоммуникаций, навигации и телематики. В этом году в рамках РНВТ выступили 150 докладчиков, в выставках приняли участие 390 экспонентов из почти двух десятков стран.

Россвязь нацелилась на цифровую экономику

Федеральное агентство связи (Россвязь) в рамках РНВТ провело расширенное совещание, на котором подвело итоги 2018 года и озвучило планы на будущее. В текущем году Россвязь и подведомственные организации сфокусируются на реализации мероприятий в рамках национальной программы «Цифровая экономика РФ».

В ходе расширенного совещания Федерального агентства связи его руководитель Олег Духовницкий напомнил о роли агентства в реализации мероприятий нацпрограммы «Цифровая экономика РФ»

Фото: СТАНДАРТ

В совещании принял участие министр цифрового развития, связи и массовых коммуникаций РФ Константин Носков, который отметил успешную работу ведомства, в том числе в таких направлениях деятельности как устранение цифрового неравенства, подготовка кадров для цифровой экономики, а также восстановление региональных сетей связи, применяемых для оповещения населения о чрезвычайных ситуациях. Министр выразил уверенность в том, что большой опыт и высокий профессионализм сотрудников Россвязи позволят им решать и все будущие задачи.

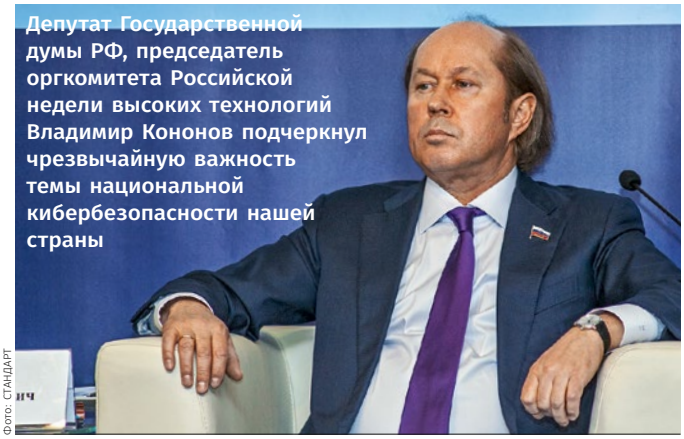
Руководитель Россвязи Олег Духовницкий напомнил, что ведомство принимает участие в реализации федерального проекта «Информационная инфраструктура» в рамках нацпроекта «Цифровая экономика РФ». В частности, агентство отвечает за поддержание работоспособности и наращивание отечественной орбитальной группировки спутников связи и вещания гражданского назначения. В рамках этого направления деятельности в 2018 году подведомственное Россвязи ФГУП «Космическая связь» (ГПКС) начало оказывать телекомуслуги в интересах Центрального банка РФ. Также совместно с ПАО «Ростелеком» ГПКС обеспечило предоставление цифровых услуг связи для Федеральной налоговой службы РФ. На 2019 год запланированы запуски космических аппаратов «Экспресс-80» и «Экспресс-103».

В текущем году Россвязь намерена завершить согласование проекта концепции ФЦП «Развитие орбитальной группировки космических аппаратов связи и вещания гражданского назначения, включая спутники на высокоэллиптических орбитах, для решения задач обеспечения безопасности, государственного управления и развития экономики РФ на 2019-2025 годы». Развитие системы спутниковой связи на высокоэллиптических орбитах является проектом в рамках программы «Цифровая экономика РФ». Перспективная система «Экспресс-РВ» должна решить проблемы со связью в северных, в том числе арктических районах России, для которых характерна плохая наблюдаемость геостационарных спутников. Заместитель руководителя Россвязи Игорь Чурсин отметил, что социально-экономическое развитие арктических регионов идет семимильными шагами и на этом фоне создание группировки «Экспресс-РВ» – логичный шаг. Он подчеркнул, что проект перешел на стадию практической реализации – в частности, высока степень проработки технологического облика космических аппаратов. В ходе презентации проекта «Экспресс-РВ», состоявшейся в дни РНВТ, директор департамента продаж операторских и корпоративных решений ГПКС Михаил Глинка сообщил, что проектирование облика спутников новой группировки завершено. Игорь Чурсин выразил надежду, что ввод в строй спутниковой группировки на высокоэллиптической орбите спровоцирует взрывной рост потребления спутникового ресурса на подвижных объектах. По прогнозам ГПКС, за год количество пассажиров, которые смогут пользоваться возможностями «Экспресс-РВ», составит до 1 млн человек на морских судах, до 12 млн авиапассажиров, до 13 млн человек на поездах дальнего следования, до 25 млн пассажиров междугородных автобусов. Кроме того, каждый год системой смогут пользоваться до 2,5 млн водителей легковых автомобилей и до 1 млн водителей грузовиков. Замглавы Россвязи не исключил перспективы развития в стране спутникового радиовещания после запуска «Экспресс-РВ».

Еще одним направлением деятельности агентства в рамках проекта «Информационная инфраструктура» является разработка генеральной схемы развития систем связи и инфраструктуры хранения и обработки данных на период 2019-2024 годов. Схема должна стать инструментом средне- и долгосрочного планирования, цель которого – повысить эффективность реализации инфраструктурных проектов в сфере связи для государства, государственных компаний, а также компаний с государственным участием. Такое планирование должно учитывать планы развития энергетической и телекоммуникационной инфраструктуры, объемы хранимых данных, а также доступных вычислительных мощностей. Документ должен появиться до конца 2019 года.

Искусственный интеллект отражает атаки

В ходе РНВТ прошел форум «Российский софт: эффективные решения», организатором которого выступили Министерство цифрового развития, связи и массовых коммуникаций РФ, Центр компетенций по импортозамещению в сфере ИКТ, Ассоциация разработчиков программных продуктов «Отечественный софт» и АО «Экспоцентр». Главным вопросом форума стало применение наиболее эффективных отечественных решений для обеспечения информационной безопасности во всех сферах жизни.



Депутат Государственной думы РФ, председатель оргкомитета Российской недели высоких технологий Владимир Кононов подчеркнул чрезвычайную важность темы национальной кибербезопасности нашей страны

Фото: СТАНДАРТ

«В условиях стремительного развития информационных технологий Россия должна за короткое время занять лидирующие позиции в разработке собственных решений для обеспечения безопасности и комфортной жизни населения», – такими словами открыл работу пленарной части форума член комитета Государственной думы РФ по образованию и науке, председатель оргкомитета РНВТ Владимир Кононов.

Заместитель председателя правления ПАО «Сбербанк» Станислав Кузнецов констатировал, что развитие средств безопасности, в том числе информационной, отстает от развития технологий. При этом даже имеющиеся средства внедряются недостаточно активно. В итоге ситуация с угрозами остается крайне напряженной. Главными вызовами Станислав Кузнецов назвал рост мощности атак класса «отказ в обслуживании» (DDoS), взрывной рост утечек, а также сохранение восприимчивости к использованию средств социальной инженерии и фишинга. Долю сотрудников Сбербанка, которые восприимчивы к фишинговым атакам, Станислав Кузнецов оценил в 30%. В итоге уже в этом году мировой ущерб от киберпреступности только в финансовом секторе может составить $2,5 трлн. Причем преступники атакуют не только финансовые организации, но и потребителей их услуг. Что касается Сбербанка, то на его вкладчиков приходится 88% всех посягательств. При этом наиболее уязвимы пожилые люди, которые более внушаемы и хуже осведомлены об угрозах.

«В таких условиях мы просто обязаны выстроить систему защиты», – подчеркнул Станислав Кузнецов. Ее ядром является Центр мониторинга и реагирования на инциденты ИБ (SOC), который Сбербанк построил в 2018 году. Также работает центр мониторинга фрода и мошенничества. Для обработки 4,7 млрд событий в день обе эти системы используют искусственный интеллект, благодаря чему эффективность защиты составляет 98%.

Президент ПАО «Мобильные ТелеСистемы» Алексей Корня назвал задачу защиты кибербезопасности сетей передачи данных, в том числе мобильных, одним из наиболее серьезных глобальных вызовов. При этом, по его словам, если раньше посягательствам подвергались в основном сети операторов, то в последние годы активность киберпреступников сместилась на клиентские устройства и очень серьезным вызовом является защита в сегменте M2M. Глава МТС рассказал, как компания отвечает на эти вызовы: в частности, в МТС работает SOC, активно используются технологии аналитики и искусственного интеллекта. «Ни одна из эпидемий 2017-2018 годов не нанесла ущерба нашим абонентам», – резюмировал Алексей Корня, отметив при этом необходимость международного обмена данными и знаниями, а также предупредив об опасности изоляционизма.

Заместитель руководителя департамента информационных технологий города Москвы Александр Горбатько рассказал, что попытки атак на инфраструктуру столичного ДИТ фиксируются в среднем каждые две секунды, а за второе полугодие 2018 года было отражено без малого 10 млн атак. По словам Александра Горбатько, положение осложняется тем, что внешние пользователи недостаточно внимания уделяют вопросам безопасности. Для того чтобы изменить ситуацию, необходимы программы повышения осведомленности с самым широким охватом – от младших школьников до пенсионеров.

Директор центра компетенций по импортозамещению в сфере ИКТ Илья Массух обратил внимание участников форума на такой риск как политически мотивированное отключение от сервисов и отказ от технической поддержки и сопровождения программных решений, избежать которых помогают меры в области импортозамещения. Илья Массух подчеркнул, что необходимо стимулировать спрос на отечественные программные продукты, а также обозначил глобальный тренд перехода от программно-аппаратных к программным архитектурам.

Сеть как ключевой актив

В рамках конференции «Практика применения цифровых технологий на промышленных предприятиях» прошел круглый стол «Требования к транспортным сетям для промышленных предприятий при реализации задач «Индустрии 4.0».

Участники круглого стола отметили, что цифровая трансформация на предприятиях существенно повышает требования к сетевой инфраструктуре. По словам генерального директора ООО «Т8 НТЦ» Владимира Трещикова, сети связи начинают использоваться для управления сложными объектами, что в свою очередь повышает роль сетевой инфраструктуры.

Главный инженер ООО «Проектинвест» Игорь Кандаков связывает рост объемов трафика со все более широким распространением технологий виртуальной и дополненной реальности. При этом, по его мнению, выбор технологий доступа для промышленных предприятий во многом ограничен, в основном за счет регуляторных требований, которым мобильные сети не удовлетворяют.

Генеральный директор некоммерческого партнерства Центр прикладных исследований компьютерных сетей Руслан Смелянский рассказал об использовании таких подходов как сегментация сетей и дифференциация групп пользователей, а также о применении технологий программно определяемых сетей, которые позволяют снизить сетевые задержки. Среди перспективных решений были особо выделены системы гибкого управления каналом, которые предлагаются в том числе российскими компаниями – например, «Т8 НТЦ».

Заместитель директора по коммерческим вопросам АО «Микран» Егор Гараев рассказал о разработке IoT-устройства, предназначенного для дистанционного измерения температуры контактов в высоковольтных реле по заказу входящего в холдинг «Сибур»

10

АО «Воронежсинтезкаучук». Решение данной задачи осложнялось тем, что предприятие расположено в зоне плотной застройки, что создавало непреодолимые сложности для работы сетей GSM и Wi-Fi, в связи с чем была выбрана сеть LoRaWAN, которая обеспечивала покрытие во всех помещениях, кроме подвальных. Применение данной технологии также позволило сделать IoT-устройство компактным: на его размер сильно повлияли габариты аккумулятора, обеспечивающего работу устройства на срок не менее 5 лет.

Акцент на беспилотный транспорт

В рамках РНВТ прошел XIII Международный навигационный форум. Его основной темой традиционно остается коммерческое использование систем геопозиционирования и спутниковой навигации, прежде всего российской ГЛОНАСС, а также вопросы государственной и международной политики в данной сфере. В текущем году акцент был сделан на применение навигационных технологий в программах по цифровизации, в том числе связанных с развитием беспилотного транспорта.

Сопредседатель Фонда «Сколково» Аркадий Дворкович в приветственном слове участникам форума отметил, что технологии геопозиционирования активно развиваются и широко используются в системах навигации, контроля движения товаров и грузов. Роль государства на этом рынке должна состоять в регулировании и распространении лучших практик. Наиболее чувствительными сферами Аркадий Дворкович назвал развитие отечественной компонентной базы, обеспечение кибербезопасности и выход на внешние рынки.

Спецпредставитель президента РФ по вопросам цифрового и технологического развития Дмитрий Песков также обратил внимание на развитие отечественной компонентной базы. Однако основной акцент в его выступлении был сделан на развитие технологий беспилотного транспорта. По мнению чиновника, у России есть шанс занять достойное место на мировом рынке, но для этого разработчикам навигационных решений необходимо участвовать в работе по созданию международных стандартов, в том числе в области искусственного интеллекта.

Президент НП «ГЛОНАСС», соруководитель рабочей группы НТИ «Автонет» Александр Гурко оценил мировой рынок коммерческих услуг с использованием геопозиционирования в $75 млрд, отметив, что доля России на нем мала, а внутренний рынок развит недостаточно. Александр Гурко подчеркнул: то, что мы уступаем рынок клиентского оборудования иностранным компаниям, является серьезным фактором риска для нашей страны. При этом развитие целого комплекса программ, в том числе «Умный город», а также практика совместного использования автомобилей (каршеринга) будут серьезными драйверами роста данного сегмента.

Глава постоянного представительства Европейского космического агентства в РФ Рене Пишель рассказал о развертывании глобальной навигационной спутниковой системы Galileo, которую агентство развивает совместно с Европейским союзом. Он назвал навигационные сервисы важной частью экономики и высоко оценил накопленный в России опыт применения технологий геопозиционирования для государственных нужд, который ЕС активно перенимает.

Директор департамента автомобильной промышленности и железнодорожного машиностроения Министерства промышленности и торговли России Денис Пак назвал использование беспилотного транспорта одним из главных приоритетов в развитии автотранспорта. Он напомнил о проектах компаний «Яндекс», КАМАЗ, КБ «Аврора», НАМИ и подчеркнул, что для беспилотного транспорта необходима соответствующая инфраструктура, прежде всего телекоммуникационная, а также подготовка нормативной базы. Серьезной проблемой является и недостаточное развитие технологической базы, прежде всего систем машинного зрения и принятия решений. Попытки устранить барьеры на пути широкого применения беспилотного транспорта предпринимает рабочая группа НТИ «Автонет».

Директор практики Arthur D. Little Вадим Панарин обратил внимание участников форума на тот факт, что результаты глобальных опросов демонстрируют снижение доверия широких масс к беспилотному транспорту. По его данным, если в 2015 году на вопрос «Готовы ли вы воспользоваться полностью беспилотным автомобилем?» утвердительно отвечали 64% опрошенных, то в 2018 году – уже 57%. В России уровень доверия к автономным автомобилям еще ниже – всего 51%.

Генеральный директор ООО «Яндекс.Такси» Тигран Худавердян отметил, что эту тенденцию удастся переломить лишь тогда, когда беспилотный транспорт на практике покажет свою безопасность, причем показатели аварийности у автономных машин должны быть на порядок ниже, чем у тех, которыми управляют люди.

РСВО оповестит о ЧС по всем каналам

Подведомственное Федеральному агентству связи (Россвязь) ФГУП «Российские сети вещания и оповещения» (РСВО) анонсировало создание единой платформы оповещения и информирования о чрезвычайных ситуациях. Предприятие выступило с инициативой включить в будущую платформу федеральную систему централизованного оповещения с использованием стандарта эфирного цифрового телевещания DVB-T2, специальные системы оповещения малых населенных пунктов на базе инфраструктуры универсальных услуг связи и системы внутридомового информирования и оповещения.

Функционал красного таксофона расширяется: теперь это не только средство связи, но и оповещения о ЧС

Фото: СТАНДАРТ

В проекте создания единой платформы РСВО планирует задействовать универсальный программно-аппаратный комплекс (УПАК РСВО), который объединит разные системы связи и оборудование для гарантированного экстренного оповещения о чрезвычайных ситуациях (ЧС). Глава Россвязи Олег Духовницкий в ходе расширенного совещания агентства сообщил, что комплекс уже прошел приемо-сдаточные испытания по линии МЧС России, и в данный момент решается вопрос о его вводе в промышленную эксплуатацию.

Заместитель руководителя Россвязи Игорь Чурсин пояснил, что информационно-техническое взаимодействие всех

систем безопасности в РФ не может рассматриваться как единый организм. «На программном уровне разработаны разнородные системы и существуют различные каналы связи. Также многократно дублируются данные об одних и тех же объектах и событиях. Это засоряет информационные системы. Как следствие, в стране отсутствует единая высокопроизводительная телекоммуникационная платформа, объединяющая все автоматизированные системы», – обозначил проблему замглавы агентства.

Заместитель директора по развитию, директор по инновациям РСВО Дмитрий Грицаев предложил унифицировать процесс разработки и проектирования программного и аппаратного сопряжения таких систем. Кроме того, предприятие инициировало включение в создаваемую платформу нескольких дополнительных систем – в частности, федеральной системы централизованного оповещения на базе цифрового стандарта DVB-T2, специальных систем оповещения малых населенных пунктов на базе инфраструктуры универсальных услуг связи и системы внутридомового информирования и оповещения.

В свете перехода России на цифровое телевещание в стандарте DVB-T2 РСВО выступило с инициативой задействовать инфраструктуру цифрового ТВ для оповещения и информирования населения о ЧС. Ведомство рассчитывает создать комплекс программных и технических средств, предназначенных для встраивания данных (сигналов оповещения и информирования о ЧС, специальных информационных сообщений) в телевизионный сигнал для адресного оповещения жителей домовладений, находящихся в зоне покрытия первого и второго мультиплексов.

Внедрять решение РСВО планирует на готовой общероссийской инфраструктуре телерадиовещания ФГУП «Российская телевизионная и радиовещательная сеть» (РТРС) и ФГУП «Космическая связь» (ГПКС) с ее минимальной технической доработкой для использования специальных решений в виде оконечных устройств.

Помимо этого, Россвязь поручила РСВО довести сигналы оповещения о ЧС на базе инфраструктуры универсальных услуг связи (УУС) до малых населенных пунктов с плотностью населения ниже 10 человек на 1 км². По словам Дмитрия Грицаева, данную инициативу уже одобрили руководители Министерства цифрового развития, связи и массовых коммуникаций РФ.

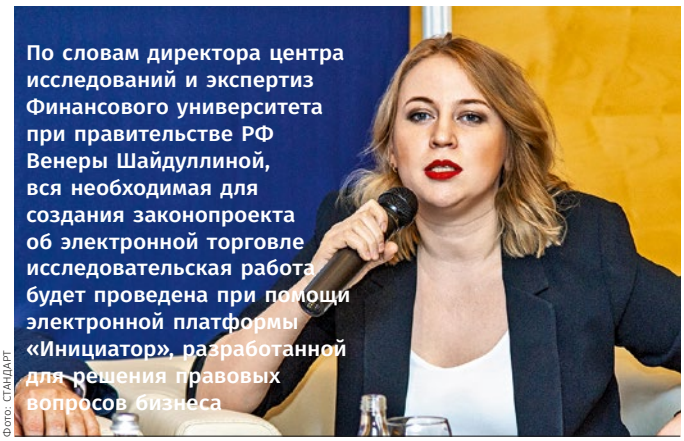
По данным РСВО, в зоне оказания УУС находится более 400 тыс. домохозяйств. Для решения проблемы оповещения и информирования о ЧС ведомство предлагает дооснастить универсальный таксофон оконечным оборудованием, включая устройства связи, усилительное оборудование, рупорные громкоговорители. Зона оповещения одним громкоговорителем мощностью 50 Вт составит 0,2-0,3 км². «Мы хотим превратить таксофон в сосредоточие безопасности удаленного населенного пункта. В принципе все необходимое для этого есть: энергопитание, система резервного питания, телекоммуникационная инфраструктура. Фактически это маленький сельский телепорт», – сказал начальник управления технического развития РСВО Эдуард Шарай. По данным на 2019 год на территории РФ действует свыше 147 тыс. таксофонов.

Кроме того, Эдуард Шарай отметил уязвимость сетей подвижной связи во время ЧС в местах максимальной концентрации населения. В целях минимизации подобных рисков РСВО совместно с профильными департаментами правительства Москвы в 2018 году проработало систему внутридомового информирования (СВИ). Эта система включает в себя три подсистемы: этажное оповещение (на этажах устанавливают громкоговорители), оповещение на придомовых территориях (громкоговорители устанавливают на подъездной группе жилого дома) и поквартирное оповещение (информирование жителей с помощью абонентских трубок подъездных домофонов без их дооснащения). При этом СВИ представляют собой энергонезависимые комплексы, которые действуют на технологической базе сети проводного радиовещания. В Москве такая сеть уже охватывает 90% жилого фонда.

РСВО выступило с предложением взять на себя обязательство обеспечить создание энергонезависимых СВИ в жилом фонде Москвы из собственных средств под гарантии денежных потоков: РСВО готово за свой счет осуществить монтаж и ввод в эксплуатацию СВИ в соответствии с установленным правительством Москвы графиком и адресной программой.

«Инициатор» сформирует закон

В ходе форума «Российский софт: эффективные решения» одной из обсуждаемых тем стала кибербезопасность в сфере электронной коммерции. Как оказалось, здесь накопилось множество проблем, среди которых наиболее острая – высокий уровень мошенничества и потребительского экстремизма.



По словам директора центра исследований и экспертиз Финансового университета при правительстве РФ Венеры Шайдуллиной, вся необходимая для создания законопроекта об электронной торговле исследовательская работа будет проведена при помощи электронной платформы «Инициатор», разработанной для решения правовых вопросов бизнеса

Фото: СТАНДАРТ

Ситуацию в данной сфере научный руководитель факультета прикладной математики и информационных технологий Финансового университета при правительстве РФ Борис Славин сравнил с тем, как если бы из города вдруг полностью ушли все правоохранительные органы и бизнес стал вынужден решать вопросы защиты от посягательств криминала с помощью всех возможных средств, которые удается найти. Однако рынок электронной коммерции уже достиг внушительных размеров, и необходимо навести здесь порядок.

О работе над законодательством в области электронной коммерции подробно рассказала директор центра исследований и экспертиз Финансового университета при правительстве РФ Венера Шайдуллина, отметив, что сейчас приходится решать массу проблем и противоречий, связанных с коллизиями в области международного и частного права, с вопросами налогообложения, защиты персональных данных, правового статуса веб-сайтов. Для облегчения исследовательской работы над законом была создана платформа «Инициатор», которая собирает и анализирует практику разных стран в данной области.

GR-директор Alibaba Сергей Лебедев также подчеркнул важность изучения лучших мировых практик, особенно накопленных на рынках с параметрами, близкими к российским. Среди таких параметров – уровень доходов, предпочтения продавцов и покупателей, шаблоны поведения участников рынка. Сами законы, по мнению Сергея Лебедева, должны создаваться некоммерческими и научными организациями – государственными НИИ, независящими от крупнейших игроков рынка. При этом он подчеркнул, что важно

12

обеспечить баланс между внутренним и трансграничным рынком, чему есть как положительные (США, КНР), так и отрицательные (Белоруссия) примеры.

Борис Славин посоветовал шире использовать услуги внешних центров реагирования на инциденты (SOC/CIRT/CSIRT), где собраны команды экспертов и отработаны механизмы контроля угроз, в том числе с использованием искусственного интеллекта. По мнению представителя Финансового университета при правительстве РФ, главной задачей при этом должна быть защита от неправомерного использования персональных данных.

Кадровый вопрос

Участники форума Международной академии связи обсудили развитие национальной системы квалификации в условиях формирования цифровой экономики. В ходе пленарной дискуссии обсуждался целый комплекс актуальных проблем, стоящих перед отраслью связи и сферой образования – как среднего, так и высшего.

Открывая дискуссию, вице-президент Международной академии связи, председатель Профсоюза работников связи России Анатолий Назейкин отметил, что цифровизация необходима для повышения производительности труда, а значит, и конкурентоспособности страны. Обратной стороной данного процесса, по его словам, является сокращение рабочих мест, что уже становится заметно. К примеру, автоматизация учета привела к тому, что количество бухгалтеров снизилось втрое. Решить эту проблему помогла бы разработка программ по профессиональной переподготовке, но их нет, что грозит серьезными социальными проблемами.

Начальник отдела образования управления финансово-экономической и образовательной деятельности Федерального агентства связи Жанна Скрипкина отметила, что цифровая трансформация экономики невозможна без квалифицированных кадров. «Рынок труда мобильный, новые профессии постоянно появляются, при этом уходят старые. В таких условиях необходимо сильное открытое образование, появление которого невозможно без устойчивого диалога между работодателями и образовательными учреждениями», – убеждена она.

Первый заместитель генерального директора АНО «Национальное агентство развития квалификаций» (НАРК) Юлия Смирнова, сославшись на Росстат, оценила долю неквалифицированных работников на российском рынке труда в 35%. По ее словам, задача повышения уровня квалификации в России стоит весьма остро, и национальная система квалификаций призвана снизить издержки при переходе человека из системы образования в систему труда, а также с одного уровня квалификации на другой. Это помогает человеку быстрее перестроиться в тех случаях, когда в этом возникает необходимость. «Работники отрасли связи как никто другой понимают, насколько важен темп изменений, – считает Юлия Смирнова. – Мы стараемся сделать так, чтобы этот темп ускорялся. Созданы нормативные, методические, организационные и цифровые условия для использования инструментов национальной системы квалификаций, а значит, и для ускорения всех процессов». Юлия Смирнова также проинформировала участников форума о том, что за период с 15 по 21 апреля 2019 года количество людей, прошедших независимую оценку квалификаций, увеличилось на 2 тыс. человек по сравнению с аналогичным периодом предыдущего месяца. Кроме того, разрабатывается стратегия развития национальной системы квалификаций до 2030 года.

Заместитель председателя Совета по профессиональным квалификациям в области телекоммуникаций, почтовой связи и радиотехники (СПК связи), директор направления ПАО «Ростелеком» Юрий Мельников рассказал о разработке проекта отраслевой рамки квалификаций в области телекоммуникаций и радиотехники: «Сложность заключается в том, что в отрасли до сих пор используется терминология 1990-х годов, так что вузы и работодатели порой не могут найти общий язык, чтобы сформулировать требования к квалификации работников. Отраслевая рамка необходима, так как является одним из механизмов сопряжения рынка труда и системы образования, и она должна быть динамичной».

Проректор МТУСИ Андрей Муханов призвал к тому, чтобы система образования становилась более гибкой, и это должно найти отражение в нормативной базе. В качестве положительного примера он привел цифровых кураторов, которых готовит общество «Знание».

Заместитель председателя Комитета по образованию и науке Государственной думы РФ, председатель российского общества «Знание» Любовь Духанина рассказала о работе над законопроектом о совершенствовании подготовки обучающихся, поскольку работодатели хотят видеть больше практических навыков у выпускников системы профессионального образования. Она также призвала к тому, чтобы студенты учились актуальным технологиям. По ее словам, устаревшие программы демотивируют учащихся. В завершении дискуссии Любовь Духанина подчеркнула важность оценки сквозных квалификаций и предложила найти ее оптимальную модель, которая устроит всех.

Требования избыточные и противоречивые

Ключевым мероприятием конференции «Практика применения цифровых технологий на промышленных предприятиях» стал круглый стол «Доверенная информационная среда, созданная на базе отечественных критических технологий, – основа для национальной цифровой инфраструктуры».

Главной задачей круглого стола, как подчеркнула его модератор, заместитель генерального директора, руководитель спецпроектов АО ПО «Молния» Алла Морозова, стало знакомство российских компаний, занятых выпуском оборонной продукции и оборудования двойного назначения, с имеющимися отечественными программными и аппаратными системами, предназначенными для создания цифровой инфраструктуры. Такие системы позволяют решить целый комплекс проблем, включая зависимость от иностранных технологий и эксплуатацию разного рода уязвимостей.

Первый заместитель генерального директора ООО «ЭОС актив», председатель контрольно-ревизионной комиссии ассоциации разработчиков программных продуктов «Отечественный софт» Алексей Мальков рассказал, что уже созданы типизированные стеки из отечественных программных и аппаратных продуктов, ориентированные на решение широкого спектра задач. По его оценке, ситуации в разных классах ПО заметно отличаются друг от друга: в таком сегменте как решения для информационной безопасности отечественные продукты имеют существенное преимущество перед зарубежными; в сегменте ПО для автоматизации бизнес-процессов достигнут паритет, причем у российских продуктов есть все шансы уже в ближайшем будущем занять лидирующее положение; среди офисных редакторов до сих пор подавляющее преимущество – у зарубежного продукта, а именно у Microsoft Office.

Участники круглого стола вскрыли немало проблем. Так, директор НПЦ «Орион» Юрий Софьянников обратил внимание на то обстоятельство, что даже самые элитные российские силовые подразделения используют системы связи иностранного производства, часто устаревшие. В итоге обеспечение скрытной и помехоустойчивой связи

становится сложной задачей, решение которой затрудняет затянувшийся кризис в отечественной радиопромышленности. При этом до сих пор за российскую выдается по факту зарубежная продукция.

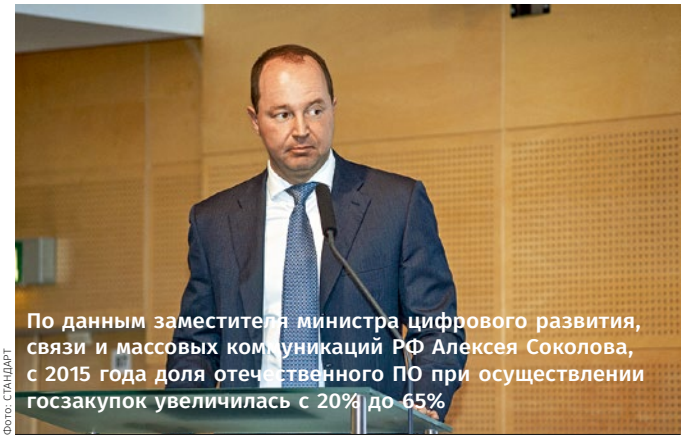
Помощник генерального директора АО «МЦСТ» Константин Трушкин рассказал о препятствиях, которые испытывают разработчики отечественных процессоров. По его словам, процессоры «Эльбрус» приходится производить за рубежом, и это обстоятельство лишает их преимуществ при закупках. «С формальной точки зрения «Эльбрусы» являются точно такими же зарубежными продуктами как платформы от Intel или AMD, и к тому же стоят дороже», – отметил Константин Трушкин и предложил распространить преференции для отечественной продукции на изделия, дизайн которых создан в России.

Генеральный директор группы компаний «Сторус» Александр Чичковский констатировал полное отсутствие внимания государства к такой сфере как суперкомпьютеры, без которых невозможно решение целого комплекса задач, связанных с моделированием в разных областях, включая разработку авиационной, космической, автомобильной техники, разведку месторождений нефти и газа, точное прогнозирование погоды. При этом отставание от передовых стран за последние годы ощутимо увеличивается. По словам Александра Чичковского, если в 2016 году отставание России от США составляло около 5 лет, то по итогам 2018 года оно превысило 11 лет.

Генеральный директор ООО «Базальт СПО», член правления ассоциации разработчиков программных продуктов «Отечественный софт» Алексей Смирнов обратил внимание, что до сих пор не преодолены противоречия, связанные с критериями оценки происхождения ПО, между постановлениями правительства №719 и №1236. При этом требованиям, которые предъявляются к офисному ПО согласно постановлению №325, не удовлетворяет ни один из представленных на российском рынке продуктов.

Итоги и новые планы

До конца текущего года в компаниях с госучастием долю отечественных программ планируется довести до 45%. По планам Министерства цифрового развития, связи и массовых коммуникаций РФ, к 2024 году российским будет 70% ПО, закупаемого госкомпаниями, и 90% ПО, закупаемого госучреждениями.



По данным заместителя министра цифрового развития, связи и массовых коммуникаций РФ Алексея Соколова, с 2015 года доля отечественного ПО при осуществлении госзакупок увеличилась с 20% до 65%

Фото: СТАНДАРТ

Такие прогнозы озвучил заместитель министра цифрового развития, связи и массовых коммуникаций РФ Алексей Соколов в своем выступлении на форуме «Российский софт: эффективные решения». Он подчеркнул, что в реестр отечественного ПО включено более 5,2 тыс. продуктов, разделенных на 24 класса. Как напомнил Алексей Соколов, в конце 2018 года произошел ряд значимых событий: запущен Реестр евразийского программного обеспечения, которое полностью приравнено к российскому; введен запрет на принудительное обновление и управление ПО из-за рубежа; установлены ограничения на гарантийное и техобслуживание, а также на модернизацию ПО иностранными компаниями; введена возможность включения в реестр того ПО, которое предоставляется по модели SaaS (ПО как сервис).

В качестве успешного примера перехода на отечественное ПО Алексей Соколов привел ПАО «Российские железные дороги». В компании создан постоянно действующий координационный орган, доработана ИТ-стратегия, создан план по переходу на отечественное ПО, включая ERP-систему, офисные продукты, а также защитные системы.

Алексей Соколов также объявил, что готовится постановление правительства, где вводится ограничение на госзакупки иностранной радиоэлектронной продукции. Кроме того, планируется выпустить директивы по закупкам преимущественно отечественного телекоммуникационного оборудования при создании инфраструктуры за счет бюджетных средств. Уже подготовлен перечень из 419 наименований оборудования, используемого для подключения социально значимых объектов к Интернету.

ARMA в помощь

В рамках РНВТ прошла конференция «Практика применения цифровых технологий на промышленных предприятиях», на которой было представлено решение InfoWatch ARMA. Это программно-аппаратный комплекс для промышленных сетей и систем, представляющий собой интегрированную платформу для поддержки информационной безопасности.

1 января 2018 года вступил в силу закон 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Данный закон и подзаконные акты обязывают компании, которые подпадают под его действие, строить системы защиты систем и сетей, отнесенных к критической информационной инфраструктуре (КИИ). Причем нарушителей норм ожидает серьезная ответственность, вплоть до уголовной.

Основным регулятором в этой области является Федеральная служба по техническому и экспортному контролю (ФСТЭК), а главным нормативным документом ФСТЭК – приказ №239, где содержится 135 мер, как организационных, так и технических. Но, как отметил директор по развитию продуктов ООО «Инфовотч Групп» Игорь Душа, нормативные требования постоянно ужесточаются. При этом ставится задача не просто формально соблюдать меры, а реально построить работающую систему защиты КИИ.

По оценке Игоря Души, для успешного решения задачи одних организационных мер недостаточно. На них приходится лишь около 30% от всего комплекса мероприятий, тогда как остальные 70% реализуемы только с помощью внедрения технических средств, включая межсетевые экраны, средства детектирования и предотвращения вторжений, средства защиты конечных точек, анализа уязвимостей, системы мониторинга и корреляции событий. Комплекс InfoWatch ARMA представляет собой экосистему средств защиты для технологических сетей комплексов АСУ ТП и позволяет закрыть если не все, то большую часть технических задач. Комплекс обеспечивает сегментирование сети и защищает периметр АСУ ТП. Также ARMA позволяет предотвращать такие действия как несанкционированная перепрошивка программируемых логических контроллеров (ПЛК), несанкционированное изменение установок ПЛК, подключение устройств в технологическую сеть, подмена сетевого адреса, попытка эксплуатации уязвимостей ПО и ПЛК, использование запрещенных функций промышленных протоколов.

Ладонь вместо паспорта

Игорь АГАПОВ

Технологии автоматизированной идентификации личности на основе индивидуальных биологических признаков (биометрия) относятся к одному из самых быстрорастущих сегментов мировой отрасли информационных технологий (ИТ). В России также отмечается динамичное развитие этого направления. Использование биометрических ИТ-систем дает новые эффективные инструменты для решения многих государственных и коммерческих задач, одновременно порождая целый ряд специфических проблем, с которыми приходится разбираться непосредственно при внедрении технологий биометрии.

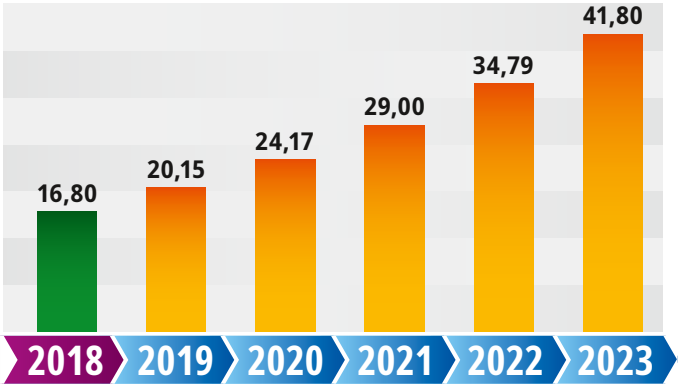
Мировые темпы роста рынка биометрических систем в среднесрочной перспективе достигнут 18-20% в год. Это позволяет отнести технологии биометрической идентификации личности к числу наиболее динамично развивающихся сегментов ИТ-отрасли.

Основные сферы, где активно используются биометрические технологии, – это государственный сектор (электронные документы, национальные биометрические программы и системы общественной безопасности); сфера путешествий и миграции (биометрические системы на транспорте и в миграционном контроле); финансовый сектор; здравоохранение; розничная торговля; корпоративный сектор (системы доступа, учета рабочего времени, охраны труда). Такой перечень свидетельствует о способности биометрических систем решать широкий спектр задач в самых разных прикладных областях.

На эту особенность систем биометрии обращает внимание директор по бизнес-развитию направления биометрических систем группы компаний «Центр речевых технологий» (ЦРТ) Андрей Хрулев. «Системы биометрической идентификации обладают полифункциональностью: например, система, созданная для обеспечения безопасности, может быть также использована для предоставления сервисов на транспорте – при автоматической регистрации пассажиров, первичном досмотре, допуске на посадку без предъявления документов. При этом во всех случаях «ядро» технологии будет оставаться одинаковым, отличия систем разного назначения будут заключаться в перечне реализуемых операций, точках их осуществления и ориентированных на конкретное применение интерфейсах», – рассказал Андрей Хрулев, выступая на конференции «Идентификация личности и контроль доступа» в рамках выставки Securika Moscow 2019.

Директор проектного офиса «Единая биометрическая система» ПАО «Ростелеком» Олег Ковпак иллюстрирует многофункциональность систем биометрической идентификации на примере Единой биометрической системы (ЕБС), которая как облачная платформа пока доступна только для предприятий банковского сектора, но в принципе может быть использована и в других отраслях экономики. «Среди основных задач, которые можно решать с применением ЕБС, – борьба с мошенничеством, получение и использование гражданами электронной подписи, предоставление государственных услуг, услуг здравоохранения и образования», – перечисляет Олег Ковпак.

Прогноз динамики мирового рынка биометрических систем ($ млрд)



Источник: MarketsandMarkets

Узнаю по походке

Биометрические системы идентификации основаны на нескольких биологических признаках, уникальных для каждого человека: к числу наиболее используемых данных относятся отпечатки пальцев (52% всего объема мирового рынка биометрических систем, по оценке J'son & Partners Consulting), изображение лица (23%), рисунок радужной оболочки глаза (12%), голос (5%), рисунок вен ладони (5%). Другие признаки (поведенческие реакции, эмоции и т. д.) занимают 3% мирового рынка биометрических систем.

Идентификация по отпечаткам пальцев, изображению лица и рисунку радужной оболочки применяется давно и уже стала привычной. В мире первые биометрические ИТ-системы появились в 1990-х годах, а начало их активного распространения приходится на первую половину 2000-х годов. Это относится и к России: в нашей стране с 1998 года существует единая дактилоскопическая база, пользователями которой являются правоохранительные органы и Вооруженные силы РФ.

Фото: СТАНДАРТ

Директор по бизнес-развитию направления биометрических систем группы компаний «Центр речевых технологий» (ЦРТ) Андрей Хрулев подчеркивает, что системы биометрической идентификации могут использоваться в различных целях, при этом отличия систем заключаются в интерфейсах, перечне операций и точках их осуществления

Фото: СТАНДАРТ

Директор проектного офиса «Единая биометрическая система» ПАО «Ростелеком» Олег Ковпак считает борьбу с мошенничеством актуальной задачей, для решения которой целесообразно применение биометрии, так как с ростом цифровизации услуг в банковском секторе растет и уровень киберугроз, в том числе при использовании банкоматов

В 2009 году в России стали выдаваться биометрические заграничные паспорта, в чип которых заносилась информация о межзрачковом расстоянии, а с 2015 года – и об отпечатках указательных пальцев.

Особый интерес с точки зрения развития биометрической идентификации представляет использование в системах относительно новых видов биологических данных.

Директор по развитию ООО «Прософт-Биометрикс» Александр Горшков рассказал о возможностях идентификации по рисунку вен ладони: «Этот вид идентификации является одним из наиболее точных методов опознавания личности наряду с идентификацией по радужной оболочке глаза. Кроме того, скомпрометировать или подделать рисунок вен крайне сложно. Причем этот метод менее затратен по сравнению с другими биометрическими методами идентификации. Системы идентификации по венам ладони могут быть интегрированы с другими ИТ-системами, такими как пожарно-охранная сигнализация, система учета персонала, бухгалтерский учет».

Директор департамента маркетинговых исследований J'son & Partners Consulting Наталья Шленова считает, что в среднесрочной перспективе поведенческая биометрия и распознавание эмоций станут одними из наиболее растущих сегментов мирового биометрического рынка. «Объем мирового рынка решений для идентификации личности и выявления состояния человека на основе анализа поведенческих реакций увеличится с $870 млн в 2018 году до $2,55 млрд в 2023-м. За этот же период рынок решений для распознавания эмоций вырастет с $8,1 млрд до $33,9 млрд», – прогнозирует аналитик.

Перспективные биометрические технологии уже рассматриваются в качестве направлений дальнейшего развития систем идентификации в России, сообщил Олег Ковпак. «Согласно постановлению правительства РФ, сейчас в ЕБС применяются технологии распознавания лиц и голоса, но в технологических решениях системы уже заложены возможности идентификации личности по рисунку вен ладони и на основе поведенческого анализа. В перспективе возможно развитие функций ЕБС для идентификации представителей юридических лиц: соответствующие шаги сейчас прорабатываются с участием Центрального банка и Минкомсвязи РФ», – уточнил директор проектного офиса «Ростелекома».

В то же время применение хорошо известных биометрических технологий в сочетании с другими мерами позволяет повысить эффективность систем безопасности, уверен начальник управления технической безопасности департамента защиты информации АО «Газпромбанк» Александр Долженко. «Мы использовали интегральный подход к организации систем контроля и управления допуском (СКУД): бесконтактная биометрия в виде распознавания лиц в комплексе с традиционными пропусками с радиочастотной идентификацией (Radio Frequency IDentification, RFID). В частности, это исключает возможность передачи пропусков сотрудниками банка другим лицам. Кроме того, с помощью биометрии можно внедрить так называемый стоп-лист, или перечень посетителей, которым по тем или иным причинам отказано в допуске в помещения банка. Использованный подход на практике показал свою эффективность при организации контроля на входных зонах в здание, при входе в режимные помещения, при аутентификации клиентов в помещениях, где расположены индивидуальные банковские ячейки и сейфы», – отметил Александр Долженко.

Специфика ИТ-опознания

В процессе создания систем биометрической идентификации необходимо учитывать различные факторы – с целью обеспечения надежности и безопасности таких систем.

Управляющий партнер группы компаний «Синезис» Николай Птицын указывает на характерные проблемы при внедрении биометрических технологий для СКУД. «Среди таких проблем – недостаточная точность распознавания отпечатков пальцев, ограниченный объем хранения образцов отпечатков в считывателях (около 1 тыс. единиц), сложность интеграции нескольких биометрических технологий в единую систему аутентификации. Поэтому целесообразно применять в СКУД одну или несколько биометрических технологий совместно с традиционными системами пропусков на основе радиометок ближнего действия (RFID). Для развертывания биометрических решений в составе систем контроля и управления доступом можно использовать облачные платформы, что дает возможность легко масштабировать решения. При этом важно резервировать расположенную в облаке базу данных биометрической системы на локальном контроллере, находящемся на территории объекта, чтобы работа биометрического контура СКУД не прерывалась в случае перегрузки или отключения канала связи с облаком», – рассуждает Николай Птицын.

Об особенностях систем биометрической идентификации как ИТ-решений говорит и Андрей Хрулев. «Следует иметь в виду, что у биометрических систем есть уязвимости. В основном атакам подвергаются устройства ввода данных и каналы связи. Кроме того, может быть атакован сам алгоритм работы систем биометрической идентификации – путем несанкционированного извлечения содержащихся в базе данных биометрических признаков (с последующим незаконным использованием) либо путем предъявления фальшивых биометрических признаков (муляжей отпечатков пальцев, изображений лиц и т. п.). Поэтому, в случае если не предусмотрены адекватные меры защиты, биометрическая система становится не просто бесполезной, но и опасной. Одна из возможных мер для защиты систем распознавания лиц – применение алгоритма «я живой», основанного на анализе параметров, отличающих

16


Фото: СТАНДАРТ

По словам директора департамента маркетинговых исследований J'son & Partners Consulting Натальи Шленовой, наиболее быстрый рост использования биометрии в России следует ожидать в финансовом секторе, а к перспективным направлениям внедрения биометрических технологий также относятся транспорт и розничная торговля


Фото: СТАНДАРТ

Начальник управления технической безопасности департамента защиты информации АО «Газпромбанк» Александр Долженко отмечает, что одна из проблем внедрения биометрических систем – несовместимость их программного обеспечения с другим прикладным ПО, что требует модернизации программно-аппаратной платформы общей системы безопасности

живое лицо от изображения или маски (мимика, движение глаз, дыхание и другие), – поясняет директор по бизнес-развитию направления биометрических систем ЦРТ. – Для крупных проектов биометрической идентификации надежность центров обработки данных, в которых размещается биометрическая СКУД, является ключевым аспектом. В таких проектах следует использовать существующие крупные ЦОДы с подготовленным персоналом и надежной защитой доступа. На небольших объектах биометрические системы контроля и управления доступом могут быть размещены на одном хорошо защищенном промышленном компьютере».

Отдельной задачей с точки зрения обеспечения надежности биометрических технологий является их стандартизация, уверен директор НП «Русское биометрическое общество», председатель ТК 098 «Биометрия и биомониторинг» Данила Николаев: «Нормативно-техническое регулирование (стандарты) является необходимым условием развития технологий биометрической идентификации. Несоблюдение или недостаточная разработанность стандартов могут привести не только к ошибкам в срабатывании систем аутентификации, но также к нанесению ущерба гражданам и организациям из-за утечки биометрических данных вследствие незащищенности системы. В настоящее время в мире действует более 80 стандартов в сфере технологий биометрической идентификации, в России – 46 и еще 19 находятся в разработке. В частности, в нашей стране с 2017 года действует стандарт терминологии биометрических данных, создан стандарт обмена биометрическими данными, завершается разработка серии стандартов для хранения биометрических данных на индивидуальной электронной индентификационной карте».

Идентификация по-российски

По оценке Натальи Шленовой, наш рынок технологий биометрической идентификации имеет несколько черт, отличающих его от мирового рынка. «Российский рынок биометрических технологий в 2014-2018 годах рос быстрее мирового – в среднем на 33,7% ежегодно, тогда как мировой темп составил 26,8% в год. Эта тенденция сохранится: согласно прогнозам J'son & Partners Consulting, в 2018-2022 годах биометрический рынок в России будет расти со среднегодовым темпом 29,5% против общемировых 18,2% в год. Российская специфика рынка проявляется и с точки зрения используемых видов биологических данных. Например, в мире большинство решений биометрической идентификации основано на распознавании отпечатков пальцев – 52% объема рынка, а в России этот вид решений занимает только 29% рынка. В то же время половина рынка биометрических решений в нашей стране (50%) приходится на распознавание лиц, тогда как в мире такие решения занимают всего 23% рынка. Есть различия и по другим биометрическим технологиям. Если идентификация по рисунку вен ладони занимает 17% российского рынка биометрии, то в мире – всего 5%. Обратное соотношение – для идентификации личности по радужной оболочке глаза: 12% в мире и лишь 0,3% в России. Кроме того, если во всем мире отмечается сокращение доли государственных заказчиков на рынке биометрии, то в России растет доля госструктур и компаний с государственным участием, которые внедряют биометрические системы», – характеризует особенности российского рынка директор департамента J'son & Partners Consulting.

Один из наиболее крупных биометрических проектов в нашей стране – создание ЕБС для банковского сектора. Согласно постановлению правительства РФ, оператором системы назначен «Ростелеком». В Единой биометрической системе должны аккумулироваться данные клиентов, которые банки обязаны фиксировать согласно требованиям действующего законодательства. В настоящее время биометрические данные клиентов собирают около 150 российских банков, причем закон требует, чтобы сбор таких данных к 1 июля 2019 года был обеспечен в 60% отделений каждого банка, а к началу 2020 года – во всех отделениях. Более того, принятый 31 декабря 2017 года Федеральный закон №482 «О внесении изменений в отдельные законодательные акты РФ» гласит, что банки могут дистанционно открывать счета (вклады), предоставлять кредиты и осуществлять переводы без личного присутствия клиента с использованием его биометрических данных и Единой системы идентификации и аутентификации (ЕСИА). Однако пока возможность оказывать услуги на основе биометрических данных клиентов реализована только в четырех банках – в Альфа-Банке, ВТБ, банке «Открытие», Почта Банке.

Кроме предоставления услуг, биометрия позволяет решить и другие актуальные для банковского сектора задачи. «Среди основных задач, которые можно решать с применением ЕБС, – борьба с мошенничеством, получение и использование гражданами электронной подписи, предоставление государственных услуг. Борьба с мошенничеством – особенно актуальная задача, для решения которой целесообразно применение биометрии. С ростом цифровизации услуг в банковском секторе растет и уровень киберугроз. Один из самых подверженных кибератакам сервисов – интернет-банкинг: здесь существуют высокие риски компрометации устройства абонента и канала связи с банком путем внедрения вредоносного ПО. Кроме того, биометрические технологии позволяют снизить уровень мошенничества при использовании банкоматов и расширить перечень предоставляемых с их помощью услуг. Применение биометрии даст возможность банкам применять простую электронную подпись клиента при составлении юридически значимых документов, чего сейчас делать нельзя. Кроме того, биометрия поможет сократить время и трудозатраты на аутентификацию клиента при его

Фото: СТАНДАРТ

Управляющий партнер группы компаний «Синезис» Николай Птицын указывает на то, что для обеспечения максимальной надежности работы в системах контроля и управления доступом целесообразно применять одну или несколько биометрических технологий совместно с традиционными системами пропусков на основе радиометок ближнего действия

Фото: СТАНДАРТ

Директор НП «Русское биометрическое общество», председатель ТК 098 «Биометрия и биомониторинг» Данила Николаев подчеркивает, что недостаточная разработанность стандартов может привести не только к ошибкам в срабатывании систем аутентификации, но также к ущербу из-за утечки биометрических данных вследствие незащищенности системы

дистанционном обращении в банки – например, в случаях, когда клиент забывает контрольные слова, пароли, номера банковских карт», – пояснил директор проектного офиса «Ростелекома» Олег Ковпак.

Помимо сферы банковского обслуживания, технология биометрической идентификации используется и в других областях экономики и общественной жизни.

«Уже сейчас в нашей стране работает несколько систем на базе технологии идентификации на основе рисунка вен ладони, – отмечает Александр Горшков. – В одном из банков она применяется для контроля доступа в кассу. В промышленности эта технология используется для предотвращения прохода посторонних лиц на территорию предприятия, а также для распознавания личности при прохождении автоматического теста на алкоголь в выдыхаемом воздухе (система, контролирующая наличие алкогольного опьянения у сотрудников). В Росгвардии технология применяется для организации доступа на наиболее важные объекты штабов, узлов связи, командных пунктов. При крупных масштабах проекта экономическая эффективность технологии идентификации по рисунку вен ладони достаточно высока: внедрение технологии в 700 российских ресторанах «Бургер Кинг» для учета рабочего времени окупилось за один год».

Применяется биометрия и для решения задач общественной безопасности. Известно, что система распознавания лиц была развернута на стадионах и в других местах массового посещения во время Чемпионата мира по футболу FIFA в России 2018 года. Недавно аналогичный проект был реализован в «Ельцин Центре» в Екатеринбурге: внедренная система биометрической идентификации позволяет осуществлять интеллектуальный поиск по изображению лиц с получением полной статистики о времени и дате всех посещений центра конкретным человеком. В результате полной автоматизации поиск и идентификация подозрительных лиц сокращается до нескольких минут. Среди других функций – создание стоп-листов, списков VIP-посетителей, идентификатор местоположения посетителей, аналитика аудитории по полу, возрасту и средней длительности пребывания в центре.

Поле для биометрии

Специалисты отмечают несколько тенденций и отдельных направлений развития биометрических технологий в России.

«Прежде всего стоит отметить рост доли биометрических технологий в системах контроля и управления доступом. Наиболее быстрый рост использования биометрии в нашей стране в период 2018-2022 годов следует ожидать в финансовом секторе экономики – в среднем на 54% ежегодно. Кроме того, среди перспективных направлений внедрения биометрических технологий – их применение на транспорте для автоматической регистрации пассажиров и контроля посадки, а также для регистрации в отелях. Большой потенциал есть у биометрических платформ для оплаты покупок в розничной торговле: объем транзакций с помощью биометрии в перспективе четырех-пяти лет может составить до 1,5 млрд покупок в год на общую сумму до 1,35 трлн рублей, или 4-5% всех розничных покупок», – отмечает директор департамента маркетинговых исследований J'son & Partners Consulting Наталья Шленова.

Директор по развитию ООО «ЭсЭл Девелопмент» Павел Голобородько обращает внимание на важность создания единой системы биометрических данных для решения задач правоохранительной деятельности. «В настоящее время для России актуально создание единой платформы интеллектуальной видеоаналитики деятельности сотрудников правоохранительных органов. Это важно как для объективной фиксации событий при выезде сотрудников на происшествия, так и для оперативного обмена информацией между полевыми сотрудниками и командными центрами. Единая платформа повысит оперативность управления мобильными группами и усилит контроль за действиями каждого сотрудника при выполнении заданий. Биометрическая идентификация с помощью распознавания лиц и голоса как элемент такой интеллектуальной системы обеспечит однозначное определение любого сотрудника, попадающего в кадр видеорегистратора. Кроме того, такая система обеспечит быстрое обращение к базе данных лиц, находящихся в розыске, и оперативный ответ по опознанию. Мы осуществили внедрение такой системы для Росгвардии, и подобный проект может быть реализован для других правоохранительных органов», – говорит Павел Голобородько.

Председатель ТК 098 «Биометрия и биомониторинг» Данила Николаев обозначил перспективы дальнейшей стандартизации биометрических технологий: «Для России перспективой в этой области является появление стандартов для ЕБС, работа над которыми уже идет. В мире тоже продолжается расширение сферы стандартизации биометрии. Например, в 2020 году планируется включить международные биометрические стандарты в состав регуляторных документов Международной организации гражданской авиации (International Civil Aviation Organization, ICAO), касающихся машиночитаемых биометрических показателей».

В России планируется реализовать несколько крупных проектов биометрической идентификации. Например, уже в текущем году правительство Москвы намерено развернуть общегородскую систему распознавания лиц. Также появилась информация, что концерн «Калашников» обсуждает с Минстроем РФ создание систем распознавания лиц на строящихся объектах для обеспечения безопасности и предотвращения хищений. В перспективе этот проект может быть распространен на завершенные объекты (по запросам застройщиков).

Игра на опережение

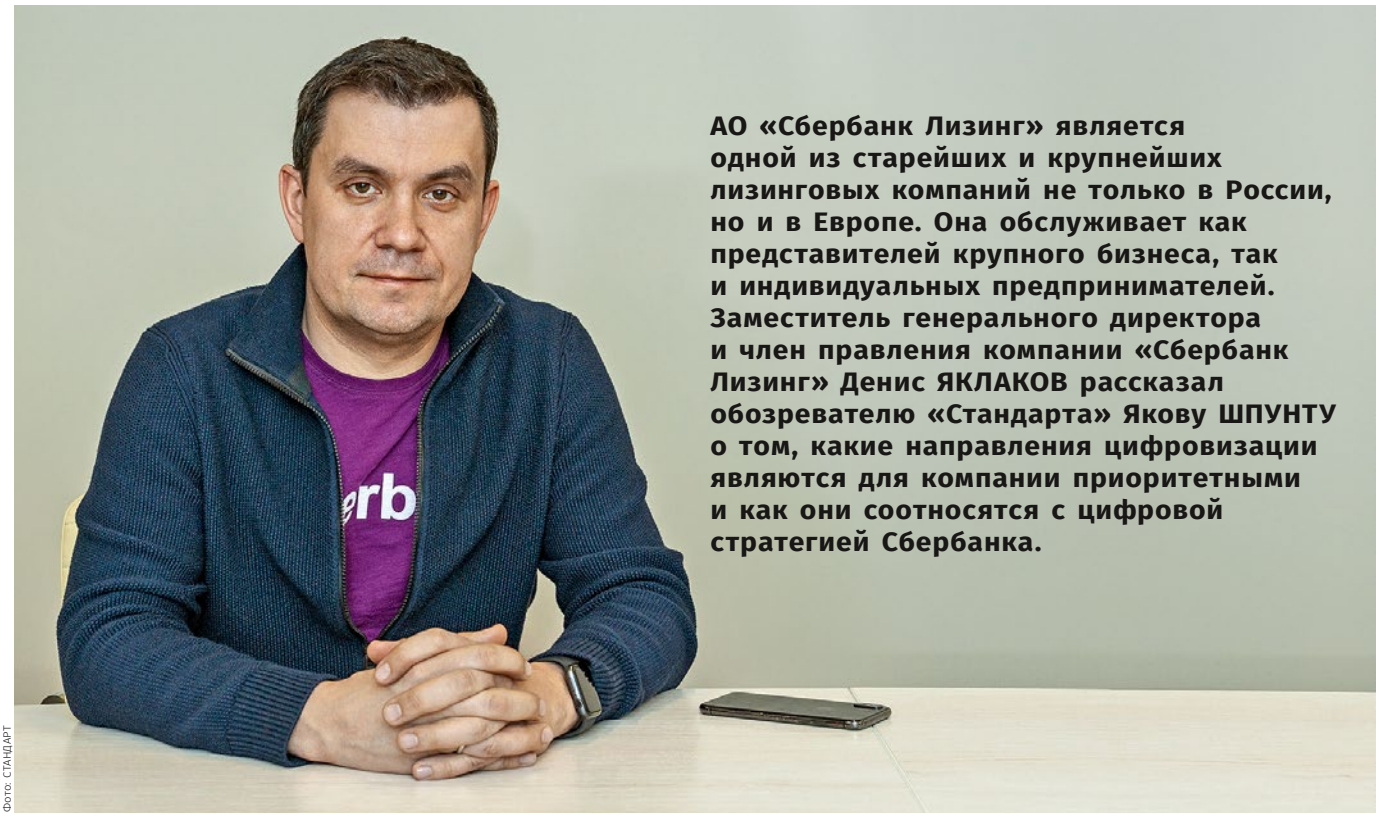


Фото: СТАНДАРТ

АО «Сбербанк Лизинг» является одной из старейших и крупнейших лизинговых компаний не только в России, но и в Европе. Она обслуживает как представителей крупного бизнеса, так и индивидуальных предпринимателей. Заместитель генерального директора и член правления компании «Сбербанк Лизинг» Денис ЯКЛАКОВ рассказал обозревателю «Стандарта» Якову ШПУНТУ о том, какие направления цифровизации являются для компании приоритетными и как они соотносятся с цифровой стратегией Сбербанка.

– Какие задачи в области цифровой трансформации ставит перед «Сбербанк Лизингом» материнская компания и какие шаги реализуете по собственной инициативе? Есть ли единая стратегия трансформации, охватывающая все дочерние компании Сбербанка?

– У «Сбербанк Лизинга» есть ИТ-стратегия, разработку которой мы начали еще пять лет назад. Она согласована архитекторами ПАО «Сбербанк» и утверждена в соответствии с корпоративными процедурами. Эта стратегия тесно связана с материнской организацией: проекты «Сбербанк Лизинга» реализуются в связке с банковскими, и мы активно используем инфраструктуру Сбербанка.

При этом лизинг – отдельный бизнес, имеющий серьезные отличия от банковского. Соответственно, нам нужно автоматизировать бизнес-процессы, которых в банке нет. Поэтому в итоге большая часть процессов автоматизирована в системах «Сбербанк Лизинга», и только те процессы, которые полностью унифицированы с банком, – в его системах. Такой подход утвердило руководство Сбербанка.

Но в любом случае развитие ИТ-систем «Сбербанк Лизинга» является предметом для обсуждения с архитекторами на уровне Сбербанка. И это полезно, поскольку уровень компетенций специалистов блока «Технологии» банка высок, их мнение и рекомендации для нас очень ценны.

– Расскажите о программе Digital, которую реализует «Сбербанк Лизинг». Когда она была принята? Каковы ее основные положения?

– Программа принята в начале 2018 года. Ее цель – ответить на актуальные для нас цифровые вызовы и обеспечить выполнение задач, которые ставит перед нашей компанией бизнес.

Мы определили для себя пять ключевых вызовов. Первый – работа с большими данными. Второй – повышение скорости принятия бизнес-решений и их надежности. Третий – развитие web- и мобильной платформ: наши клиенты становятся моложе, они привыкли получать необходимые услуги через мобильные устройства. Четвертый вызов – интеграция. Мир стал одной большой системой, части которой связаны огромным количеством каналов. А значит то, что мы создаем, должно «уметь» интегрироваться с системами банка, регуляторов, партнеров, клиентов, любых других субъектов, с которыми придется взаимодействовать. Пятый вызов – удобство в использовании наших систем, ориентированных прежде всего на клиентов. Последние исследования показывают, что клиенты, особенно молодые, все чаще отдают предпочтение удобным, а не дешевым сервисам. Так что интерфейсы взаимодействия с клиентами и партнерами должны быть удобными.

Отвечая на эти вызовы, бизнес (точнее, внутренний заказчик) сформулировал для нас ключевые задачи. Прежде всего нам нужно было создать собственную фронтальную систему, позволяющую взаимодействовать с клиентами, партнерами и банком напрямую. И поскольку более половины продаж стандартных продуктов «Сбербанк Лизинга» проходит через банк, второй задачей стала интеграция фронтальной системы в сервис «Сбербанк Бизнес Онлайн», который является ключевой составляющей всей экосистемы Сбербанка.

Третья задача – внедрение мощной CRM-системы, позволяющей вывести качество работы с клиентами на новый уровень. Четвертая – обновление ERP-системы на базе Microsoft Dynamics Nav, которую мы «переросли». К тому же в ближайшее время ожидается многократный рост количества операций, так что компании нужна более современная и производительная

платформа. Также мы осознали необходимость внедрения BPM-модуля для более качественного управления бизнес-процессами. И наконец, в прошлом году мы завершили первый этап внедрения SAP SuccessFactors HR Management: эта система внедряется во всем Сбербанке с целью развития наиболее ценного ресурса – человеческого капитала.

– Вы как-то говорили, что будущее есть только у тех компаний, которые создадут свою экосистему или станут частью более крупной системы. Как эффективно выстроить такую систему?

– При реализации любого плана надо четко понимать потребности компании, причем не только сегодняшние, но и те, которые возникнут через несколько месяцев или даже лет. Только так можно понять, нужно строить свое или интегрироваться в чью-то инфраструктуру. Если вы понимаете, что необходимо работать с большим количеством внешних систем, то потребуется мощная платформа, и на рынке представлено большое разнообразие решений. Но делая выбор, нужно обращать внимание на то, насколько потенциальное решение соответствует вашим текущим и будущим потребностям. Для этого нужно задать такой вопрос: как будет выглядеть система и что вам даст ее использование? Так же осознанно нужно относиться к партнерству с интегратором, который, как правило, тоже участвует в выборе платформы. И если потенциальные партнеры способны жить потребностями вашего бизнеса, если возникла бизнес-эмпатия, то вероятность успешности проекта значительно вырастает.

– В 2017 году компания запустила сервис юридически значимого электронного документооборота E-Leasing. В чем особенность данного сервиса? Какие преимущества от его использования получает «Сбербанк Лизинг» и клиенты компании? Потребовал ли сервис доработок после ввода в эксплуатацию?

– Любой сервис требует постоянных доработок. С помощью специалистов нашего партнера ООО «КОРУС Консалтинг» мы интегрируем E-Leasing с платформой Terrasoft, которая внедряется в нашей компании. Это позволит реализовать механизм трехстороннего подписания непосредственно на портале «Сбербанк Лизинга».

Система E-Leasing дает возможность подписывать документы без использования бумажных носителей и без физического контакта клиента с нашими менеджерами и сотрудниками поставщика. Это экономит время и сокращает потребности в кадровых ресурсах, мы экономим на поиске, обучении, оплате труда персонала. В этом заключен важный экономический эффект: сделка с использованием E-Leasing стоит для нас существенно дешевле.

Есть определенное ограничение в скорости распространения этого сервиса – соответствующий «уровень подготовки» клиентов и поставщиков. В первом квартале 2019 года с использованием E-Leasing было оформлено более 15% стандартных сделок. В текущем году мы планируем поднять этот уровень минимум до 25%. Есть регионы, где доля электронно оформленных сделок существенно выше: это результат более активной позиции сотрудников «Сбербанк Лизинга» на местах, а также готовность крупных поставщиков к более активному использованию электронной подписи. В целом мы планируем в текущем году протестировать и запустить в эксплуатацию технологию, позволяющую не только уйти от бумажного документооборота, но также исключить сотрудников нашей компании из процесса рассмотрения и заключения лизинговой сделки.

> **«При реализации любого плана надо четко понимать потребности компании, причем не только сегодняшние, но и те, которые возникнут через несколько месяцев или даже лет»**

– В конце 2018 года вы начали проект по модернизации CRM. Как вы выбирали систему для перехода? С какими сложностями столкнулись в ходе проекта?

– Как уже говорилось, наши прежние системы устарели, они перестают нас устраивать как по функциональности, так и по масштабируемости. Поэтому возникла необходимость их замены, что нашло отражение в ИТ-стратегии «Сбербанк Лизинга».

Мы рассматривали все возможные варианты, за исключением полностью облачных сервисов, которые не локализованы в России. В конце концов список свелся к трем решениям – от Oracle, Microsoft и Terrasoft. Мы сопоставляли стоимость, расходы на внедрение и сопровождение, функциональные возможности, наличие экспертизы и команд, способных реализовывать проекты. Решение Terrasoft в наибольшей степени отвечало нашим требованиям. Кроме того, в ходе встреч представители этой компании доказали, что лучше других понимают наши задачи, предложив для их решения несколько вариантов. Кроме того, они продемонстрировали, что на одной платформе можно реализовать функционал как CRM, так и фронтальной системы «Сбербанк Лизинга». Совокупность факторов определила наш выбор.

Сейчас проект находится на стадии активной реализации, и пока у нас нет оснований сомневаться в правильности сделанного выбора.

– Для выполнения ИТ-проектов компания привлекает штатных специалистов или сотрудников внешних организаций? Ощущает ли «Сбербанк Лизинг» дефицит ИТ-кадров и как справляется с этой проблемой?

– Для реализации крупных проектов мы используем комбинированные команды. Любой масштабный проект требует дополнительных ресурсов, брать которые «на борт» сложно да и порой не нужно. На рынке есть крупные, хорошо себя зарекомендовавшие интеграторы. Компания Terrasoft предоставила нам перечень своих партнеров с успешным опытом реализации проектов. Среди них мы и выбрали победителя.

Что касается проблемы дефицита ИТ-кадров, то она есть. Мы столкнулись с ней при работе с продуктом Microsoft Dynamics Nav, специалистов по развитию которого относительно немного. В поиске мы многократно «просеиваем» рынок, выделяем в HR-отделе сотрудников на подбор ИТ-специалистов, в итоге закрывая требуемые вакансии.

– Видите ли вы перспективы применения таких технологий как искусственный интеллект, машинное обучение, blockchain, голосовые помощники? В каких бизнес-процессах «Сбербанк Лизинга» они могут быть востребованы?

– Да, мы видим перспективы для этих технологий в «Сбербанк Лизинге». В вопросах внедрения новых технологий также исходим из интересов бизнеса, это наш приоритет. Внедрять что бы то ни было ради внедрения, или просто потому что это модно, мы не будем.

Искусственный интеллект и машинное обучение используются в системах управления кредитными рисками всего Сбербанка, мы их тоже применяем. Также развиваем собственный чат-бот – консультанта по имени Лиза.

Ломая стереотипы

Современные сети из каналов передачи данных превратились в источники контекста для любого бизнеса: анализируя их работу, предприятия получают информацию, необходимую для принятия управленческих решений. Компания Cisco изменила подход к созданию сетевой инфраструктуры и управлению ею, предложив концепцию интуитивной сети. О том, насколько она близка заказчикам из нефтегазового, банковского и других секторов, а также о том, какие вызовы стоят перед ними с точки зрения цифровизации, редактору «Стандарта» Ксении ПРУДНИКОВОЙ рассказал директор департамента Cisco по работе с корпоративными клиентами Алексей ПЕРЕВЯЗКИН.

Фото: СТАНДАРТ

– Вы более 10 лет работаете с корпоративными заказчиками Cisco в России. Как за это время изменились потребности и запросы российского бизнеса к вендорам?

– Для ИТ-рынка 10 лет – значительный отрезок времени, за который изменились не только потребности заказчиков, но и сами производители оборудования, в том числе наша компания. В прошлом клиенты в первую очередь требовали от систем связи надежности и возможности соединения решений. И действительно, на рынке было много технологий и продуктов, которые не были взаимосвязаны. Производители предлагали их секторами – например, оборудование для компьютерных сетей, системы безопасности или унифицированных коммуникаций и т. д. Как результат, компании наращивали ИТ-инфраструктуру, сначала закрывая базовые потребности предприятия и лишь затем задумываясь о дополнительных возможностях.

За 10 лет произошел качественный скачок – мы шагнули в эру цифровизации. Если еще несколько лет назад представители ИТ-департаментов заказчиков затруднялись сформулировать, что такое «цифровизация», то теперь бизнес приходит к ИТ-специалистам с вопросом, какие цифровые инициативы они могут предложить.

Сегодня наших крупных корпоративных клиентов интересует, как с помощью ИТ повышать эффективность бизнеса, меняя его, что называется, на ходу. Трансформировалась и компания Cisco: мы выпускаем продукты, существование которых еще три-пять лет назад сложно было себе представить.

– В каких областях цифровизация может принести наибольший эффект?

– Прежде всего, это B2B- и B2C-сегменты и онлайн-бизнес. Так, всем известны успешные примеры из транспортной сферы, давшие толчок другим отраслям. Сегодня цифровизация глубоко проникла в сферу предоставления услуг, включая государственные, банковские и ретейл.

Пару лет назад Cisco совместно со швейцарской бизнес-школой IMD провели исследование и опубликовали книгу Digital Vortex («Цифровой водоворот»): мы выявили, какие отрасли находятся в эпицентре цифровизации. Хочу отметить, что крупные инфраструктурные заказчики, находящиеся на периферии, постепенно продвигаются к центру этого водоворота. Значительные шаги сделаны в энергетическом и нефтегазовом секторах. Примечательно, что у наших крупнейших заказчиков появляются обособленные подразделения и назначаются вице-президенты, отвечающие за цифровизацию. Задачи по цифровой трансформации бизнеса обсуждаются на уровне советов директоров предприятий. Это, безусловно, положительный тренд: сегодня компании могут реализовать проекты, к которым они не были готовы еще два-три года назад.

– В ходе конференции Cisco Connect, проходившей в Москве, прозвучала мысль о том, что в будущем обязанности директора по развитию бизнеса и по цифровизации будет выполнять один топ-менеджер...

– Должность директора по цифровым технологиям (Chief Digital Officer) появилась не так давно, но роль менеджеров, отвечающих за развитие бизнеса, в том числе за счет ИТ, трудно переоценить. Выбор цифровых решений – крайне сложный процесс, особенно для крупных компаний, где важно понимать, насколько эффективным в масштабах всего бизнеса может быть применение того или иного digital-решения.

– В Cisco вы отвечаете за работу с крупнейшими клиентами. Какой процент от общего количества заказчиков они составляют в России? Какие вызовы, с точки зрения оптимизации бизнеса за счет технологий, стоят перед этими компаниями, и играет ли роль отраслевая специфика?

– Я работаю приблизительно со 100 компаниями, которые вносят значительный вклад в наш российский бизнес.

Что касается вызовов, то для крупных компаний была характерна ситуация, когда на инновационные проекты им требовалось слишком много времени: от стадии планирования до начала реализации проходило от полутора до двух лет. За это время могло смениться несколько поколений технологий.

Сейчас мой департамент предлагает возможность проводить микропилотные проекты, которые реализуются либо в «песочницах», либо в виртуальной инфраструктуре Cisco dCloud. Мы применяем подход Proof of Value, демонстрируя, как при помощи наших технологий можно решить конкретные задачи заказчика. Это оправданная стратегия: крупные корпоративные заказчики крайне редко выбирают решения, предварительно их не опробовав. Для них цена ошибки слишком высока.

Также мы действуем на опережение. Cisco активно продвигает на рынке архитектуру программно определяемой глобальной сети (Software-Defined Wide Area Network, SD-WAN). Передо мной стояла амбициозная задача показать это решение «в живую» 50% заказчиков, но интерес с их стороны оказался настолько велик, что эту цифру вполне можно довести и до 100%. Решение настолько простое в использовании, что клиенты в буквальном смысле выстраиваются в очередь, чтобы увидеть его своими глазами.

> **«Наших крупных корпоративных клиентов интересует, как с помощью ИТ повышать эффективность бизнеса, меняя его на ходу»**

Стоит отметить, что мы также рискуем: неправильно проведенные пилотные проекты, не отвечающие потребностям заказчика, могут отрицательно повлиять на развитие направления. Не увидев всех возможностей решения или технологии, клиент может выбрать то, что на самом деле не подходит его бизнесу, и разочароваться в технологическом партнере.

– Какие еще продукты Cisco адресованы в первую очередь крупнейшим заказчикам?

– С весны прошлого года мы активно продвигаем решения для сети, управляемой на основе намерений (Intention-Based Network, IBN). Кстати, уже упомянутое решение SD-WAN является частью этой экосистемы. IBN – это без преувеличения революция в мире сетей; спрос на такие продукты превзошел все наши ожидания, в результате чего мы даже вынуждены были на несколько недель увеличить сроки производства соответствующего оборудования. Для удовлетворения потребностей заказчиков мы планируем задействовать производственные мощности Cisco в России. Говоря о конкретных решениях, хочу отметить коммутаторы серии Catalyst 9300/9400, которые чрезвычайно просты в использовании и позволяют эффективно развивать сетевую инфраструктуру. Помимо этого, наши продукты в области IBN обладают непревзойденными возможностями по анализу зашифрованного трафика, что чрезвычайно важно для выявления и блокировки вредоносной активности в корпоративной сети.

В целом, мы стараемся уделять максимум внимания комплексности подхода в построении ИТ-архитектур, интегрируя весь спектр технологий – от сетевых решений до безопасности и облаков. То есть многие производители предлагают коммутаторы, маршрутизаторы и прочее оборудование, вполне сопоставимое по скорости работы, количеству портов и качеству обслуживания, но сегодня этого недостаточно. С появлением программно определяемых продуктов (SD-WAN, SD-VLAN, SD-Access) мы сломали представление о Cisco как о производителе коммутаторов, что позволяет нам конкурировать на совершенно ином уровне. Мы изменили сам подход к построению сетей. А комплексная система Cisco DNA Center дает возможность по-новому управлять сетевой инфраструктурой, позволяя автоматизированно подключать новых клиентов, соблюдая все требования безопасности.

Также можно отметить решение в области информационной безопасности Cisco Stealthwatch, которое позволяет корпоративному заказчику отслеживать поведение сети, обеспечивая ее защиту. Данный продукт уникален еще и потому, что стирает границы, работая в интересах как департамента обеспечения информационной безопасности, так и подразделения по управлению сетевой инфраструктурой. Это еще одна ключевая особенность продуктов Cisco: практически все они обладают сквозными функциями встроенной безопасности и работают как единое целое. И это дает основание предполагать, что со временем ИТ-подразделения возьмут на себя функции служб обеспечения безопасности.

Примечательно, что уже сейчас в России есть ряд заказчиков, которые используют до 90% решений и технологий, производимых Cisco.

– В компаниях любых масштабов высок спрос на грамотных ИТ-специалистов. Как Cisco помогает решать проблему дефицита кадров?

– С одной стороны, у нас есть программы по сертификации и обучению специалистов. С другой – в России и мире действует программа Сетевая академия Cisco, наша крупнейшая инициатива в области корпоративной социальной ответственности. Эта программа позволяет студентам вузов получать своеобразные «водительские права для ИТ» – базовые навыки в области высоких технологий.

Но еще раз отмечу, что не менее важно повышать квалификацию уже работающих специалистов. С появлением продуктов, позволяющих автоматизировать многие процессы, меняется и роль ИТ-специалистов, у них появляется больше времени для творчества и решения нестандартных задач.

Важно и то, что ИТ-решения появляются все быстрее, и специалистов, готовых с ними работать, не так много. Вместе с тем снижается потребность в узкоспециализированных кадрах, которые просто не успевают за всеми технологическими новинками. Мы стараемся решать эту проблему: например, проводим специальные тренинги через сеть авторизированных партнеров Cisco. Помимо этого мы организуем семинары двойного назначения, состоящие из теоретической и практической частей. Такие киберучения позволяют отрабатывать инциденты безопасности на сети.

Если говорить в целом о роли ИТ-менеджеров, то сейчас она укрепляется: они участвуют в принятии управленческих

22

решений, входят в советы директоров. Отрадно, что ИТ-подразделения перестали воспринимать как затратную часть организации. Стало очевидно, что они способны трансформировать бизнес, повышать его эффективность. ИТ-инфраструктура стала все больше отвечать текущим потребностям бизнеса, за счет своей гибкости позволяя либо сокращать издержки, либо наращивать мощности. Если посмотреть на клиентские сервисы – например, на мобильные приложения, – то они должны быть доступны в режиме 24/7, что также повышает требования к надежности сети.

– Действительно, управление производительностью приложений играет ключевую роль в любом бизнесе. Какие возможности в данной сфере предлагает Cisco своим заказчикам?

– В результате приобретения компании AppDynamics мы сформировали комплексный пакет решений для корпоративных заказчиков – это как раз пример комплексного архитектурного подхода, о котором я упоминал ранее. У нас есть решение для автоматизации дата-центров (Cisco Application Centric Infrastructure, ACI). Платформа Cisco Tetration Analytics позволяет проанализировать работу ЦОДа. Продукты AppDynamics дополняют этот стек решений, позволяя отслеживать работу приложений. Теперь, в случае возникновения сбоя, не составляет труда выяснить, где находятся его причины – на стороне разработчика приложения, владельца сетевой инфраструктуры или в дата-центре. Более того, мы научились выявлять «узкие места» в программном коде приложений и предлагаем варианты, как их исправить. Все это позволило сократить сроки устранения неисправностей: теперь вместо нескольких недель это считаные дни.

– Компания Cisco взяла курс на повышение продаж программных продуктов и оказание ИТ-сервисов. Воспринимают ли российские корпоративные заказчики компанию как поставщика именно программных решений?

– Глобальная стратегия Cisco предусматривает предложение как можно большего количества программных продуктов и ПО по подписке. В России эта тенденция будет чуть менее выражена. Отчасти это связано с тем, что два-три года назад многие наши заказчики провели масштабное обновление инфраструктуры и пока работают по традиционной модели. В то же время стоит учитывать, что жизненный цикл оборудования снижается. Однако связано это не с его качеством, а с постоянным повышением требований к производительности сетей. Отмечу, что заказчики с большей легкостью меняют оборудование, получив возврат инвестиций, а пожизненная лицензия уже никому не нужна.

Более того, масштабируемая программная архитектура сетей позволяет по мере необходимости докупать и подключать любое ПО. По сути, мы предлагаем конструктор: продукты Cisco легко конфигурировать за счет программного обеспечения. Это отвечает потребностям современного заказчика, которому для повышения эффективности бизнеса и получения прибыли больше не нужно перестраивать сетевую инфраструктуру – достаточно оплатить подписку на нужный в данный момент софт.

Я не сталкиваюсь с тем, что нашу компанию воспринимают исключительно как производителя аппаратных решений. Наших клиентов скорее волнует, не уйдем ли мы в облако. На этот счет у нас очень ясная стратегия: практически все выпускаемые продукты Cisco доступны в облаке и по модели on-premise. При этом обновления для них выходят практически одновременно. Мы четко понимаем, что у наших крупнейших заказчиков есть частные облака, от использования которых они не откажутся, потому что такая инфраструктура дает им возможность быстро разворачивать сервисы в масштабах нашей большой страны. Для них мы также готовы предложить решения, которые будут работать в их облаке.

ITU TELECOM WORLD '19

Budapest 9–12 September

BETTER SOONER

ITU TELECOM WORLD 2019

The global event for governments, corporates and tech SMEs.

Accelerating ICT innovation to improve lives faster.

9-12 September 2019, Budapest, Hungary

ITU Telecom World 2018 is the global platform to accelerate ICT innovations for social and economic development. It's where policy makers and regulators meet industry experts, investors, SMEs, entrepreneurs and innovators to exhibit solutions, share knowledge and speed change. Our aim is to help ideas go further, faster to make the world better, sooner.

Visit telecomworld.itu.int to find out more.

#ituworld
telecomworld.int

Матрица на службе

Яков ШПУНТ

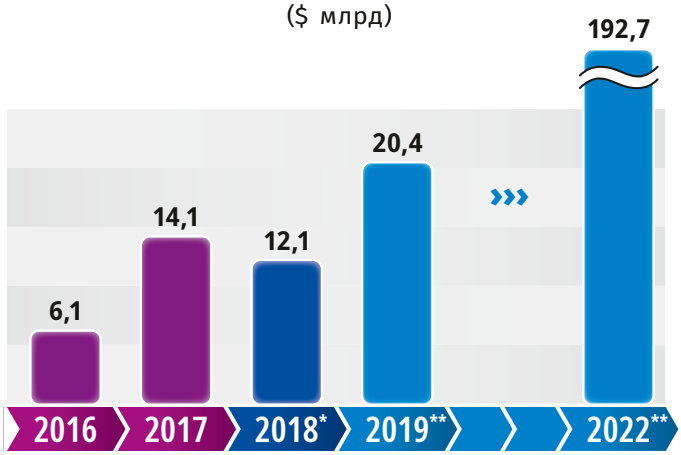
Технологии виртуальной и дополненной реальности (Virtual and Augmented Reality, VR/AR) уже применяются для решения реальных задач во множестве отраслей. Эти технологии эффективно сочетаются с концепцией цифровых двойников, которая в свою очередь стала новым этапом развития цифрового производства. Устройства виртуальной и дополненной реальности помогают анализировать работу того или иного объекта на всех стадиях его жизненного цикла, от проектирования до вывода из эксплуатации. Ремонтные и сервисные подразделения промышленных предприятий уже накопили успешный опыт применения данных технологий и существенно снизили издержки благодаря им.

Технологии виртуальной и дополненной реальности быстро развиваются и захватывают все новые ниши. Изначально предполагалось, что VR-технологии будут использоваться исключительно в сфере развлечений и сегмента инфотейнмент, однако им также нашлось место в промышленности, в строительстве и многих других областях. И вскоре VR/AR оказались в списке наиболее перспективных технологий для развития концепции «Индустрия 4.0».

Объем поставок устройств виртуальной реальности вышел на миллионы. По данным IDC, в 2018 году было продано более 4 млн таких устройств, из которых почти 2,8 млн пришлось на потребительский рынок, а более 1,2 млн – на корпоративный. По предварительным данным Tractica, в прошлом году объем глобального рынка VR для корпоративного применения в денежном выражении превысил $1 млрд, из которых 60% приходится на оборудование, а 40% – на ПО. При этом потенциал роста остается высоким: по прогнозам IDC, поставки VR-устройств до 2022 года в количественном выражении вырастут в 8 раз, а по оценкам Tractica, в 2025 году объем продаж таких устройств и ПО достигнет $12,6 млрд.

Объем мирового рынка виртуальной и дополненной реальности (VR/AR)

($ млрд)



*Предварительные данные
**Прогноз

Источник: Statista.com

Стоит отметить, что эти оценки были серьезно скорректированы в сторону снижения. В прогнозе Tractica на 2021 год, сделанном в 2016 году, объем продаж VR-устройств был запланирован на уровне $36 млрд в денежном выражении и 130 млн штук в количественном. Однако уход с рынка ряда заметных игроков и разочарование массовых потребителей в технологиях виртуальной реальности привели к тому, что в 2018 году объем рынка в количественном выражении снизился на треть.

Иная ситуация в сегменте AR. «Входным билетом» в мир этих технологий является наличие смартфона или планшета, счет которым идет на сотни миллионов. Благодаря этому AR-технологии сразу же после появления начали применяться в промышленности. Например, специальными приспособлениями, где обычная реальность сочеталась с искусственными графическими объектами, оснастили электриков, обслуживающих самолеты Boeing.

К тому же AR оказались лучше совместимы с физиологией человека, чем VR. Как результат, уже в середине 2010-х годов AR-решения стали по-настоящему массовыми, проникая в самые неожиданные, на первый взгляд, ниши. При этом их внедрение позволяло добиться заметной экономии финансов и времени.

Однако списывать VR со счетов преждевременно. Тем более что развитие этих технологий уже в ближайшем будущем позволит устранить значительную долю «узких» мест и снизить стоимость входа на этот рынок. Например, появляются специальные костюмы, позволяющие задействовать не только зрение, но и осязание.

Удобно, дешево и практично

Для применения на промышленных предприятиях интеллектуальные AR-устройства часто закрепляют на спецодежде и защитных средствах – как правило, на касках. Емкость аккумулятора таких устройств достаточна для автономной работы в течение всего рабочего дня, при этом руки и карманы сотрудников остаются свободными.

AR-устройства выпускают, в частности, международная компания Honeywell и российский интегратор «КРОК». «Каски с интеллектуальным устройством обеспечивают сотрудникам легкий доступ к инструкциям и рекомендациям, которые могут понадобиться для ремонта или обслуживания оборудования. Доступ обеспечивается через голосовые команды. Кроме того, такая гарнитура оснащена камерой, позволяющей техническому специалисту получать помощь от удаленных

Фото: Honeywell

По словам руководителя подразделения «Промышленная автоматизация» Honeywell в России и странах Таможенного союза Алексея Зенкевича, носимые устройства с VR/AR-технологиями помогают повысить продуктивность персонала на 15% и сократить количество потенциально опасных ситуаций на предприятии на 30%

Фото: Schneider Electric

Руководитель по развитию направления Datacenter Infrastructure Management (DCIM) подразделения Secure Power Schneider Electric Андрей Ивашов считает, что технологии AR более востребованы в промышленности за счет относительной легкости внедрения и возможности использовать смартфоны и планшеты без дополнения их очками или шлемами

экспертов, которые могут видеть то, что видит специалист. Также с помощью AR-технологий сотрудник может найти необходимые элементы установки и «увидеть насквозь» некоторые узлы, дорисовывая в виртуальном пространстве то, что скрыто корпусом шкафа или станка. Носимые VR/AR-устройства помогают повысить продуктивность персонала на 15% и сократить количество потенциально опасных ситуаций на предприятии на 30%», – так оценил эффект от внедрения систем руководитель подразделения «Промышленная автоматизация» Honeywell в России и странах Таможенного союза Алексей Зенкевич.

Руководитель по развитию направления Datacenter Infrastructure Management (DCIM) подразделения Secure Power Schneider Electric Андрей Ивашов считает, что AR в промышленности востребована благодаря относительной простоте внедрения и возможности использовать стандартные смартфоны и планшеты без какого-либо усложнения и дополнения их очками или шлемами. Он обозначил три сферы применения AR-решений: моделирование при разработке новых продуктов, обслуживание оборудования и повышение безопасности. «При этом пользователю не нужно разрабатывать дорогостоящую цифровую модель – достаточно создать виртуальные метки для ключевых точек в реальном мире. Например, при программировании какого-либо устройства достаточно добавить его описание и документацию, которые автоматически появятся на экране смартфона или планшета, когда пользователь наведет камеру на устройство, – отметил Андрей Ивашов. – Это можно использовать для обучения персонала, для снижения риска при производстве работ, для аудита и решения многих других задач».

По словам руководителя команды AR-разработки АО «Бэлл Интегратор» (Bell Integrator) Александра Сенченко, успешные кейсы в AR – это не редкость. Один из них – реализованный Bell Integrator проект по созданию мобильного приложения по подбору колесных дисков для американской компании Icon-Media. Приложение позволяет понять, насколько хорошо диски будут смотреться на авто. Для этого нужно просто навести камеру смартфона на автомобиль: нейронная сеть распознает модель и марку машины и предлагает имеющиеся в наличии диски, подходящие по типоразмеру. Другой проект Bell Integrator выполнил для сотового ретейлера, внедрив разнообразный AR-функционал с целью увеличения продаж в розничных точках. Александр Сенченко напомнил об AR-проектах Ikea и Leroy Merlin, благодаря которым можно визуализировать в квартире элементы интерьера из каталогов компаний. Компания «Яндекс» использует AR в навигации, а Danone – в рекламе молочных продуктов под брендом «Растишка».

Как отметил исполнительный директор SAP CIS Дмитрий Красюков, AR все чаще применяют кадровые службы компаний, представляя персоналу новых сотрудников.

Руководитель отдела «Мультимедийные системы и видеоконференцсвязь» ООО «ЛАНИТ-Интеграция» Леонид Жестев рассказал, что с 2018 года компания реализовала на российских предприятиях большое количество проектов с использованием AR, в том числе внедрила такие сервисы, как «удаленный помощник», «приложение электронного наряда-допуска», «интерактивная карта ремонта оборудования».

Визуализация для цифрового двойника

В промышленности доводка оборудования по традиционной технологии идет через натурные испытания, для проведения которых необходимы специальные полигоны или подготовленные помещения, а также изготовление прототипов. Все это вместе занимает много времени и требует серьезных финансовых вложений. Оцифровка позволяет заменить натурные испытания виртуальными, которые моделируют работу изделия под воздействием различных факторов.

Настоящий прорыв произошел в начале 2000-х годов, когда появилась и быстро нашла практическое применение технология цифровых двойников.

Цифровой двойник представляет собой не просто виртуальную модель объекта, в качестве которого может выступать агрегат, установка, цех, предприятие, город или даже страна, а совокупность всех имеющихся сведений о физическом объекте, от момента его проектирования до вывода из эксплуатации.

Интересно, что первой сферой успешного применения цифровых двойников стало проектирование и эксплуатация ЦОДов. Пионерами в этой области стали IBM и APC, тогда еще независимая компания, позднее поглощенная Schneider Electric. «Решение EcoStruxure IT Expert позволяет пользователю сравнить состояние батарей в источниках бесперебойного питания с состоянием аналогичных элементов у других пользователей – точнее, с усредненной моделью. Если срок жизни собственных батарей ниже, чем у модели, то это веская причина применить меры для исправления ситуации», – делится опытом Schneider Electric Андрей Ивашов.

Леонид Жестев предупреждает, что создание модели – самый простой шаг при разработке цифрового двойника. На следующем шаге необходимо объединить полученную модель с существующей системой датчиков, а также с системами управления производством (Manufacturing Execution System, MES) и ресурсами (Enterprise Resource Planning, ERP), с решениями видеоаналитики и IoT. Однако специалист «ЛАНИТ-Интеграции» убежден, что результат того стоит: «Такой подход позволит получать полную информацию о состоянии производства, контролировать и предупреждать возникновение нештатных ситуаций».

«Ключевой элемент цифрового двойника – матрица целевых показателей и ресурсных ограничений. В сложной технической системе количество этих показателей может доходить до 50 тыс., в отличие от традиционного варианта, где их всего около 500», – отметил проректор по перспективным

26

Фото: SAP CIS

Исполнительный директор SAP CIS Дмитрий Красюков отмечает, что для реализации VR/AR-технологий нужна сложная инфраструктура: каналы передачи данных, системы их накопления и обработки, оборудование для визуализации, специальное программное обеспечение для построения 3D-моделей, а в некоторых случаях и специально подготовленные помещения

Фото: «КРОК»

Директор центра виртуальной реальности (CROC VR) АО «КРОК инкорпорейтед» Илья Симонов обратил внимание на то, что VR-проекты имеют более длительный горизонт окупаемости, чем другие цифровые инициативы, и не сразу можно оценить их влияние на бизнес

проектам Санкт-Петербургского политехнического университета Петра Великого Алексей Боровков, выступая на форуме «Открытые инновации 2018». Данные собираются с устройств IoT, в том числе в период эксплуатации изделия, за счет чего цифровой двойник становится еще «умнее».

При этом создание прототипа изделия для виртуальной реальности требует серьезной вычислительной мощности и высокой пропускной способности сети. Например, для продуктивной работы с отечественной системой трехмерного виртуального прототипирования VR Concept требуется рабочая станция на основе процессора Intel Xeon с 64 Гб оперативной памяти и профессиональным трехмерным ускорителем nVidia Quadro или AMD FireGL. Для аналогичных решений, представленных в апреле этого года на II Всероссийском фестивале виртуальной и дополненной реальности VRAR Fest, разработчики озвучили схожие требования к оборудованию.

Дополненная реальность отображает данные, полученные с цифровых двойников, которые накапливают огромное количество информации об оборудовании. По словам исполнительного директора SAP CIS, это позволяет осуществить целый комплекс сценариев. «Например, можно организовать помощь при проведении сложных ремонтов. В таких случаях у сотрудника в AR-очках отображаются интерактивные инструкции к конкретному оборудованию. Кроме того, можно подключить коллег, которые могут в онлайн-режиме наблюдать за действиями находящегося на объекте сотрудника и давать необходимые рекомендации. Другой интересный сценарий – управление складом: с помощью AR-технологий сотрудник видит маршрут до нужного ему объекта, может считать штрих-код с товара и получить по нему полную информацию. В энергетике технологии визуализации востребованы полевым персоналом, потому что позволяют получить доступ к информации, хранящейся в компьютерных системах, и работать с ней, не отвлекаясь от непосредственной задачи. Например, совместно с «МРСК Сибири» мы сделали прототип цифрового трансформатора, на котором специалисты могут оттачивать навыки работы с оборудованием подстанций. А находясь на объекте электромонтер в режиме реального времени получает сведения о текущем состоянии оборудования и принимает решение о необходимости его ремонта. Это позволяет компании снизить риск аварийных и смертельных случаев на производстве, а также повысить контроль за действиями ремонтного персонала, – делится опытом реализации проектов Дмитрий Красюков. – Для металлургии и энергетики актуален сценарий диспетчерских, которые обычно представляют собой помещение с дорогостоящей видеостеной. На нее выводится множество данных, но представлены они мелко, и отдельные данные сотрудникам приходится смотреть на компьютере. Очки дополненной реальности позволяют сделать процесс более гибким: сотрудник, во-первых, может менять размер изображения, а во-вторых, сидя за компьютером одновременно видеть интерактивную стену. Еще один сценарий – интерактивная отчетность для руководства компаний. Он позволяет в онлайн-режиме анализировать данные, полученные с предприятия, и видеть их поверх 3D-моделей».

«Для «СИБУР Холдинга» мы разработали цифровую модель крупнейшего производственного комплекса компании – «ЗапСибНефтехима». Она основана на иммерсивных технологиях и воссоздает производственные процессы, сооружения и инфраструктуру комплекса, включая установку пиролиза, мощности по производству различных марок полиэтилена и полипропилена. Такой уровень детализации позволяет увидеть практически любой процесс или объект», – рассказывает о проекте в нефтехимическом холдинге директор центра виртуальной реальности (CROC VR) АО «КРОК инкорпорейтед» Илья Симонов. По его словам, в дальнейшем похожие программно-аппаратные комплексы могут использоваться для решения широкого спектра задач цифровой трансформации. «При объединении модели с данными систем MES, ERP и АСУ ТП, с данными видеоаналитики и IIoT можно получать единую картину о состоянии производственных активов и отслеживать взаимодействие различных процессов и устройств», – говорит глава CROC VR.

Алексей Зенкевич отмечает, что технологии дополненной и виртуальной реальности позволят принципиально по-новому работать с данными цифровых двойников.

Распределение мирового рынка VR/AR

($ млрд)

Источник: Statista.com

«С появлением VR и AR взаимодействие с моделью больше не будет ограничено двухмерным пространством компьютерного экрана. Визуализация модели VR/AR-средствами в сочетании с оперативным обновлением данных, полученных по каналам Интернета вещей, кардинальным образом изменит принципы эксплуатации, обслуживания и ремонта в рамках жизненного цикла изделий», – пояснил руководитель подразделения «Промышленная автоматизация» Honeywell.

Леонид Жестев видит большие перспективы VR/AR-технологий в сфере управления городской средой – за счет объединения решений визуализации с большим количеством городских систем (водоснабжения, электрификации, видеонаблюдения, анализа дорожной обстановки, управления светофорами и городским освещением), которое выведет управление комплексом систем на новый уровень. Представитель компании «ЛАНИТ-Интеграция» считает, что в результате полученные данные помогут оптимизировать внутренние городские процессы. Например, «умное» управление светофорами может ускорить движение машин скорой помощи. «Совмещение данных из разных источников в подобном комплексе и сбор статистики позволят получать предиктивную аналитику жизни города и обеспечивать гармоничное развитие городской инфраструктуры», – уверен эксперт. Что касается сферы производства, то здесь, по мнению Леонида Жестева, на основе подобной модели можно проводить обучение сотрудников в области охраны труда и промышленной безопасности. Кроме того, можно использовать такие модели для оптимизации производственных цепочек.

VR: возможности и ограничения

В бизнесе VR-решения в основном применяются для разного рода тренажеров. С их помощью готовят военных и гражданских пилотов, врачей (стоматологов и хирургов), специалистов, обслуживающих дорогое и редкое оборудование; их используют для отработки действий в условиях разного рода нештатных и чрезвычайных ситуаций. Одним словом, VR-технологии применяют там, где обучение на реальных образцах обходится очень дорого или сопряжено с опасностью для жизни. Не менее актуальна возможность добиться за счет VR имитации различных явлений, в том числе невесомости или давления внутри скафандра. Важно и то, что у VR-решений довольно длительный жизненный цикл.

Как отмечает Александр Сенченко, сейчас дешевле написать приложение, чем отправлять персонал на обучение. Тем более что всегда есть резервы для снижения стоимости решения – например, за счет использования бесплатного ПО. Более того, как подчеркнул Алексей Зенкевич, с появлением VR и AR взаимодействие с моделью больше не ограничено двухмерным пространством компьютерного экрана.

Руководитель отдела продуктов НТС в России и СНГ Николай Блохин в своем выступлении на VRAR Fest напомнил об эксперименте профессора Государственного университета Огайо Эдгара Дейла. Согласно результатам эксперимента, через две недели студент забывает 95% того, что услышал на лекции, и 90% того, что прочитал в учебнике, однако если студент «прожил» ту или иную ситуацию, то забывает лишь 10% материала. Николай Блохин подчеркнул, что технологии виртуальной реальности как раз позволяют «прожить» ту или иную ситуацию, что многократно повышает эффективность обучения для всех возрастов.

Однако одними только тренажерами сфера применения VR не ограничивается. «Виртуальная реальность применяется в области проектирования сложных технологических комплексов – от объектов атомной промышленности до морских судов. Широко распространены решения на основе Tech-Viz, позволяющие рассматривать объекты проектирования в едином трехмерном пространстве и совмещать данные

Дивный новый мир

Фото: СТАНДАРТ

В середине марта оператор МТС запустил в режиме beta-тестирования медиаплатформу для геймеров и любителей киберспорта WASD.tv, на которой можно смотреть и создавать видеотрансляции игрового процесса. МТС рассчитывает, что WASD.tv станет прибыльной через два-три года.

Признаться, я сравнительно недавно узнала о существовании стриминговых платформ, на которых «вещают» обычные пользователи. И больше всего меня удивило даже не то, что кто-то хочет наблюдать подобный контент, а что за это готовы вносить пожертвования (донаты).

В России, согласно исследованию «Яндекс.Кассы» и Data Insight, в 2018 году около 10 млн человек жертвовали другим пользователям за просмотр того, как те проходят игры. Всего насчитывается около 2 тыс. популярных русскоязычных стримеров, личный доход которых достигает миллионов рублей в месяц. В основном стримы смотрят на платформе Twitch и YouTube.

Зарабатывают на подобных сервисах и бизнесмены. Например, выручка крупной китайской стриминговой платформы YY в 2018 году составляла 15,76 млрд юаней ($2,29 млрд), а чистая прибыль – 1,64 млрд юаней ($239 млн). Акции компании торгуются на NASDAQ, а ее капитализация по данным на середину апреля этого года составляла $6,98 млрд.

Платформа YY собирает 90,4 млн активных пользователей в месяц. В отличие от других стриминговых сервисов популярностью здесь пользуются не только стримы про игры, а самый разнообразный контент. Недавно я посмотрела документальный фильм про эту платформу – «Народная республика желания». В центре истории – два популярных стримера платформы: певица и юморист. Им удается зарабатывать на платформе десятки, а то и сотни тысяч долларов в месяц. Что они для этого делают? На первый взгляд кажется, что практически ничего: садятся перед экраном компьютера и начинают болтать; то песню запоют, то подарки попросят у других пользователей. Но по ходу повествования понимаешь, что герои могут лишиться популярности на платформе так же легко, как и получили ее: симпатия аудитории в одночасье может смениться ненавистью. Основную часть прибыли благодаря стримерам получают не они сами, а платформа и специальные агентства по продвижению пользователей.

При этом популярные стримеры выглядят глубоко несчастными людьми, которым в реальном мире не хватает любви близких и преданности друзей. Внезапно разбогатевшие герои платформы похожи на новых русских из 1990-х годов. Они тратят деньги на позолоченные предметы интерьера, дорогие автомобили и бриллианты, а их уровень культурного развития остается довольно низким: они чавкают, редко принимают душ и, похоже, не чистят зубы.

Третий герой «Народной республики желания» – фанат юмориста. Это мигрант, который вынужден работать с утра до ночи практически без выходных за $400 в месяц, и из этой небольшой суммы он умудряется выделять деньги на пожертвования юмористу. Фанат переживает, что его кумир никак не может занять первое место по популярности на YY. Стримы он смотрит с экрана мобильного телефона, и это чуть ли не единственное развлечение, доступное ему в жизни.

Анна Балашова,
редактор отдела телекоммуникаций РБК, специально для «Стандарта»


Фото: «Бэлл Интегратор»

Руководитель команды AR-разработки АО «Бэлл Интегратор» (Bell Integrator) Александр Сенченко считает, что в военном деле технология искусственной реальности просто необходима: возможно, в дальнейшем с ее помощью будет полностью прорабатываться любое военное действие


Фото: «ЛАНИТ-Интеграция»

Руководитель отдела «Мультимедийные системы и видеоконференцсвязь» ООО «ЛАНИТ-Интеграция» Леонид Жестев подчеркнул, что при создании цифрового двойника разработка модели объекта – самый простой шаг; на следующем этапе необходимо объединить модель с системой датчиков, а также с системами управления производством и ресурсами, с данными видеоаналитики и IoT

из большинства распространенных систем автоматизированного проектирования в онлайн-режиме», – напомнил Леонид Жестев. Причем стоит отметить, что сочетание VR с технологиями цифровых двойников и цифровых прототипов дает синергетический эффект.

Однако в отличие от ситуации с AR, широкому распространению VR препятствует ряд труднопреодолимых факторов – дороговизна устройств виртуальной реальности, их малая автономность, плохая эргономика. «Часто возникали сложности, связанные с необходимостью обеспечить физическую защиту пользователя в системах с эффектом полного погружения. Кроме того, в силу особенностей сенсорных систем организма, у человека может возникать ощущение укачивания, к тому же VR-устройства не передают тактильные ощущения и только частично воссоздают звуковые образы. Несмотря на эти ограничения, само оборудование стоит дорого, а также возникают сложности с масштабируемостью решений», – по мнению Алексея Зенкевича, такие недостатки больше всего мешают внедрению VR.

«Пока все модели устройств, которые представлены на рынке, оставляют желать лучшего с точки зрения их массы, габаритов, энергонезависимости, качества визуализации контента, – сетует Дмитрий Красюков. – Более того, для реализации VR/AR-технологий нужна достаточно сложная инфраструктура: каналы передачи данных, системы их накопления и обработки, оборудование для визуализации, специальное программное обеспечение для построения 3D-моделей. А в некоторых случаях требуются и специально подготовленные помещения».

Илья Симонов отмечает, что экономический эффект от внедрения VR не всегда прозрачен: «VR-проекты имеют более длительный горизонт окупаемости, чем другие цифровые инициативы, и их влияние на бизнес можно оценить не сразу. Более широкое проникновение VR/AR-технологий станет возможным с появлением на предприятиях необходимой инфраструктуры и платформ, ориентированных на стек XR-технологий. Помимо этого, необходимы изменения в производственной культуре, программы адаптации сотрудников к работе с цифровыми технологиями и развитие у персонала цифровых навыков».

Андрей Ивашов отмечает, что VR-технологии менее востребованы для массового промышленного применения, поскольку требуют создания сложной цифровой модели и схемы поведения в ней пользователя. Специалист Schneider Electric подчеркнул, что затраты на внедрение сложного оборудования высоки, поэтому применение VR-технологий целесообразно только в том случае, если сотрудник не может или не должен физически находиться в реальном окружении.

Есть и другие сложности. В частности, многие участники VRAR Fest отметили, что создание VR-контента на 80-90% зависит от дизайнеров с довольно специфичными навыками, а таких специалистов пока не готовят ни технические, ни художественные вузы.

Многие из обозначенных сложностей со временем будут преодолены, уверен Николай Блохин. Например, уже сейчас можно транслировать VR-контент на любой экран, в том числе на экран смартфона, и такая трансляция существенно повышает требования к пропускной способности сети, однако с появлением инфраструктуры связи 5G это перестанет быть проблемой. Соответственно, можно будет создать полностью беспроводную систему с поддержкой VR, обладающую высокой автономностью.

Уход в искусственную реальность

Следующий шаг на пути развития данного вида технологий – моделирование полностью искусственной реальности (Simulated Reality).

Причем Simulated Reality уже нашла область применения: стало известно, что IBM использовала для проектирования суперкомпьютеров RoadRunner и Watson визуализированные 3D-модели в стиле миров, которые необходимо строить в играх семейства The Sims. Это одно из первых практических применений технологии цифровых двойников, дополненной интерактивной визуализацией.

Андрей Ивашов полагает, что Simulated Reality будет востребована в ресурсоемких областях, где применяются сложные технологические решения с большим разнообразием модулей и элементов. Это многие виды производства, химическая промышленность, сложная переработка.

«Обучающие курсы и приложения с применением компьютерной симуляции (serious games) и VR-технологий помогают снизить влияние человеческого фактора на производственные процессы. Интерактивное погружение и вовлечение, построенные на геймификации, помогают отрабатывать профессиональные навыки или коллективные действия персонала в условиях нештатной ситуации. Если говорить о развитии гибких навыков сотрудников, например, в банковском секторе или телекоме, то иммерсивные тренажеры помогают отработать сложные ситуации, связанные с обслуживанием клиентов», – уверен Илья Симонов.

Алексей Зенкевич отметил, что виртуальные инструменты позволяют находить новые решения и проводить испытания до запуска реального производства. Благодаря этому можно повысить эффективность работы предприятия и гарантировать выпуск лучшей продукции, которая точно будет соответствовать потребностям конечного пользователя. При этом открываются блестящие перспективы – в частности, можно устранить прогнозируемые проблемы до того, как они возникнут на самом деле.

«В военном деле технология искусственной реальности просто необходима. Возможно, в дальнейшем любое военное действие будет полностью прорабатываться с помощью данной технологии», – таким видит будущее Александр Сенченко.

Организатор:

10 лет COMNEWS CONFERENCES

Стратегический партнер:

МегаФон

Спонсор сессии:

OrionM2M

Бизнес-форум Smart City & Region Сочи

14 июня 2019
отель «Swissôtel Resort Сочи Камелия»
Сочи,
Курортный пр., д. 89

Цифровые технологии на пути к «умной» стране

Ключевые темы форума:

- Smart country, Smart city – разработка концепции и масштабирование успешных моделей
- Вклад региона и города в реализацию национальной программы «Цифровая экономика»
- Первые практические результаты внедрения проектов «умный» город
- Решения на службе «умного» города. Практический опыт интеграции
- Телекоммуникационная инфраструктура для «умных» городов
- Возможности создания типовых сценариев и продуктов для «умного» города
- Новые возможности для операторов – владельцев информационной инфраструктуры при реализации проектов «умный» город и «умный» регион
- Возможности регионального бизнеса и бизнес-объединений для цифровизации региона

Спикеры:

Евгений Борисов,
директор по развитию,
Фонд развития интернет-инициатив (ФРИИ)

Андрей Дорошев,
заместитель главы муниципального образования город Краснодар,
Администрация города Краснодар

Владимир Зарубин,
заместитель директора Департамента координации и реализации проектов по цифровой экономике,
Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Александр Зорин,
директор по региональной политике,
АНО «Цифровая Экономика»

Григорий Микрюков,
начальник управления отраслей экономики,
Аналитический центр при Правительстве Российской Федерации

Александр Минов,
генеральный директор,
АО «Национальный исследовательский институт технологий и связи»

Александр Молчанов,
директор по развитию Краснодарского филиала,
ПАО «Ростелеком»

Евгений Панасенко,
старший менеджер,
EY

Александр Похлебаев,
начальник управления информатизации и связи,
Администрация города Сочи

Евгений Юшков,
руководитель,
Департамент информатизации и связи Краснодарского края

При поддержке:

ITU

Администрация города Сочи

фрии

РУС СОФТ

НАДИКС

Международная Академия Связи

яИТы
КЛУБ IT&DIGITAL ДИРЕКТОРОВ

iotas

Для регистрации: +7 495 933 5483, conf@comnews.ru, www.comnews-conferences.ru/smartsochi2019

Готовь сайты загодя

Во второй половине апреля 2019 года компания Huawei во второй раз провела в Москве мероприятие Russian Mobile Network Infrastructure Ecosystem Forum. Его задачей стал диалог с мобильной экосистемой о том, как лучше подготовить сетевую инфраструктуру и сайты к скорому запуску сетей пятого поколения (5G). На полях форума о ключевых темах в этом направлении главному редактору «Стандарта» Леониду КОНИКУ рассказали три менеджера Huawei Russia – вице-президент по маркетингу и продажам бизнес-решений Лу ЛИБО, руководитель департамента сетевых технологий Чжан ФАНЬ и директор отдела по решениям беспроводных сетей Лю ЮНГАН.

– Как вы оцениваете состояние и готовность российского рынка к внедрению технологии 5G?

Лу Либо:
Huawei участвует в большом количестве форумов и конгрессов по мобильной тематике, включая те, где выступают руководители сотовых компаний, и мы видим, что повсеместно самый горячий аспект – это радиочастотный спектр. Более сорока стран уже выдали частоты для сетей 5G или анонсировали четкий план их распределения, и во многих государствах правительства сделают это до конца года. Причем речь идет не только об С-диапазоне (3,4-3,8 ГГц, – *прим. «Стандарта»*) – некоторые страны распределяют для создания 5G-сетей частоты в полосах 600 МГц, 700 МГц, 2,3 ГГц, 2,6 ГГц, 4,5 ГГц, 4,9 ГГц, и это очень интересно. Так что на первом месте в вопросе готовности к 5G – в том числе в России – стоит спектр.

Следующий важный вопрос, который обсуждается повсеместно, – варианты применения сетей 5G (use cases), то есть то, как можно сделать с их помощью бизнес. Ведь даже если какой-то оператор получил частоты, имеет инвестиции и знает, как заработать на 5G, он не сможет развернуть сеть за одну ночь – это невозможно. Поэтому готовиться нужно заранее. Именно поэтому в конце апреля текущего года Huawei, уже во второй раз, провел в России форум, посвященный инфраструктуре для сотовых сетей – Russian Mobile Network Infrastructure Ecosystem Forum 2019. На этом мероприятии мы поделились с российскими операторами, башенными компаниями и регуляторами идеями об эффективных способах создания сетевой инфраструктуры для 5G – о том, что необходимо делать уже сейчас, чтобы поддержать будущий 5G-бизнес.

Фото: Huawei

Чжан Фань,
руководитель департамента сетевых технологий Huawei Russia:
«Около 70% сотовых сайтов в мире имеют проблемы с местом для размещения новых базовых станций»

– Вы обозначили множество частотных диапазонов для 5G. Видите ли вы риски того, что в случае применения для сетей 5G различных полос частот в разных странах возникнут проблемы с роумингом?

Лу Либо:
В конечном счете все участки спектра должны пройти рефарминг в 5G – вопрос только в том, в какие сроки это произойдет в различных регионах, а это зависит от регулирующих органов и правительств. Технически наше оборудование может работать в любом из названных частотных диапазонов. К примеру, в Канаде наши клиенты-операторы получили спектр 600 МГц, и мы поставляем им оборудование с поддержкой этого диапазона.

– Вы говорите о сетевом оборудовании. А способны ли смартфоны Huawei поддерживать все частотные диапазоны?

Лу Либо:
В январе 2019 года Huawei запустил для смартфонов серии Mate чипсеты Kirin 980 и Balong 5000, которые поддерживают любые частотные диапазоны ниже 6 ГГц.

– Каковы особенности создания сайтов для сетей 5G?

Чжан Фань:
Эта задача значительно отличается от организации сайтов для сетей предыдущих поколений. При использовании существующих площадок для 5G будут возникать проблемы, связанные со свободным местом, несущей способностью и электрической мощностью. По нашей статистике, около 70% сотовых сайтов в мире имеют проблемы с местом для размещения новых базовых станций. В России особые сложности будут возникать с площадками на крышах зданий и с отдельно стоящими опорами. При этом российский офис Huawei за последние годы приобрел богатый опыт в развертывании сайтов для мобильных сетей. Наши возможности позволяют создавать в любом крупном российском городе свыше 300 базовых станций в месяц – такие масштабы обеспечивают инновационные ИТ-инструменты и сеть партнеров. Когда сети 5G станут в России коммерческой

реальностью, Huawei сможет преодолеть все сложности, построить хорошие сети и помочь стране достичь полной подключенности.

– Huawei в последнее время часто говорит об открытых сайтах. Что имеется в виду?

Чжан Фань:
До сих пор создание сайтов было весьма тривиальной задачей, но в будущем это изменится – по мере того как для 5G будут использоваться частоты выше 26 ГГц. Зона охвата базовой станции и проникновение сигнала в столь высоких частотных диапазонах очень ограничены. Это означает, что операторам придется искать гораздо более гибкие площадки для новых сайтов, и этот процесс нужно максимально упростить. Мы считаем, что Huawei может в этом помочь.

Лу Либо:
На протяжении двух последних лет мы помогали нашим заказчикам в создании сайтов в одном крупном российском городе. И теперь мы не понаслышке знаем, как непросто вести переговоры об установке новых базовых станций с владельцами земли и объектов недвижимости. У них есть масса ограничений по весу и размерам оборудования, а подчас они и вовсе требуют, чтобы оно было спрятано. Huawei имеет опыт оптимизации решений под различные специфические требования.

Из общения с башенными компаниями мы выяснили, что они используют опоры высотой 30-39 метров, но иногда владельцы недвижимости против столь высоких конструкций. У Huawei есть мощное оборудование, которое может покрыть равную территорию при подвесе на меньшей высоте – и тогда можно обойтись без высоких мачт. Мы считаем, что необходимо выработать стандарты и согласовать их между всеми сторонами – операторами, владельцами недвижимости и вендорами. Это упростит создание новых сайтов. В портфеле Huawei есть такие уникальные решения как семейство компактных базовых станций LampSite – их можно спрятать даже в рекламную конструкцию (так, к примеру, сделал один оператор во всех своих салонах в Санкт-Петербурге). Никогда прежде не существовало столько эффективных способов создания сайтов. Это мы и называем решениями для открытых сайтов.

– Несколько лет назад активно обсуждалась тема устройства базовых станций на уличных конструкциях – например, на рекламных щитах и остановках общественного транспорта. Актуальна ли она сейчас?

Чжан Фань:
Да, конечно. У нас есть опыт размещения LampSite в уличных рекламных щитах в России. Автобусные остановки также пригодны для этого: к ним обычно подведено электричество, часто бывают небольшие опоры с табло, и они весьма прочные. В отличие от зданий или земельных участков, у которых разные владельцы, автобусные остановки управляются городским правительством или единой инфраструктурной компанией, поэтому оператору удобно договариваться о размещении сразу на множестве конструкций.

К тому моменту когда сети 5G станут массовым явлением, мы намерены разработать решения, удовлетворяющие всем потребностям операторов и требованиям владельцев любых объектов инфраструктуры.

Лу Либо:
Из общения с сотовыми компаниями я знаю, что они заинтересованы не только в создании новых сайтов, но и в 100%-ном переиспользовании уже построенной инфраструктуры. И решения вендоров должны быть пригодны для размещения не только на новых площадках, но и на существующих – мы в Huawei об этом заботимся.

Лю Юнган:
Не менее важный вопрос – новые типы оборудования, гарантирующие емкость и другие показатели. При этом мы должны уменьшить количество шкафов и иных конструкций – ограничения по размерам оборудования являются одним из ключевых вызовов для сотовых компаний по всему миру. И самое узкое место здесь – антенна. Huawei недавно вывел на рынок решение, которое интегрирует все частотные диапазоны и поколения (2G, 3G, 4G, 5G) в одной антенне: мы называем его All-in-One Antenna. Оно критически важно для развертывания сетей 5G в ближайшем будущем: за счет его применения мы сокращаем затраты оператора на развертывание сети.

В то же время операторы модернизируют действующие сети, и мы советуем им использовать новое оборудование с поддержкой эволюции в 5G. И если оператор в будущем захочет задействовать имеющийся спектр для сети пятого поколения, то ему не придется менять оборудование – достаточно будет простого программного обновления.

– Увеличение количества сайтов ведет к росту энергопотребления. Это грозит ростом затрат оператора, а в некоторых регионах есть ограничения по доступной электрической мощности. Какие вы видите способы решения этой проблемы?

Фото: Huawei

Лу Либо,
вице-президент по маркетингу и продажам бизнес-решений Huawei Russia:
«Необходимо выработать стандарты для сайтов и согласовать их между всеми сторонами – операторами, владельцами недвижимости и вендорами»

Лю Юнган:
Энергопотребление – одна из существенных статей операционных затрат оператора. В прошлом году Huawei запустил решение, основанное на искусственном интеллекте (ИИ). Бывает, что в течение целого дня через определенную базовую станцию практически нет трафика, но оборудование все равно работает и постоянно потребляет электричество. Теперь, применяя ИИ, мы можем контролировать энергопотребление: когда трафика нет, оборудование временно отключается – можно сказать, переходит в режим сна, а как только он появляется – все немедленно включается.

Лу Либо:
Мы формулируем цель так: 0 бит = 0 ватт, то есть нулевой объем затрат для оператора.

Лю Юнган:
Мы уже внедрили это решение в нескольких странах, а в России ведем переговоры о его поставке с несколькими операторами. Первый практический опыт применения этого ИИ-решения показывает, что оператор может экономить 15-20% энергопотребления.

32

Фото: Huawei

Лю Юнган,
директор отдела по решениям беспроводных сетей Huawei Russia:
«Применяя искусственный интеллект, Huawei контролирует энергопотребление: когда трафика нет, базовая станция временно отключается»

Лу Либо:
Особенно актуально такое решение для действующих сайтов, на которых размещено оборудование 2G, 3G и 4G. Добавление аппаратуры 5G приводит к росту энергопотребления и требует монтажа нового энергетического оборудования и новых аккумуляторных батарей. Используя решение на базе ИИ, мы хотим сохранить потребление электроэнергии при запуске 5G на уровне работы сетей стандарта 4G и даже сделать его ниже. Это избавит операторов от дополнительных расходов на системы электропитания.

– Есть ли новые способы оптимизации стоимости владения (TCO) сайтами?

Лу Либо:
Мы постоянно слышим от операторов, что действующие опоры полностью заняты оборудованием и при расширении сети нет никакой возможности разместить что-либо дополнительно. В этом году Huawei вывел на рынок модернизированный блок базовых станций (BBU). Прежде оператор был вынужден покупать 19-дюймовый шкаф и размещать BBU в нем. Наше новое решение работает в режиме outdoor: оно выглядит как пластина, и мы можем смонтировать его вместе с выносным радиочастотным блоком (RRU). Аккумуляторы и система питания раньше также монтировались в шкаф, а теперь мы можем установить их вместе с RRU. Про единую антенну для всех диапазонов и поколений мы уже сказали. Бывают случаи, когда дополнительную антенну просто невозможно поставить, поскольку владелец недвижимости не позволяет это сделать. Антенна All-in-One, вкупе с технологией Massive MIMO, полностью снимает эту проблему.

– Большинство операторов в мире сходятся во мнении, что базовым частотным диапазоном для сетей 5G будет 3,4-3,8 ГГц, а также миллиметровый диапазон выше 26 ГГц. Как в этих условиях строить сети вне больших городов, в сельской местности?

Лю Юнган:
Этот вопрос актуален в глобальном масштабе, и операторы оценивают затраты на создание сотовых сетей сельской связи. И получается, что возвратность инвестиций (RoI) для таких сценариев, мягко говоря, невелика. Скажем, для России RoI в этом случае составит около 10 лет, а это очень долгий срок. И мы в Huawei поняли, что нужно улучшить множество аспектов, включая передающее оборудование, систему питания и количество модулей. Исходя из этих соображений, мы разработали решение под брендом RuralStar. Традиционные радиорелейные системы передачи в нем заменены на eRelay. Высота подвеса существенно уменьшена: в большинстве случаев одна опора с лихвой покрывает всю деревню. Изменена и система питания: на смену привычным дизель-генераторам пришли солнечные батареи. И наконец, мы способны уместить все диапазоны и поколения сотовой связи в один физический модуль. С помощью такого решения мы можем сократить RoI для сотовой связи в сельской местности с десяти до трех лет. Мы уже запустили пилотные зоны с решением RuralStar в России с несколькими операторами.

Лу Либо:
Конечно, для загородной местности наиболее эффективны низкие частотные диапазоны. К примеру, в Казахстане правительство выдало разрешение на использование спектра 800 МГц компании «Казахтелеком». Наша идея заключается в том, что нужно переиспользовать диапазоны 700 МГц, 800 МГц и даже 900 МГц для новых сотовых технологий. Не обязательно полностью отказываться от предыдущих поколений связи: например, в полосе 900 МГц можно одновременно использовать проверенную временем технологию GSM и LTE.

– В России для сотовой связи также используется диапазон 450 МГц. Видите ли вы эффективность его применения для сетей 5G, а не только для LTE?

Лу Либо:
Важно, попадает ли диапазон в глобальную экосистему, особенно с точки зрения конечных устройств. Ни для 3G, ни для 4G, ни для 5G полоса 450 МГц не стала мейнстримом. Технически нет никакой сложности в том, чтобы построить сеть 5G на частоте 450 МГц, но без широкой и доступной экосистемы не будет абонентов, а без абонентов не будет бизнеса. И это никому не интересно.

– Каковы ваши прогнозы развития 5G в России?

Лу Либо:
Мы уже представили в России новые решения и технологии и обсуждаем, как помочь нашим заказчикам быстро внедрить 5G. Именно поэтому мы задумываемся о том, как оптимизировать инфраструктуру и с чего начинать. Но даже если технология идеальна, без ее понимания людьми, без талантливых инженеров ее не развернуть. Поэтому мы начали проводить тренинги по 5G, рассказывая об особенностях технологии, монтажа и бизнеса.

Чжан Фань:
Для этих целей Huawei стал применять очки виртуальной реальности (VR) – чтобы кастомизировать инсталляционные процедуры: от сбора и доставки отдельных элементов на сайт до монтажа. Задача заключается в том, чтобы на каждом шаге обеспечивался контроль качества и соблюдались регламенты. Чем быстрее операторы запускают сайты, тем быстрее начинают получать от них финансовую отдачу.

– Верите ли вы, что в России появятся корпоративные сети 5G, наподобие TETRA или DMR?

Лу Либо:
Это тонкий вопрос. В конце концов 5G – это просто технология. Она может поддерживать различные бизнес-модели, но все зависит от конкретной ситуации. В частности, важный вопрос заключается в том, будет ли правительство выдавать радиочастотный спектр корпорациям, либо его получат только операторы. С технической точки зрения, сети 5G могут строить и эксплуатировать самые различные структуры. Так же как и сети по технологии LTE: стандарт eLTE разработан Huawei специально для корпоративных беспроводных сетей передачи данных.


GSMA
MWC19™
Shanghai • 上海
26-28 June 2019 • 2019年6月26-28日
WELCOME TO THE ERA OF
INTELLIGENT
CONNECTIVITY
MWCSHANGHAI.COM
ADVERTISEMENT
MWC Shanghai 2019 is Asia's leading event for next-generation technology – 5G, IoT, AI, big data and beyond. It is where over 60,000 of the tech industry's innovators and influencers gather to explore how Intelligent Connectivity will shape the future of our digital experiences, our industry and our world.
#MWC19
DIAMOND EVENT PARTNER
中国移动 China Mobile
GLOBAL MEDIA PARTNER
MOBILE WORLD LIVE
GLOBAL PARTNER
MOBILE WORLD CAPITAL BARCELONA


Фото: Kite rocket

Нестандартный стандарт

Технология Интернета вещей (IoT) LoRaWAN с большой скоростью распространяется во всем мире. Несмотря на то, что она не входит в стек технологий 3GPP, ее применяют многие сотовые операторы, в том числе Orange, Bouygues Telecom, Swisscom, KPN, Proximus, Andorra Telecom, SK Telekom, NTT, Telkom Indonesia, Spark New Zealand. В интервью главному редактору «Стандарта» Леониду КОНИКУ генеральный директор и председатель совета директоров LoRa Alliance Донна МУР рассказала о технологических новшествах, о развитии экосистемы LoRaWAN и о том, почему она называет эту технологию стандартом де-факто.

– Какова степень распространения технологии LoRaWAN в мире?

– В LoRa Alliance уже входит свыше 500 компаний. По всему земному шару работает более ста операторов сетей LoRaWAN, причем их количество за последний год выросло на 60%. По нашим оценкам, в общей сложности в мире к сетям LoRaWAN уже подключено 70-80 млн устройств. Некоторые из них одновременно с LoRA используют IoT-сети в лицензируемых диапазонах частот (в частности, основанные на технологии NB-IoT). В зависимости от необходимых приложений применяются и будут применяться различные сетевые технологии Интернета вещей. Но большинство участников LoRa Alliance прекратили дискуссию о технологиях – теперь они говорят о решениях, масштабируемости и возврате инвестиций заказчика. По нашей оценке, из всех приложений IoT около 75% приходится на сети с низким энергопотреблением и большим охватом (LPWAN), и только 25% требуют высокой пропускной способности и малой задержки сигнала.

Мы утверждаем, что LoRaWAN стал де-факто стандартом для сетей LPWAN. Мы не просто говорим про Интернет вещей для «умных» городов, сельского хозяйства или коммунальных услуг: члены альянса внедряют IoT-решения в этих и других секторах – по всему миру и масштабно. При этом мы не противопоставляем LoRaWAN технологии 5G. У сетей пятого поколения будет высокая пропускная способность и малые задержки в передаче данных, что необходимо для таких областей применения как big data, индустрия развлечений (передача видео), подключенный/автономный автомобиль, услуги в сфере безопасности, требующие мгновенного отклика сети. А LoRaWAN обладает гибкостью, которая нужна для очень многих приложений – публичных или частных. Сети LoRa могут создаваться по различным бизнес-моделям – как на основе инвестиций в создание собственной физической сети на том или ином объекте, так и по сервисной модели.

Наряду с такими сферами как «умный» город, ЖКХ, мониторинг объектов, управление зданиями и других вертикалей, технология LoRaWAN нашла широкое применение в больницах. Прежде всего по причине того, что клиники не хотят передавать конфиденциальную информацию по общественным сетям. Но кроме этого LoRa позволяет больницам контролировать температуру в холодильниках, перемещение лекарственных средств, состояние медицинской техники и пациентов.

– Что нового появилось в технологии LoRaWAN за последнее время?

– Технология LoRaWAN развивается. Например, в октябре 2018 года выпущена новая спецификация, которая поддерживает онлайн-обновление прошивки всех конечных устройств «по воздуху» (Firmware Updates Over the Air, FUOTA). Эта функция означает кардинальные перемены на рынке: когда у вас в сети миллионы устройств, а срок их жизни превышает десять лет, обновление их прошивки становится масштабной задачей (а такие обновления нужны регулярно, в том числе в связи с кибербезопасностью). За счет использования еще одной новинки в LoRaWAN – режима multicast – одно и то же сообщение (например, новая прошивка) может быть отправлено сразу целой группе конечных устройств. Так что между тем, что делаем мы, и тем, что возможно в NB-IoT и 5G, есть немало отличий.

Очень важная характеристика сетей LoRaWAN – большой охват, что особенно актуально для «умного» города, где плотность устройств очень высока. А к одному большому промышленному шлюзу (к базовой станции) LoRa можно подключить до 10 млн конечных устройств.

В сетях LoRaWAN есть и геолокация, причем она не сокращает заряд аккумулятора в устройстве, поскольку использует триангуляцию через базовые станции (БС). Кибербезопасность – важнейшая функция наших дней – в сетях LoRaWAN организована по принципу end-to-end.

– Вы сказали, что зона охвата базовых станций LoRa очень велика. Тогда каким образом с их помощью удается точно определять координаты?

– Для этого рассчитывается шаг по параметру времени: чем дольше идет сигнал, тем дальше объект. В стандартном режиме используется трехшаговый алгоритм, но если нужно определить координаты еще точнее, то можно установить на заданной территории еще одну БС. Однако даже одна базовая станция LoRa обеспечивает точность от 20 до 200 метров, при этом затраты на определение координат в сети LoRaWAN ниже, чем при использовании любых других технологий – GPS, Assisted-GPS (AGPS), Bluetooth Low Energy (с применением indoor-маячков) и даже Wi-Fi.

– Возможен ли автоматический роуминг в сетях LoRaWAN? Считаете ли вы роуминг важной функцией?

– Да, однозначно. Разработка спецификации, описывающей роуминг в LoRaWAN, завершена. Сейчас операторы заключают друг с другом роуминговые соглашения, но LoRa Alliance в этом не участвует. Например, к концу января 2019 года мобильные компании Swisscom, KPN, Proximus и Objenious (IoT-подразделение французского сотового оператора Bouygues Telecom, – *прим. «Стандарта»*) заключили соглашения о взаимном роуминге между своими странами (соответственно, между Швейцарией, Нидерландами, Бельгией и Францией, – *прим. «Стандарта»*).

У LoRa Alliance есть масштабная программа сертификации оборудования, и как раз недавно мы ее расширили, для того чтобы гарантировать его интероперабельность (и операторам теперь нет необходимости тестировать оборудование). Мы также начали сертифицировать оборудование на срок службы аккумуляторов и проводить радиочастотные тесты. Я лично никому не советую покупать LoRa-оборудование без надписи LoRaWAN Certified.

– На рынке присутствуют и другие IoT-технологии – например, SigFox, Ingenu RPMA, «Стриж». Ощущаете ли вы конкуренцию с их стороны?

– Да, мы их видим. Но, например, технология SigFox – это проприетарное решение, и невозможно себе представить, чтобы оно превратилось в глобальный стандарт IoT. В случае с LoRaWAN имеется множество компаний, которые производят подходящие конечные устройства, шлюзы и иное сетевое оборудование. Это обеспечивает развитие, конкуренцию и доступность цен.

– Вы официально говорите, что LoRaWAN де-факто является стандартом. Но ни один орган стандартизации пока этого не сказал. Что дает вам основания для такого заявления? Планирует ли LoRa Alliance провести реальную стандартизацию технологии?

– Статус стандарта за LoRaWAN признают многие аналитики – на том основании, что количество активных устройств в этих сетях давно перевалило за 50 млн, и второй технологии с аналогичным охватом нет и близко. Мы вели дискуссии о начале полноценной стандартизации LoRaWAN на уровне совета директоров, но так и не смогли ответить на вопрос о том, что это нам даст. Наша технология бурно развивается, и в обозримом будущем мы, скорее всего, не станем обращаться в органы стандартизации. Я сама пришла из сферы стандартизации и знаю, что это такое. Но IoT – это новый мир, и ни один из 500 членов LoRa Alliance не спросил нас о формальной стандартизации.

Швейцарская финансовая компания Momenta Partners настолько поверила в технологию LoRaWAN, что в феврале 2019 года создала отдельный венчурный фонд объемом до $50 млн для инвестирования в связанные с технологией проекты. И первые получатели средств из этого фонда уже есть. Это еще один аргумент в пользу того, что LoRaWAN воспринимается на рынке фактически как стандарт.

Без eSIM и без частот

Фото: СТАНДАРТ

В Южной Корее и двух городах США – в Чикаго и Миннеаполисе – в апреле заработали сотовые сети 5G. Потихоньку их начинают разворачивать и в Европе. Параллельно в Америке и Новом Свете набирает популярность другая сотовая технология – eSIM. Суть ее в том, что для подключения к сотовой сети не нужно посещать офис продаж оператора и покупать SIM-карту: с eSIM для перехода к новому оператору достаточно просканировать специальный QR-код.

В России до последнего времени операторы с чиновниками спорили о том, строить ли 5G по отдельности, делиться ли друг с другом оборудованием, или «пересесть» на единого оператора. Но недавно выяснилось: сколько этих операторов будет – вообще неважно, потому что Минобороны РФ не хочет отдавать операторам частоты базового для 5G диапазона 3,4-3,8 ГГц. А без них полноценное покрытие сетями нового стандарта крупных городов России невозможно организовать вообще – что одному оператору, что нескольким.

Параллельно возникли проблемы и с внедрением 5G: против применения технологии выступает Федеральная служба безопасности и сами операторы. Чекисты якобы переживают из-за применения на SIM-картах отечественных алгоритмов шифрования: понятно, что записать специальное ПО на каждый смартфон, произведенный где-нибудь в китайской глубинке, будет весьма затруднительно. Операторы же опасаются, что с eSIM абонентам станет легче, чем сейчас, уходить от одного оператора к другому. Безусловно, значительно проще удерживать клиентов, препятствуя развитию новой технологии, чем предлагая им что-то привлекательнее низких тарифов.

В контексте ситуации с 5G невольно вспоминаешь историю внедрения сотовой связи третьего поколения в Москве. В 2009 году получить частоты у военных операторы смогли (и довольно быстро) только после вмешательства верховного главнокомандующего – тогдашнего президента Дмитрия Медведева. Владимир Путин тоже, говорят, поручил Минобороны «проработать вопрос» о выделении для 5G частот 3,4-3,8 ГГц. Но «проработать вопрос» – это все-таки не то, что фактически приказать силовикам поделиться частотами, как это было десять лет назад.

Происходящее выглядит пугающе. До сих пор Россия не была в авангарде телекоммуникационных инноваций, но не была и отстающей державой. В итоге за два десятилетия страна стала обеспеченной дешевой, качественной и современной связью. А теперь – вполне реальна перспектива застрять на месте и отстать от мировых лидеров в этой сфере. Остаться на долгие годы с 4G – попросту опасно. Это настоящая угроза для экономической безопасности России, ведь без сетей пятого поколения невозможно внедрение новых технологий, а также цифровизация промышленности, ЖКХ и много чего другого. И запрет eSIM тут не менее критичен, чем дефицит частот для 5G: ведь, как планируется, сотни миллионов датчиков и автоматических устройств в «умных» городах и на «умных» предприятиях должны работать без привычных встраиваемых SIM-карт. Добровольный отказ от прогресса – едва ли не худшее, что сейчас может произойти с Россией.

Валерий Кодачигов,
заместитель редактора отдела «Технологии и телекоммуникации» газеты «Ведомости», специально для «Стандарта»

Безопасность данных в сетях LoRaWAN


Фото: «ЭР-Телеком Холдинг»

Андрей ЭКОНОМОВ,
руководитель технического сопровождения IoT АО «ЭР-Телеком Холдинг»,
участник технического комитета LoRa Alliance, к.ф.-м.н.

LoRaWAN является наиболее распространенной технологией Интернета вещей из группы LPWAN (Low Power Wide Area Network). Конференции, посвященные LoRaWAN, собирают тысячи участников со всего света, в LoRa Alliance входят более пятисот компаний, а сети на базе этой технологии работают на всех обитаемых континентах. При этом информационная защищенность системы, построенной на протоколе LoRaWAN, находится на высших уровнях, характерных для сетей связи общего пользования. Применяя известные меры защиты информации, на базе этой технологии можно построить систему мониторинга и управления, в том числе критическими объектами.

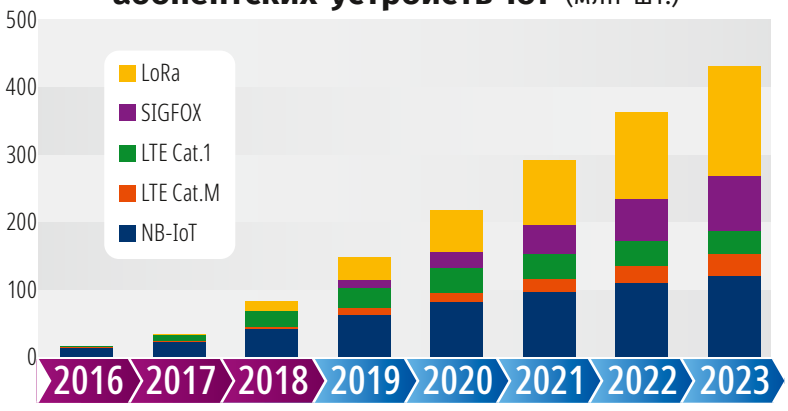
Сегодня именно LoRaWAN является драйвером развития направления IoT (Internet of Things) во всем мире и используется в качестве основного инструмента для управления критически важной инфраструктурой, транспортом, производством, здравоохранением, муниципальным и сельским хозяйством. И это далеко не пилотные проекты – например, уже 45 тыс. абонентских устройств LoRaWAN обслуживают систему «умный» город в Шанхае.

Особенно стоит отметить тот факт, что LoRaWAN является наиболее гибким с технологической точки зрения стандартом: он позволяет одновременно применять датчики разных классов, организовать международный автоматический роуминг и возможность дистанционного обновления ПО абонентских терминалов через радиоэфир (технология Firmware Upgrade Over The Air, FUOTA), использовать беспроводной репитер с питанием от батареи, организовать вещание Multicast (одновременный прием сообщения несколькими датчиками), мультилатерационную геолокацию и другие опции. Поэтому сеть LoRaWAN можно адаптировать для решения практически любой задачи, определенной заказчиком.

Как было показано на LoRaWAN Members Meeting 2018 в Токио, даже с началом коммерческой эксплуатации сетей NB-IoT (Narrow Band IoT – стандарт LPWAN, построенный на инфраструктуре существующих сетей GSM и LTE), сети LoRaWAN сохранят за собой заметную долю рынка: по разным прогнозам, не менее 25-50% (см. «Статистика и прогноз поставок абонентских устройств IoT в 2016-2023 годах»). Это связано с тем, что, несмотря на сходство, технологии NB-IoT и LoRaWAN имеют разные параметры, а области их применения пересекаются неполностью: все развитые страны ориентируются на сочетание стандартов Интернета вещей, работающих в лицензионных и безлицензионных полосах частот. Преимущество нелицензионных полос – дешевизна и быстрота развертывания. Целевая область применения сетей LoRaWAN в системах IoT – это автономные устройства без внешнего электропитания; датчики, генерирующие малые потоки данных; терминалы, сравнительно редко выходящие в эфир, а также объекты, покрытие которых необходимо развернуть быстро и с минимальными затратами.

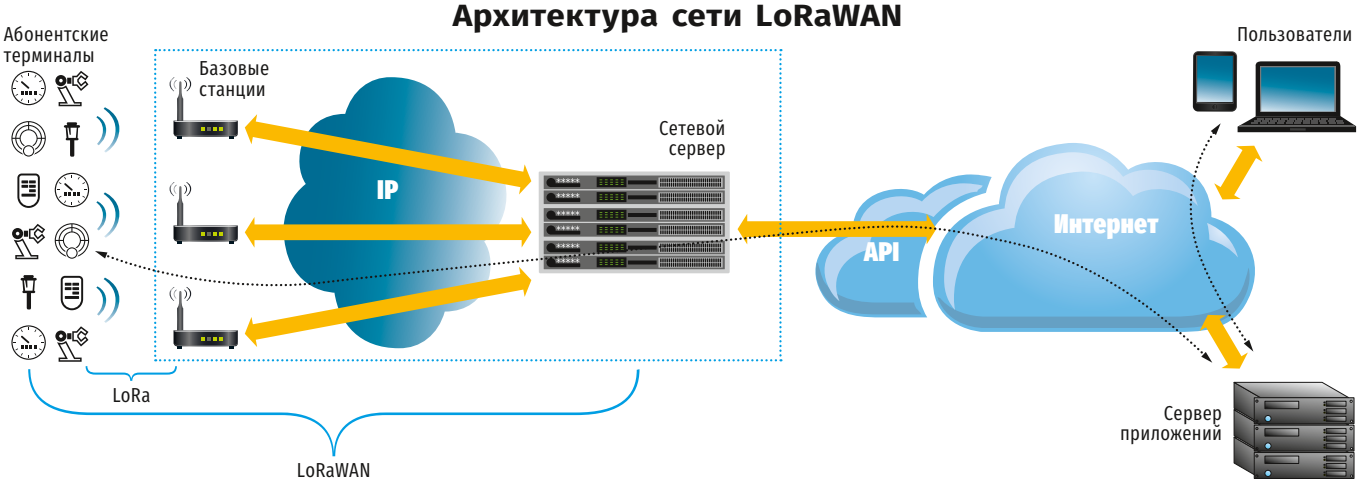
Сейчас в LoRa Alliance входят три оператора из России – АО «ЭР-Телеком Холдинг», ОАО «МТТ» и ООО «Лартех Телеком». Ассоциация участников рынка Интернета вещей (АИВ) РФ разрабатывает национальный стандарт протокола LoRaWAN, а LoRa Alliance в 2018 году стандартизировал национальный профиль для РФ (LoRaWAN 1.0.3 Regional

Статистика и прогноз поставок абонентских устройств IoT (млн шт.)



Источник: LoRa Alliance

Архитектура сети LoRaWAN



Источник: «ЭР-Телеком Холдинг»

Parameters). Производство абонентских устройств и базовых станций LoRaWAN уже освоили российские производители «Вега-Абсолют», «Гудвин», «Новоучет» и другие, а компания «Лартех» разработала ПО для сетевого сервера.

Архитектура сети LoRaWAN

Сеть LoRaWAN состоит из следующих элементов: абонентские терминалы, базовые станции (шлюзы), сетевой сервер и серверы приложений.

Абонентский терминал – обобщенное название для сенсоров, датчиков, счетчиков, актуаторов и радиомодулей IoT, устанавливаемых на стороне пользователя. Стандарт LoRaWAN определяет три класса терминалов (см. «Классы терминалов LoRaWAN»).

Базовая станция (БС) – типовое понятие для многих радиосистем, в том числе для радиосетей IoT. Применительно к сети LoRaWAN (так же как и во многих других радиосетях) БС выполняет функции сопряжения и взаимодействия радиосети с абонентским терминалом и концентрации нагрузки от группы терминалов, поэтому в документации LoRa Alliance БС именуется шлюзом и/или концентратором. Сигнал от одного терминала может приниматься несколькими базовыми станциями. Совокупность базовых станций оператора обеспечивает территорию радиопокрытия сети и прозрачную двунаправленную передачу данных между конечными устройствами и сетевым сервером. Базовая станция оснащена приемопередающей антенной (секторной или всенаправленной), а также, опционально, GPS/ГЛОНАСС-антенной для прецизионной синхронизации внутренних часов и определения точных координат антенны.

Сетевой сервер – программно-аппаратный комплекс, управляющий радиосетью, контролирующий радиосеть и выполняющий маршрутизацию пакетов данных от абонентских терминалов до соответствующих серверов приложений.

Классы терминалов LoRaWAN

A
Сеанс связи инициирует терминал. Основная задача – передавать данные от устройства к сети, прием данных возможен только сразу после передачи (терминал открывает два «окна» приема).
Терминалы класса A применяются в приложениях, где передача данных от сети возможна только как ответная реакция на получение данных от конечного устройства и требуется максимальное время работы от автономного источника питания.

B
В дополнение к возможностям класса A появляется возможность по расписанию принимать данные от сети, то есть сеанс связи может быть инициирован как устройством, так и сетью.
Терминалы класса B используются в тех случаях, когда прием данных от сети требуется, но не моментально, а по назначенному заранее расписанию (например, один раз в 32 секунды) – так соблюдается баланс между скоростью реакции устройства на внешнюю команду и его энергопотреблением.

C
Устройства класса C постоянно готовы принимать данные от сети, прием данных прекращается только во время передачи данных самим устройством. Таким образом, сеанс связи, как и для устройства класса B, может быть инициирован как устройством, так и сетью.
Терминалы класса C применяются в приложениях, где быстрота реакции на команду, полученную от сети, важнее экономии электропитания, а также в тех кейсах, где устройству необходимо получать через IoT-сеть большие объемы данных.

Источник: LoRaWAN Specification, Version V1.0.3, 2018

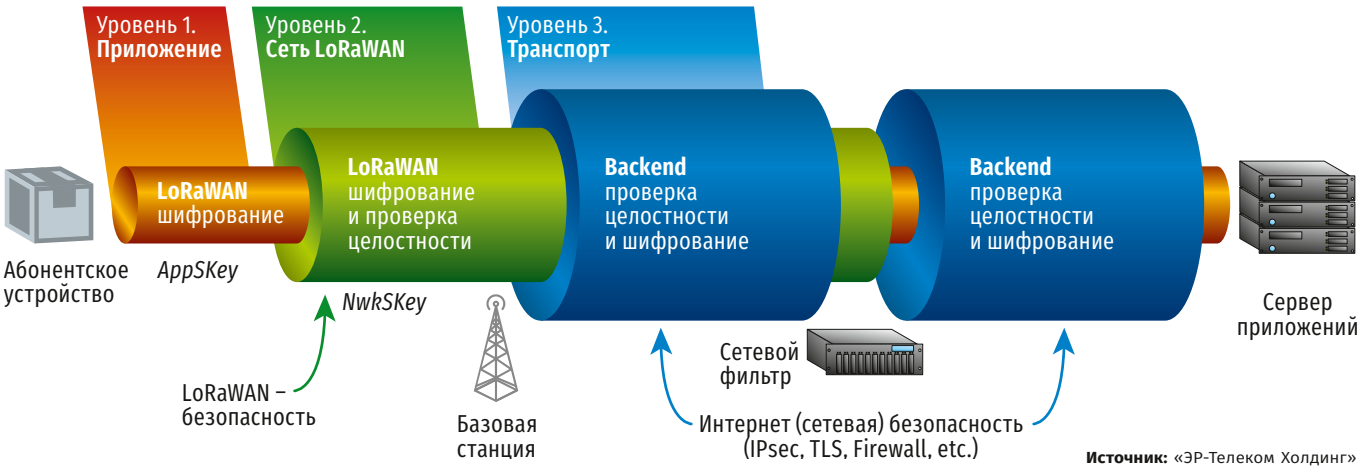
Обеспечение безопасности данных

В сети IoT LoRaWAN используется многоуровневая система безопасности передачи данных (см. «Общая схема безопасности данных в сети LoRaWAN»).

Первый уровень имеет AES-шифрование на уровне приложения (между абонентским терминалом и сервером приложений) с помощью 128-битного переменного сессионного ключа Application Session Key (AppSKey). Этот ключ шифрования хранится в абонентском терминале и на сервере приложений и недоступен оператору сети (доступ к AppSKey есть только у клиента – владельца сервера приложений). Формирование сессионного ключа AppSKey происходит параллельно в абонентском терминале и на стороне сети во время процедуры активации терминала, а через эфир AppSKey не передается.

Второй уровень предполагает AES-шифрование и проверку целостности сообщений на сетевом уровне (между абонентским терминалом и сетевым сервером) с помощью 128-битного переменного сессионного ключа Network Session Key (NwkSKey). Данный ключ шифрования также хранится в абонентском терминале и на сетевом сервере и недоступен клиенту (доступ к NwkSKey есть только у оператора сети – владельца сетевого сервера). Формирование сессионного ключа NwkSKey также происходит параллельно в абонентском терминале и на стороне сети во время процедуры активации терминала, а через эфир NwkSKey не передается.

Общая схема безопасности данных в сети LoRaWAN



Источник: «ЭР-Телеком Холдинг»

Третий уровень включает стандартные методы аутентификации и шифрования интернет-протокола (IPsec, TLS и т. п.) при передаче данных по транспортной сети между узлами сети (базовая станция, сетевой сервер, join-сервер, сервер приложений).

По команде приложения или сетевого сервера в любой момент возможен переход на новую сессию с генерацией нового комплекта ключей шифрования, что делает бесполезными старые ключи шифрования. Также есть возможность установить периодическую генерацию нового комплекта ключей NwkSKey и AppSKey.

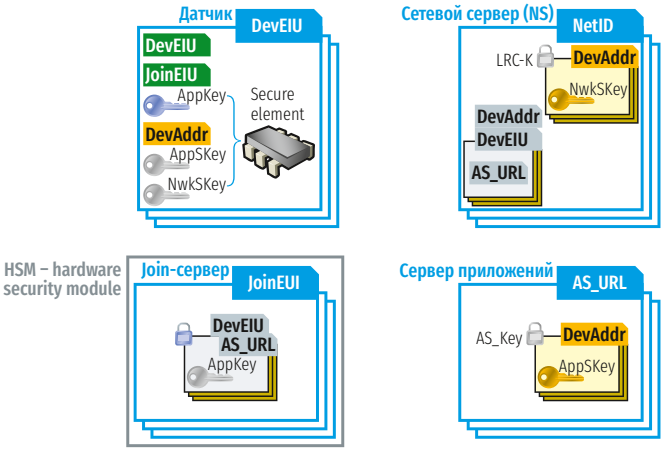
В версии стандарта LoRaWAN V1.0.x формирование сессионных ключей на стороне сети производится на сетевом сервере (Name Server, NS), однако в версии V1.1 для этих целей используется выделенный сервер – так называемый join-сервер (например, микроконтроллером Microchip ATECC608A), что исключит их компрометацию в случае физического воздействия на терминал.

Внедрение аппаратных средств защиты в сети и на терминале делает бесполезными попытки перехвата сессионных ключей при передаче их между серверами и попытки взлома сетевых серверов или абонентских устройств с целью извлечения сессионных ключей.

Рассмотренные меры также создают условия для защищенного роуминга данных – безопасную авторизацию датчиков в гостевой сети и защищенную передачу данных домашнему серверу приложений из гостевой сети.

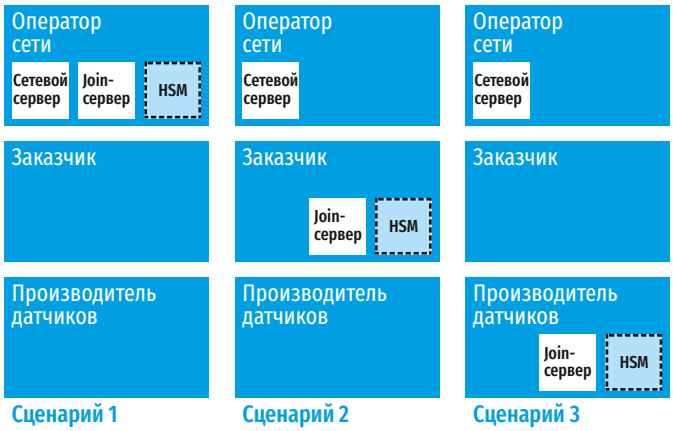
В целях дополнительной защиты процесса генерации сессионных ключей join-сервер может быть физически вынесен на территорию клиента или производителя устройств

Схема хранения ключей шифрования



Источник: «ЭР-Телеком Холдинг»

Возможные сценарии размещения join-сервера



Источник: «ЭР-Телеком Холдинг»

(см. «Схема хранения ключей шифрования»). Join-сервер может быть дополнительно защищен отдельным аппаратным модулем безопасности HSM (Hardware Security Module).

В этом случае для безопасной передачи сгенерированных сессионных ключей между серверами, а также для хранения их на сетевом сервере и сервере приложений внедряются дополнительные ключи: AS_Key для ключа AppSKey и LRC_K для ключа NwkSKey. На абонентском устройстве ключи шифрования опционально могут защищаться специальным аппаратным элементом безопасности Secure Element (см. «Возможные сценарии размещения join-сервера»). В этом случае даже сотрудники оператора не смогут получить доступ к сессионным и корневым ключам шифрования.

Несмотря на то, что в РФ не требуется обязательная сертификация средств кодирования (шифрования) при передаче сообщений, не составляющих государственную тайну[1], по требованию заказчика используемые в стандарте

[1] Извещение по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет, ФСБ РФ, 18.07.2016

LoRaWAN уровни шифрования AES-128 могут быть дополнены одним из стандартизованных в РФ алгоритмов, входящих в семейство ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 или по алгоритму «Кузнечик» (согласно ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015).

Для этого предлагается при производстве абонентских терминалов LoRaWAN устанавливать в устройства дополнительный микроконтроллер СКЗИ (средство криптографической защиты информации), сертифицированный ФСБ России и соответствующий требованиям, предъявляемым к шифровальным средствам класса КС3 (дистанционное банковское обслуживание, электронный документооборот в государственном секторе и т. д.). В качестве такого микроконтроллера могут быть использованы микропроцессоры отечественного производства «Микрон» MIK51SC72D или MIK51AD144D, сертифицированные ФСТЭК и ФСБ России, имеющие небольшие размеры (около 14 мм²) и малое энергопотребление.

Ниже представлена схема безопасности данных в сети LoRaWAN с дополнительным уровнем СКЗИ.

Ключ шифрования уровня СКЗИ – например, SubSKey (согласно ГОСТ Р 34.12-2015) – прошивается в абонентский терминал LoRaWAN при производстве, так же как и корневой ключ первого и второго уровней шифрования LoRaWAN, или внедряется в терминал вместе с микроконтроллером СКЗИ при введении терминала в эксплуатацию (используя специальный слот). Дешифрация данных уровня СКЗИ производится на территории заказчика сервером приложений после дешифрации уровня приложения сессионным ключом AppSKey. Ключ шифрования SubSKey передает клиенту вместе с датчиком непосредственно производитель абонентского терминала, и этот ключ недоступен сотрудникам оператора сети LoRaWAN.

Кастомизация системы безопасности данных

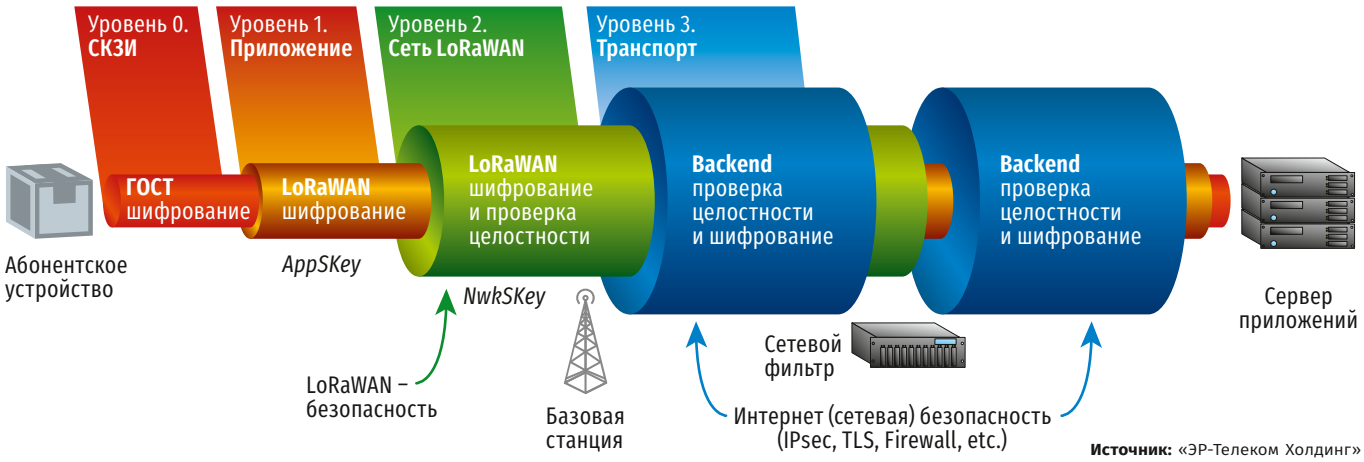
Система безопасности данных может быть кастомизирована на сетевом уровне LoRaWAN. В зависимости от требований и объема финансирования со стороны заказчика могут быть применены такие меры как: настройка для каждого абонентского терминала периодической регенерации нового комплекта сессионных ключей шифрования с помощью MAC-команды RejoinParamSetupReq; использование специального микроконтроллера для безопасного хранения корневых и сессионных ключей шифрования на стороне абонентского терминала; выделение особого join-сервера для аутентификации абонентских терминалов и хранения корневых и сессионных ключей шифрования на стороне сети; использование аппаратного модуля безопасности HSM для дополнительной защиты join-сервера; физическое вынесение связки «join-сервер и HSM» на территорию заказчика; внедрение дополнительного уровня шифрования по сертифицированным ФСБ алгоритмам СКЗИ с использованием специального микропроцессора; для передачи данных с критически важной инфраструктуры могут использоваться датчики, базовые станции и ПО сетевого сервера, разработанные и произведенные на территории РФ.

На первый взгляд может показаться, что использование в сетях LoRaWAN запатентованных чипов Semtech создает потенциальную системную уязвимость. Однако это не так. Во-первых, патент распространяется только на радиоинтерфейс LoRa (физический уровень между базовой станцией и абонентским терминалом), все остальные части сети LoRaWAN открыты, спецификации протоколов сетевого и канального уровня доступны, проверены на наличие недокументированных возможностей и используются глобальной экосистемой, в том числе российскими производителями оборудования и ПО. Так что даже если проприетарный чип Semtech и содержит так называемую «закладку», злоумышленник не сможет ею воспользоваться, так как физически нет прямого доступа извне непосредственно к чипу. Во-вторых, запатентованные чипы LoRa по лицензии Semtech производятся массово целым рядом компаний и широко представлены на мировом рынке. Их изготовление освоил, например, Microchip. Российские производители микропроцессоров тоже могут быть в числе производителей чипов LoRa.

Все остальные вопросы безопасности системы относятся к компетенции производителей оконечных устройств, сетевого оборудования, приложений, а система LoRaWAN, как упоминалось выше, может быть полностью построена на решениях и компонентах отечественного производства. Это подтверждают приведенные выше схемы обеспечения безопасности: они базируются отнюдь не на физическом уровне, где присутствует проприетарный протокол, права на который принадлежат Semtech.

Кроме того, в системах Интернета вещей, как правило, вообще не осуществляется передача персональных данных и иной чувствительной информации, кроме собственно сигналов о состоянии датчиков и иных абонентских устройств. Связывание сигнала с физическим объектом осуществляется по идентификатору датчика в программном приложении пользователя системы, и при необходимости на этом уровне могут быть приняты меры по защите чувствительной пользовательской информации.

Схема внедрения отечественных СКЗИ в структуру шифрования данных сетей LoRaWAN



Источник: «ЭР-Телеком Холдинг»

Автопром стремится в 5G

Многие телеком-вендоры и операторы связи сходятся во мнении, что подключенные (а в перспективе и беспилотные) автомобили станут значимыми потребителями услуг сотовых сетей пятого поколения (5G). Косвенно этот прогноз подтверждает тот факт, что именно автопром стал первой в мире отраслью, которая пошла на создание общей глобальной ассоциации с разработчиками телекоммуникационных решений. Такая ассоциация – 5G Automotive Association (5GAA) – была организована в сентябре 2016 года. В интервью главному редактору ИГ ComNews Леониду КОНИКУ технический директор 5GAA Максим ФЛАМЕНТ оценил зрелость различных ИКТ-технологий для автомобильной индустрии и заявил, что ассоциация заинтересована в сотрудничестве с Россией.

Фото: 5GAA

– Расскажите об истории ассоциации 5GAA – российской аудитории она малоизвестна.

– Наша ассоциация молодая – ей всего два года. Мы начинали с восьми членов, объединив представителей автомобильной и телекоммуникационной отраслей, – Audi AG, BMW Group, Daimler AG, Ericsson, Huawei, Intel, Nokia и Qualcomm Inc. Сейчас у нас 110 участников, и 5GAA – действительно глобальная ассоциация, хотя бы потому, что большинство ее членов работают по всему миру. В телекоммуникациях наиболее популярны глобальные стандарты, и мы хотим распространить эту практику на коммуникации в автомобильном секторе. Мы не являемся органом стандартизации, но 5GAA сотрудничает с такими организациями – прежде всего с 3GPP.

Несколько лет назад, начиная со стандарта LTE Release 14, мы стандартизовали технологию радиодоступа для коммуникаций между транспортными средствами (V2V), а также между автомобилями и инфраструктурой (V2I), между автомобилями и сетью (V2N). Интегрально эта технология называется C-V2X (Cellular Vehicle to Everything). Мы выступили с предложением использовать эту технологию для подключенных автомобилей во всем мире. Мы работаем с игроками на рынке США, Европы, Китая, Кореи и Японии. Конечно, мы не забываем и о других регионах и странах, в том числе о России. Что касается России – у нас крайне ограниченные возможности рассмотреть, что там происходит с точки зрения рынка. Но нам было бы интересно открыть российский рынок для себя и для технологии C-V2X. Наша ассоциация активно участвует в демонстрационных проектах и пилотных зонах. Часто в такие проекты вовлечены и местные власти.

> **«Нам было бы интересно открыть российский рынок для себя и для технологии C-V2X»**

– Когда технология C-V2X может стать массовой?

– Если говорить о зрелости технологии, LTE Release 14 появилась в 2017 году, с тех пор такие компании как Qualcomm и Huawei представили соответствующие чипы и радиоустройства. К концу 2019 года рынок C-V2X уже будет видимым, пока в основном за счет Китая. Поначалу это будет связь типа V2N, но и вариант V2V постепенно начнет набирать обороты. Для последнего варианта используется специальный нелицензируемый частотный диапазон ITS (Intelligent Transportation Systems) – 5,9 ГГц, предназначенный именно для интеллектуальных сетей на транспорте. В этом диапазоне работают различные технологии, прежде всего 802.11p, которая обеспечивает беспроводную передачу информации между высокоскоростными транспортными средствами и объектами транспортной инфраструктуры по каналу Wi-Fi. Пока она больше ассоциируется с распространенным в автопроме стандартом DSRC (Dedicated Short-Range Communications), но LTE Release 14 также позволяет ее задействовать.

– В автопроме также широко распространена технология ADAS (Advanced Driver-Assistance Systems), на которой базируются различные системы помощи водителю. Видите ли вы возможности для совместной работы ADAS и C-V2X?

– ADAS – это важная часть технологий в автопроме, особенно с учетом того, что за последнее десятилетие качество сенсоров и их доступность резко улучшились. Мы видим, что V2V и V2I применяет сенсоры, которые могут быть использованы как дополнительный информационный ресурс, потребляющий крайне незначительную компьютерную мощность (ведь определение манеры поведения соседнего автомобиля на основе полученных от него данных – не самая сложная задача). И если один автомобиль «понимает», что соседнее транспортное средство оснащено системой C-V2X, он может сократить использование ресурсов компьютера. Проблема в том, чтобы загрузить данные, полученные по радиоканалу, в платформу управления автомобильными сенсорами: нужно рассчитывать риск некорректности этих данных, ведь это связано с функциональной безопасностью машины.

ADAS является важной технологией еще и потому, что открывает путь для беспилотных автомобилей.

Текущая версия C-V2X, основанная на LTE Release 14, обеспечивает базовую безопасность за счет передачи информации. Сейчас ведется работа над C-V2X для LTE Release 16, которая будет гарантировать качество услуги за счет малой задержки и высокой скорости передачи данных. Как только такая технология станет доступна, появится возможность делиться данными со всех сенсоров и автоматически согласовывать маневры нескольких машин.

– Изначально подход к созданию автономных автомобилей подразумевал, что каждая отдельная машина будет управляться через облако. Затем возникла идея внесетевой коммуникации между соседними автомобилями на основе бортовых компьютеров. Какую перспективу развития видит 5GAA?

– Если речь идет о высоких уровнях автономности, мы считаем, что соединение с сетью необходимо. Если мы говорим об облачных сервисах, о соединении с облаком, то есть технология граничных вычислений (Edge Computing), которая может это обеспечить. В некоторых ситуациях лучше использовать связь на границе сети, чтобы гарантировать низкую задержку сигнала. Я бы объединял технологии V2V и V2N, так как не все сообщения нужно передавать в сеть: многие данные имеют сугубо локальное значение (скажем, расположение или скорость соседней машины), зато передаются буквально за 100 миллисекунд.

– Сотрудничает ли 5GAA с производителями «умных» дорожных знаков, светофоров и иных элементов интеллектуальных транспортных сетей?

– Многие члены ассоциации поставляют интеллектуальные дорожные знаки, но немногие из них делают интеллектуальные транспортные системы. Последними занимаются такие фирмы как Siemens или Kapsch, но они не входят в 5GAA. В целом такие компании предлагают использовать радиотехнологии на основе Wi-Fi. Мы с ними работаем. Например, в американском штате Колорадо у 5GAA есть проект с местным департаментом транспорта. В проекте принимает участие и компания Kapsch, поставляющая все дорожные знаки, а Panasonic (который также не входит в нашу ассоциацию) предоставил систему управления транспортом.

5GAA представляет телекоммуникационную и автомобильную отрасли. Дорожная инфраструктура является важной частью «умного» транспорта, и мы хотим сотрудничать с этой индустрией. В этом направлении мы используем такую стратегию: начинаем сотрудничать с операторами автодорог, а они в свою очередь приглашают поставщиков «умных» дорожных знаков и иного дорожного оснащения. Именно так произошло в Колорадо, где департамент транспорта привлек Kapsch и Panasonic, и наша совместная работа идет отлично.

– Различные автопроизводители используют разное количество SIM-карт на борту. Например, Jaguar и Land Rover устанавливают в каждый автомобиль две SIM-карты, а Fiat использует одну. Пытается ли 5GAA унифицировать количество SIM-карт в машинах и сколько их должно быть для полной функциональности технологии C-V2X?

– Я не уверен, что могу говорить о стратегиях разных производителей автомобилей. Если вы посмотрите анонс Qualcomm на Mobile World Congress 2019 в Барселоне, они представили новый чип Snapdragon для автомобильной платформы 5G, включающий технологию C-V2X. Этот процессор не просто поддерживает две SIM-карты, а оснащен технологией DSDA (Dual SIM Dual Active), то есть обе они постоянно активны. Одну SIM-карту может поставлять производитель автомобиля, а вторая – частная.

20 динамичных лет «Итеранет»

Фото: СТАНДАРТ

23 мая 2019 года ИКТ-компания «Итеранет» отмечает 20 лет со дня основания. Начав как телеком-подразделение международной группы компаний (МГК) «ИТЕРА», в течение последних пяти лет она развивается как независимый участник рынка и занимается большими комплексными проектами в разных отраслях экономики – как в государственном секторе, так и в коммерческом. В интервью главному редактору ИГ ComNews Леониду КОНИКУ генеральный директор ООО «Итеранет Холдинг» Игорь МАЦКЕВИЧ рассказал о том, с чем компания пришла к 20-летию и как трансформируется ее тактика на быстроменяющемся ИТ-рынке России.

– Компания «Итеранет» создавалась на базе ИТ-подразделения МГК «ИТЕРА» и полтора десятка лет была основным оператором для этого холдинга. Однако в 2013 году «Итеранет» вышла из периметра группы «ИТЕРА», а основным собственником компании стал созданный в том же году «Итеранет Холдинг». С чем были связаны эти перемены?

– В 2012 году основной актив группы «ИТЕРА» – одноименная нефтегазовая компания – был куплен «Роснефтью». У «Роснефти» есть свое подразделение, обслуживающее ИТ-системы (тогда – «РН-Информ», ныне – «Сибинтек», – *прим. «Стандарта»*), поэтому мы постепенно отошли в сторону. В 2013 году мы создали структуру «Итеранет Холдинг», в которую вошли «Итеранет», «СофтЭра» (учреждена в 2011 году) и «Моблнет» (зарегистрирована в 2014 году). Каждая компания организовывалась под профильный вид деятельности: информационная безопасность (ИБ), программное обеспечение и информационные системы, телеком.

Пока «Итеранет» входил в группу «ИТЕРА», мы решали широкий спектр задач и выполняли много функций, связанных с информационно-коммуникационным обеспечением деятельности группы: мы были оператором связи, разрабатывали и внедряли информационные системы, занимались ИБ, вели инфраструктурные проекты. На пике развития в группу «ИТЕРА» входило более 150 компаний, разбросанных по России и по миру, и мы обеспечивали весь этот комплекс заказчиков. Это позволило нам накопить большой опыт и наработать уникальные компетенции. К примеру, мы первыми в РФ установили пакет приложений Oracle E-Business Suite.

– Что принципиально изменилось для компании с того момента, когда «Итеранет» стала независимым участником ИКТ-рынка?

– Мы занимались коммерческими проектами на открытом рынке уже в те времена, когда «Итеранет» входила в периметр группы «ИТЕРА», – примерно с 2008 года. И к моменту выхода из материнской группы в 2012 году ее доля заказов составляла всего 1/3 оборота «Итеранета». Принципиально изменилось наше состояние: одно дело – быть в составе большой группы, которая может помочь с финансированием, получением кредитов, с заказами, и совсем другое дело – находиться на открытом рынке, где все эти вопросы нужно решать самостоятельно. Нам пришлось научиться быстро реагировать на внешние факторы, связанные,

например, с динамикой рынка и потребностями клиентов. Выстраивание соответствующих процессов внутри компании оказалось непростой задачей.

– Удалось ли вам заместить выпавшие доходы от МГК «ИТЕРА»?

– В 2012-2013 годы мы зафиксировали падение выручки, и нам даже пришлось прибегнуть к финансовому участию акционеров. Однако уже с 2014 года начался рост и мы наблюдаем динамичный рост выручки: например, в 2018 году она увеличилась на 45% по сравнению с 2017 годом. За неполные пять лет, которые «Итеранет» действует как независимый игрок, мы наработали новые компетенции во многих областях.

– На портале «Итеранета» обозначены пять направлений деятельности: услуги связи, информационные системы, ИБ, инфраструктура (оснащение офиса комплексом слаботочных систем с последующим обслуживанием) и отраслевые решения. Как распределяется между этими направлениями выручка компании?

– С годами эта пропорция сильно изменилась. В последнее время на первое место для нас вышли вопросы, связанные с ИБ. Это диктуется внешней средой для нашей страны, внутренними факторами и новой (постоянно меняющейся) законодательной базой в этой области. Мы делаем все больший упор на сферу ИБ, разрабатывая аппаратные и программные продукты и развивая компетенции. Второе приоритетное направление для нас – разработка программного обеспечения, как заказного, так и в рамках опытно-конструкторских работ. Также мы выполняем инфраструктурные проекты, включающие проектирование на всех этапах, поставку, внедрение и обслуживание оборудования (и сетевого, и серверного, и связанного с защитой информации).

> **«Почти в каждом проекте встают вопросы интеграции существующего ИТ-ландшафта заказчика с новой системой и создания единого центра управления»**

В начале 2000-х годов нашей основной областью деятельности был телеком, а сейчас мы лишь поддерживаем существующих клиентов, но не расширяем клиентскую базу. Причина заключается в том, что очень трудно конкурировать с государственными компаниями, которые могут вкладывать огромные деньги без ожидания быстрой отдачи. И объем выручки «Итеранета» от телеком-услуг снижается: сейчас это наименьшее с точки зрения доходов направление нашей деятельности. Когда-то мы предоставляли услуги связи по регионам России, но это уже в прошлом; мы постепенно распродаем сети в Московской области и сохраняем клиентов только в Москве. Мы сознательно не расширяем пул телеком-клиентов, работая лишь с теми, кому требуются другие наши услуги (прежде всего информационные системы и программные разработки) в совокупности со связью.

– Могли бы вы назвать крупнейших клиентов «Итеранета»?

– Нашими клиентами являются Минстрой России, Московский аэропорт Домодедово, KDV – крупный российский производитель снеков и кондитерских изделий, а также многие другие компании.

– В сфере цифровой экономики каждая отрасль и даже отдельное предприятие нуждается в уникальных комплексных ИТ- и ИКТ-решениях. Может ли оператор связи или ИТ-компания своими силами создавать такие industry-specific решения?

– Как пример, с давних пор мы внедряем системы электронного документооборота. Поначалу мы пытались использовать «коробочные» решения, которые сулили широкие возможности и короткие сроки реализации, но опыт показывал, что в таких случаях все равно требуется серьезная кастомизация под каждого клиента. И каждый раз выяснялось, что вендор (как иностранный, так и отечественный) не готов сделать дополнительный модуль или реализовать функцию по запросу одного клиента, либо это получается очень дорого. Так что как тогда, так и сейчас при переходе от клиента к клиенту с задачей внедрить аналогичную информационную систему удается использовать лишь часть предыдущих наработок – получается, что в значительной степени каждое внедрение уникально. Никуда от этого не деться: у каждого заказчика свои потребности, и под них нужно подстраиваться. Конечно, было бы проще тиражировать стандартные решения, но так не получается.

– В 2012 году «Итеранет» разработала программный комплекс АПС СОРМ. Развивается ли этот продукт и пользуется ли он спросом?

– Как раз на этом примере можно показать, что даже такой стандартный продукт требует кастомизации. Действительно, пять лет назад мы разработали СОРМ для интернет-услуг. Задолго до этого, еще в 2000-х годах, мы своими силами создали DLP-систему Business Guardian – для защиты бизнеса от утечек информации. Система DLP (Data Loss Prevention) имеет гораздо большую функциональность, чем СОРМ, и мы решили сделать на ее базе комплекс СОРМ – и для себя (как оператора телематических услуг), и для сторонних операторов связи. Однако из-за специфических требований ФСБ к системам СОРМ нам пришлось существенно доработать Business Guardian.

– Пользовалась ли успехом на рынке ваша АПС СОРМ?

– Перечень компаний, которые разрабатывают СОРМ, ограничен: они поделили весь российский рынок по географическому признаку и не очень-то открыты к сотрудничеству. Поэтому мы не стали дальше продвигать АПС СОРМ и продолжили развивать систему Business Guardian. Она внедрена у многих клиентов, и мы расширяем инсталляционную базу этой системы.

– Какие отрасли экономики являются для «Итеранета» самыми значимыми с точки зрения выручки и перспектив?

– Мы работаем с любым клиентом, из какой бы отрасли экономики он ни пришел, и не ставим приоритеты по отраслям или направлениям деятельности заказчиков. Много работая с государственными заказчиками, мы последовательно повышаем уровень присутствия в коммерческом секторе, реализуя все больше проектов в банковском секторе, в ретейле, в аэропортах, в крупных производственных структурах, в управлении недвижимостью.

– Насколько значимо для компании направление собственной разработки программных систем и ИТ-решений?

– Это важное для нас направление, и «Итеранет» имеет очень большой опыт в части создания заказного программного обеспечения. Я уже упомянул о Business Guardian – о нашей разработке в сфере ИБ, предназначенной для контроля информационных потоков в сетях. Мы ее постоянно дорабатываем, так как меняются сети, протоколы и потребности клиентов. Отраслевой специфики для таких систем

нет – различаются лишь задачи, которые клиенты могут решать с их помощью.

Еще один пример: сейчас в аэропорту Домодедово внедряется аппаратно-программный комплекс для передачи видеопотока высокой четкости в режиме реального времени, с широким набором функций по всему аэропорту, включая контроль стационарных и подвижных объектов. Мы выполняем программные разработки, а оборудование поставляет сторонний производитель.

Третий пример нашей программной разработки – платежно-пропускная система на горнолыжном курорте Сорочаны под Москвой.

Мы выполнили много сложных и уникальных проектов для государственных заказчиков, но по условиям контрактов не можем их называть. Почти в каждом проекте встают вопросы интеграции существующего ИТ-ландшафта заказчика с новой системой, а также создания единого центра управления – в этом «Итеранет» также обладает большой экспертизой. Создание интерфейсов интеграции – еще одна востребованная и растущая сфера деятельности «Итеранета».

– Видите ли вы возможности для развития «Итеранета» в новых государственных программах и инициативах: в нацпроекте «Цифровая экономика РФ», ведомственном проекте «Умный город», в государственных информационных системах типа ЕГАИС, «Меркурий», ГИС маркировки товаров и др.?

– Мы стремимся участвовать в конкурсах по таким проектам – где-то самостоятельно, а иногда в кооперации с другими крупными игроками. Группа компаний «Ростелеком» перетянула на себя немалую часть этого рынка, но и для независимых игроков здесь остается возможность работы. Наряду с федеральными ведомствами много инициатив реализуют региональные власти, и мы выполнили немало проектов, к примеру, для структур правительства Москвы. По сути, такие проекты и обеспечивают нам рост, ведь на госконтракты приходится большая часть российского ИТ-рынка.

Конечно, госкомпании имеют большие инвестиционные возможности, но у любой крупной структуры (не обязательно государственной) есть очевидный минус: высокая забюрократизированность. Принятие решений в таких структурах (а будучи в структуре холдинга «ИТЕРА», я знаю об этом не понаслышке) представляет собой длительный цикл. Поэтому у нас есть преимущество: мы значительно быстрее способны подстраиваться под задачи клиента и оперативно принимать решения о том, куда направлять усилия.

– Каков главный итог первых 20 лет работы «Итеранета»? И какова стратегия развития на перспективу?

– Главный итог – это то, что за 20 лет мы не исчезли, а живем и успешно развиваемся. И на протяжении двух десятилетий динамика роста доходов у нас всегда была положительной, за исключением трех периодов. Первым стал экономический кризис 2009-2010 годов (тогда падения доходов не случилось, но была стагнация), второй такой «плоский» с точки зрения доходов период пришелся на кризис 2014-2015 годов, а третьим стал наш внутренний кризис 2012-2013 годов, когда мы вышли из «ИТЕРЫ» и потеряли треть выручки. Это говорит о том, что тактика работы у нас правильная и позволяет компании развиваться динамично и стабильно, а не скачкообразно.

Что касается стратегии – я читал много стратегий, и ни одна потом не выполнялась. Более чем на один-два года вперед я планировать не берусь. У нас есть отдельные работы с горизонтом три года, но они не меняют общую картину бизнеса. Поэтому я бы говорил не о стратегии, а о принципах и ценностях, на которых нужно основывать свою работу. Главное что у нас есть – это люди и их компетенции. Второе по значимости – финансовые ресурсы. Имея и то и другое, можно с оптимизмом смотреть вперед.

IV Федеральный ИТ-форум
электроэнергетической отрасли России

SMART ELECTRO

Цифровая трансформация электроэнергетического сектора

20 июня 2019

отель «Хилтон Гарден Инн Москва Красносельская»,
Москва,
Верхняя Красносельская ул., д. 11а, стр. 4

Организатор: 10 лет COMNEWS CONFERENCES

Генеральный партнер: РОССЕТИ

При официальной поддержке: МИНИСТЕРСТВО ЭНЕРГЕТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Спонсоры сессий: ECI THE ELASTIC NETWORK, poly, РусГидро

При поддержке: Ассоциация ГП и ЭСК, АО «СО ЕЭС»

Smart Electro 2019 – это:

- Более 200 делегатов
- Поддержка ведущих отраслевых ассоциаций и объединений участников рынка
- Акцент на актуальные вопросы по работе и взаимодействию ИТ–служб российских электроэнергетических компаний в новых экономических условиях
- Насыщенная интеллектуальная программа с признанными экспертами делового сообщества
- Отличные возможности для делового общения и новых контактов

Основные секции форума:

- Пленарная сессия с участием руководителей ИТ–служб крупнейших электроэнергетических компаний РФ
- Будущее электроэнергетики в условиях развивающейся цифровой экономики
- Цифровая трансформация и адаптация подходов «Индустрии 4.0» к потребностям электроэнергетической отрасли
- ИТ как инструмент для повышения технико–экономической эффективности энергосистемы России
- Круглый стол. Энергетика будущего: технические решения для создания энергетических и информационных систем нового поколения

Среди докладчиков:

Любовь Андреева, директор департамента цифровой энергетики и коммерческого диспетчирования АЭС, АО «Концерн Росэнергоатом»

Евгений Грабчак, директор Департамента оперативного контроля и управления в электроэнергетике, Министерство энергетики Российской Федерации

Егор Гринкевич, заместитель генерального директора по развитию технического и нормативного регулирования, АО «НоваВинд»

Олег Калинко, советник директора, АО «Системный оператор Единой энергетической системы» (АО «СО ЕЭС»)

Сергей Микушин, начальник управления ССиТКС департамент КиТАСУ, ОАО «МРСК Урала»

Игорь Норвейшис, директор департамента ИТ, ПАО «Россети»

Валерий Селезнев, первый заместитель председателя Комитета по энергетике, Государственная Дума Федерального Собрания Российской Федерации

Роман Шульгинов, вице–президент, ПАО «Ростелеком»

Для регистрации: +7 495 933 5483, conf@comnews.ru, www.comnews-conferences.ru/smartelectro2019

Цепочка автоматизации

Фото: «Черкизово»

Летом 2018 года ПАО «Группа «Черкизово» завершила строительство мясоперерабатывающего завода-робота в Каширском районе Московской области. Эта производственная площадка, работающая под управлением платформы на базе продуктов SAP (S4/HANA и Master Data Governance), по уровню автоматизации является уникальной не только для России, но и для Европы. На заводе люди полностью исключены из большинства производственных процессов. Руководитель проектного офиса департамента ИТ ГК «Черкизово» Денис ГОРБУНОВ рассказал обозревателю «Стандарта» Якову ШПУНТУ о том, как шли работы над данным проектом.

– Что представляла собой площадка до начала работ по проекту?

– От предыдущего завода остались только стены, а кое-где и вовсе одни сваи. Оборудование было вывезено в Калининград, большая часть коммуникаций была демонтирована, они устарели и требовали замены. Так что начинали мы практически с нуля – со строительства новых корпусов со всеми коммуникациями и инфраструктурой, включая оборудование. В нашем случае можно провести аналогию с ремонтом в квартире: переделывать старое часто оказывается сложнее, чем доводить до желаемого вида «голую» коробку. С заводом ситуация схожа, особенно с точки зрения внедрения ИТ: пока идут пусконаладочные работы, есть время на то, чтобы все решения тщательно протестировать. На действующей площадке такая возможность ограничена технологическими окнами. Например, на складе время для отладки ИТ-систем можно выделить только в те промежутки, когда помещение моют, а это в среднем один час в неделю. В нашем же случае мы успевали установить и протестировать ИТ-инфраструктуру за то время, пока оборудование еще только поступало на завод.

– Кто отвечал за выбор производственного оборудования и сопряженных с ним ИТ-систем?

– У проекта был руководитель, который отвечал за все, в том числе курировал выбор технологического оборудования. Насколько я знаю, этот процесс согласовывался с производственным блоком. Что касается ИТ-составляющей, то в выборе MES-системы участвовали сотрудники моего направления стратегических проектов. Также пожелания ИТ-департамента учитывались при выборе систем низкого уровня – в частности, контроллеров. В итоге в ходе проекта «Кашира 1» был выработан стандарт, который будет использован для тиражирования на другие площадки группы «Черкизово».

– Основная часть производственных процессов на заводе автоматизирована. Пришлось ли наносить специальную разметку на пол складов или сенсорика логистических роботов позволяла обойтись без нее?

– Мне неизвестны примеры успешного использования технологии машинного зрения для логистических роботов – сейчас это фантастика. Существует несколько экспериментальных моделей, поддерживающих технологию машинного зрения, но пока они представлены только на выставочных стендах производителей роботов. Системы автоматической сенсорики также не могут обеспечить необходимой точности. Хотя для других применений – например, для измерения производительности труда сотрудников, – технологии машинного зрения использовать можно, что мы и делаем на других предприятиях группы «Черкизово».

В ходе проекта «Кашира 1» нам пришлось наносить специальную разметку. Всего в пол было вмонтировано 29 тыс. магнитов, по которым двигаются роботы-тележки.

– Нередки случаи, когда проекты по цифровизации оборачиваются для бизнеса разочарованием – отдача от проектов оказывается ниже ожидаемой, что в свою очередь связано с тем, что не были обеспечены сбор и обработка данных. Сталкивались ли вы с чем-то подобным?

– До сих пор мало кто может объяснить, что такое большие данные. Сам этот термин является зонтичным и объединяет множество разных технологий и подходов. При этом давно известна методика проведения статистического анализа, для которого нужна широкая подборка данных, позволяющая выявлять неочевидные на первый взгляд зависимости. Зачастую большими данными начинают заниматься лишь потому, что это модно и просто интереснее, чем решать рутинные задачи.

> **«В ходе проекта был выработан стандарт, который будет использован для тиражирования на другие площадки группы «Черкизово»»**

Мы считаем, что только устранив беспорядок можно приступить к большим данным. А для этого нужно выстроить цепочку «план – производство», как она описана в классической литературе 1970-1980-х годов. Инновационность нашего проекта для России, на мой взгляд, как раз состоит в том, что нам удалось решить задачи автоматизации стандартных производственных процессов, причем по всей цепочке. Отмечу, что только после этого можно приступать к внедрению элементов концепции «Индустрия 4.0», которая действительно содержит много полезного.

– Какие из технологий «Индустрии 4.0» приносят наибольший эффект при минимуме затрат?

– На мой взгляд, понятия «Индустрия 4.0» и «минимум затрат» являются антонимами, в первую очередь это касается капитальных затрат. Но если говорить об операционных расходах, то благодаря применению ряда технологий можно рассчитывать на их снижение в перспективе года-двух. Это происходит за счет того, что из производственной цепочки исключается человеческий фактор, а гибкость многих процессов, причем не только производственных, повышается. И наконец, инновации позволяют увидеть целостную картину, что человеку просто не под силу. Особенно это актуально для аграрного сектора. Человек не может оценить состояние всего стада скота или стаи птиц; в лучшем случае он оценивает группу животных и в итоге может упустить что-то критичное – например, заражение болезнями или паразитами.

Пока для многих отраслей, в том числе для нашей, мясоперерабатывающей, нет шаблонов внедрения решений, относящихся к «Индустрии 4.0». А некоторые технологии для пищевой промышленности и вовсе неприменимы – например, цифровые двойники. Но постепенно для наших индустрий начинают появляться типизированные подходы к внедрению перспективных технологий. Правда, мы в самом начале этого пути и идем буквально наощупь. В целом опыт внедрения решений, которые принято объединять термином «Индустрия 4.0», пока очень небольшой и до конца непонятно, насколько такое внедрение экономически оправдано.

Сейчас с помощью технологий RFID и промышленного Интернета вещей мы отслеживаем буквально каждую единицу сырья и готовой продукции, и за счет этого увеличивается контролируемость всей логистической цепочки. В этом, на мой взгляд, главный экономический эффект для всей индустрии производства товаров повседневного спроса. А повышение качества всей производственно-логистической цепочки улучшает взаимодействие с розничными сетями, с основным каналом сбыта продукции.

На других предприятиях группы «Черкизово» применяются технологии машинного зрения для расчета уровня производительности труда сотрудников. При этом если раньше уровень выработки рассчитывался на бригаду, то теперь мы можем вести статистику по каждому работнику. Однако принципиально нового тут ничего нет: такие рекомендации по учету выработки содержались в труде основателя научной организации труда Фредерика Тейлора «Принципы научного менеджмента» 1911 года. Мы же смогли реализовать этот подход только в 2018 году. Хотя тут вопрос технологии вторичен – все упиралось в организационные сложности.

– Проект «Кашира 1» реализован собственными силами?

– Привлекались вендоры, включая SAP, Sabris, разработчик MES-системы, ABB. Строительство комплекса ИТ-инфраструктуры велось при активном участии интегратора «Открытые технологии». Мы привыкли работать с подрядчиками. Это существенно экономит ресурсы и облегчает решение многих проблем. Выполнение проектов своими силами, на мой взгляд, – уходящая практика.

– За счет чего был достигнут экономический эффект проекта автоматизации вашего производства? Он уже окупился?

– За счет роботизации процессов на заводе работает 200 человек, хотя обычно для такой площадки нужно около 700 сотрудников. Но сокращение персонала – не единственный и не главный достигнутый эффект. Особенно с учетом того, что квалификация и, как следствие, заработная плата сотрудников, работающих на инновационном предприятии, выше, чем у тех, кто работает на традиционном производстве.

Мы решили задачу повышения качества продукции, при этом поддержание его уровня стало управляемым процессом. Качество неизменно сегодня, завтра, через неделю. На обычном заводе аналогичных результатов добиваются при существенно большем уровне затрат.

Также нам удалось добиться повышения уровня ритмичности и равномерности поставок. Это критичные параметры для работы с розничными сетями. И завод «Кашира 1» вышел на необходимые параметры за очень короткие сроки.

Но в целом об экономическом эффекте проекта говорить пока рано. С момента запуска завода прошло меньше года, и в течение этого времени продолжались пусконаладочные работы и решались возникающие проблемы.

Грани самостоятельности

Владимир ЗАХАРОВ, генеральный директор ООО «Датана» (Datana), директор департамента цифровых решений ГК «ЛАНИТ»

Фото: ЛАНИТ

Разработка собственных ИТ-решений для автоматизации бизнес-процессов с учетом специфики этой деятельности дает возможность организациям и предприятиям снижать зависимость от дорогостоящих проприетарных продуктов производителей ИТ-систем. У самостоятельных разработок есть целый ряд преимуществ, однако предприятию необходимо хорошо понимать специфику создания и внедрения собственных разработок при выборе метода автоматизации бизнес-процессов.

Основа любого ИТ-проекта в сфере автоматизации бизнес-процессов – это выбор правильного метода его реализации с учетом всех рисков. Поэтому многие компании задаются вопросом: что целесообразнее – внутренняя разработка решения или привлечение внешних подрядчиков? Преимущество собственной (in-house) разработки состоит прежде всего в том, что заказчику не нужно обучать сторонних специалистов специфике предметной области, подробно рассказывать обо всех бизнес- и технологических процессах. В другом случае заказчик тратит время внутренних экспертов на обучение чужих сотрудников, и такие инвестиции окупаются лишь при выстраивании долгосрочного сотрудничества с компанией-разработчиком. Кроме того, тут срабатывает другой немаловажный фактор – опасение заказчика попасть в зависимость от ценообразования и условий работы компании-разработчика, в случае если он переведет свои критические бизнес-процессы на стороннее ИТ-решение.

Какие же проблемы возникают при применении собственных разработок, и почему не всегда целесообразно использовать такой подход? Основная сложность при работе по модели in-house заключается в том, что компания-заказчик должна быстро стать ИТ-компанией, то есть выстроить процессы разработки и внедрения решений, нанять редких и дорогостоящих специалистов, обеспечить их мотивацию: это равносильно задаче построить бизнес «с нуля» и не дать ему времени на разгон. Ведь производство уже работает, процессы идут, автоматизация нужна срочно, сроки горят. И в этих условиях приходится скрупулезно выстраивать непрофильную деятельность, со всеми договариваться, искать новых специалистов. Эта задача не то чтобы нерешаемая, но как минимум очень сложная. Оптимальный подход – это создание на предприятии службы заказчика, которая представляет собой управленческую структуру по организации работ силами привлекаемых подрядчиков. Помимо менеджеров, в ее состав должны войти технолог, аналитик, системный архитектор и специалист контроля качества. Такая служба должна решать следующие задачи: управление проектом со стороны заказчика, коммуникация с другими подразделениями предприятия, четкая, проработанная вплоть до архитектуры постановка задачи для подрядчика и приемка результатов его работ. Как правило, при таком подходе заказчик минимизирует эффект «несговорчивого» подрядчика, создает масштабируемый орган управления задачами автоматизации, снижает время, затрачиваемое на передачу экспертизы стороннему разработчику за счет собственного экспертного буфера.

Какие условия необходимы для создания собственных эффективных решений и их эксплуатации? Прежде всего – вовлеченность персонала заказчика в выполнение задачи повышения эффективности всего предприятия. Добиться этого очень непросто, но при разработке правильной, связанной модели KPI разных структурных подразделений вероятность успеха высока. Важно сформулировать общий курс предприятия на повышение эффективности и дать сотрудникам возможность не просто приходить с инициативами о премировании, но также принимать участие в их реализации. С технической стороны имеет значение информационный ландшафт предприятия, интеграция ключевых систем между собой – как основа для автоматизации бизнес-процессов и процессов управления данными.

Собственные разработки для автоматизации бизнес-процессов могут конкурировать с проприетарными решениями за счет более глубокой экспертизы. Никто лучше сотрудников предприятия не знает его специфики, реальных условий деятельности, технологических требований, а также стратегических задач бизнеса в целом. Кроме того, эффективности собственных решений способствует отсутствие зависимости от стороннего разработчика, а также возможность менять исходный код. В собственных разработках, как правило, нет ограничений на распространение и модификацию ПО. Внедрение собственных разработок дает возможность более оперативно реагировать на изменения производственных процессов и вносить в решения корректировки для автоматизации этих процессов.

Конечно, не во всех случаях проприетарные решения могут быть заменены собственными разработками. Во-первых, этого нельзя сделать, когда нужно быстро внедрить решение или продукт, когда сроки внедрения привязаны к определенной дате. Во-вторых, не всегда удается быстро нанять достаточное количество нужных специалистов для создания собственного решения. Поэтому главное ограничение для использования модели in-house в сфере автоматизации бизнес-процессов – это время. Порой выполнение проекта автоматизации собственными силами компании просто невозможно по ряду объективных причин – экономических, кадровых или технологических.

Взаимодополняющая автоматизация

Дмитрий ХОРОШИХ, менеджер по развитию бизнеса Cisco

Применение собственных ИТ-решений зачастую является оптимальным способом автоматизации бизнес-процессов, так как подобные решения позволяют наиболее полно учесть специфику конкретного производства. Существующие инструменты разработки дают возможность вполне успешно создавать собственные решения для автоматизации. Тем не менее разработка полного цикла – от платформенного решения до исполнительных приложений – является очень трудоемкой задачей. Поэтому полезно сочетать преимущества собственных разработок и проприетарных продуктов.

Фото: Cisco

Самостоятельные разработки и доработки ИТ-решений, в том числе для автоматизации бизнес-процессов, будут всегда, ведь ни одна коммерческая система автоматизации «из коробки» не сможет на 100% удовлетворить все потребности предприятия. Главное – не увлекаться собственно разработкой. Большинство самостоятельных проектов не дают результата из-за того, что ИТ-команда предприятия вместо прикладных задач начинает решать исследовательские, причем в тех областях, где уже существуют готовые, проверенные решения. Например, за последние пять лет потерпело неудачу множество проектов в области больших данных, потому что их разработчики хотели сами строить платформу, тратили на это слишком много времени и денег – и просто не успевали приступить к решению самой задачи за отведенное на проект время. При этом, например, компания Cisco с 2013 года поставляет на рынок готовые платформы для работы с большими данными.

Некоторые предприятия просто боятся ввязываться в проекты создания собственных решений, опасаясь, что все придется делать своими силами, а ресурсов на реализацию всего стека технологий у них нет. Важно понять, какие именно функции проектируемой системы не реализуются за счет имеющихся на рынке решений, так как создание подсистем именно для таких функций принесет компании конкурентное преимущество, и именно такие подсистемы имеет смысл разрабатывать самостоятельно.

Есть несколько принципов, которые следует соблюдать, чтобы создать собственные эффективные решения. Любое решение по сути является многослойным, и его разработка состоит из определенных этапов. Сначала строится «база» – вычислительная платформа, система передачи, накопления и хранения данных, сети датчиков и т. д. И тут важно не изобретать велосипед: если существующие на рынке продукты могут в полной мере решить эти задачи, то имеет смысл ими воспользоваться. Часто компания начинает собственную разработку, чтобы снизить стоимость решения, рассчитывая на использование открытого ПО и свои силы. Такой подход хорош на этапе проверки гипотезы, но промышленная эксплуатация разработанной таким образом системы зачастую превращается в кошмар и часто ведет к непродуктивному расходованию ресурсов компании. Слова Kubernetes и Docker сейчас знает любой разработчик: использование этих инструментов позволяет очень быстро прототипировать, создать и организовать первоначальное развертывание комплексных проектов. Однако службу эксплуатации, которая решает задачи обеспечения непрерывности работы бизнес-сервисов и их интеграцию между собой, такой подход часто приводит в замешательство. У них просто нет людей, которые могут поддерживать созданные с помощью указанных инструментов системы. В этом случае успеху проекта очень поможет использование готовых решений для контейнерной виртуализации, включающих «железо», ПО, да еще и техническую поддержку вендора из единого окна.

Сравнивая собственные решения для автоматизации бизнес-процессов с проприетарными решениями, правильнее ставить вопрос не о конкуренции, а о наиболее органичном дополнении одних решений другими. Собственную разработку стоит затевать тогда, когда готового продукта на рынке нет, а решение поставленной задачи может дать компании существенные преимущества перед конкурентами. И даже в этом случае имеет смысл смотреть на готовые решения для отдельных подсистем. Например, если компания использует облачные сервисы – почти всегда для миграции приложений в облака применяются самописные скрипты. По мере разрастания приложения поддержка актуальности таких скриптов превращается в отдельный трудоемкий процесс. В этом случае использование проприетарного ПО, управляющего перемещением приложений в многооблачной среде, поможет значительно сократить расходы на эксплуатацию системы. А компания сможет сосредоточиться на решении наиболее важных для себя задач.

Конечно, практически любую ИТ-систему для автоматизации можно сделать самостоятельно. Скорее, это вопрос времени, потраченных людских ресурсов и, конечно, экономической целесообразности. Важным преимуществом крупного вендора является то, что он может делить затраты на разработку сложных систем между всеми своими заказчиками. В России, к сожалению, компании часто начинают разрабатывать те продукты, которые гораздо проще и быстрее купить готовыми. Выигрывают на рынке те, кто может трезво оценить свои силы и ценит возможность сэкономить время, обоснованно выбирая правильный метод автоматизации – за счет покупки готового решения или разработки собственного.

Старый новый налог

Фото: СТАНДАРТ

Наталья КОВАЛЕНКО, партнер и руководитель телекоммуникационной группы «Пепеляев Групп», к.ю.н.

Правительство РФ вынесло на общественное обсуждение законопроект о включении в Налоговый кодекс РФ (НК РФ) новой главы о налоге на операторов сети связи общего пользования. Вслед за этим в СМИ прокатилась волна публикаций о введении нового налога на операторов связи. Но является ли такой налог новым? И увеличит ли нововведение налоговую нагрузку на операторов связи?

Среди налоговых экспертов, представителей финансовых органов и научных деятелей давно идет дискуссия о «легализации» в НК РФ платежей, которые формально не названы налогом или сбором, не регулируются налоговым законодательством, но являются парафискальными, являются частью квазиналоговой системы и увеличивают нагрузку на бизнес. К таким платежам, ложащимся на плечи операторов сети связи общего пользования, с 2007 года относятся отчисления в резерв универсального обслуживания. Еще в 2006 году, когда принимались поправки в федеральный закон «О связи», налоговые эксперты говорили о том, что данный вид отчислений обладает признаками налога и содержит все элементы юридического состава налога. И спустя 13 лет с этим согласились представители российского Министерства финансов и, соответственно, правительства РФ.

Сейчас отчисления в резерв универсального обслуживания операторы делают с доходов, полученных в течение квартала от оказания услуг связи абонентам и иным пользователям в сети связи общего пользования, – по ставке 1,2%, не позднее 30 дней с момента окончания квартала. С 1 января 2020 года (срок вступления в силу поправок в НК РФ, в случае если они будут приняты) для операторов будут действовать практически те же правила. Выплачивать налог, так же как и делать отчисления в резерв универсального обслуживания, операторы будут самостоятельно.

В чем же отличия? Придание рассматриваемому платежу статуса налога означает, что у этого платежа меняется администратор – теперь им станет система налоговых органов. Соответственно, платеж должен быть включен в налоговую отчетность, и становится обязательной подача налоговой декларации. Таким образом, этот платеж попадает в число проверяемых в ходе камеральных и выездных налоговых проверок. Его взыскание в случае полной или частичной неуплаты будет происходить в рамках налоговых процедур, а не через суд с Россвязью. Размер штрафа в случае нарушений может доходить до 40% от подлежащего уплате налога (вместо 50-100 тыс. рублей, предусмотренных ст. 13.38 КоАП РФ за несвоевременную или неполную уплату оператором обязательных отчислений в резерв универсального обслуживания). Несогласие оператора связи с размером доначислений по итогам налоговой проверки влечет за собой прохождение обязательной досудебной процедуры обжалования. С учетом этого нагрузка на бизнес все-таки увеличивается, даже для добросовестных налогоплательщиков.

В связи с этим есть ряд вопросов, над которыми точно стоит задуматься и, возможно, поднять в ходе активного обсуждения законопроекта, пока еще не ставшего законом. Например, законопроект не предлагает внести изменения в закон «О связи» для упразднения института отчислений в резерв универсального обслуживания. А во избежание дублирования платежей такие поправки нужны.

Изначально такие отчисления были направлены на пополнение резерва универсального обслуживания, который расходуется на возмещение операторам универсального обслуживания затрат на оказание универсальных услуг связи (таксофоны, инфоматы, точки коллективного доступа к Интернету и др.).

Принятие поправок будет означать, что уплаченный налог приобретет статус обезличенного дохода в федеральном бюджете. Альтернативного механизма пополнения резерва универсального обслуживания правительство РФ пока не предложило. И если так и не предложит, то существует риск, что вмененная операторам универсального обслуживания обязанность оказывать универсальные услуги связи никак не будет компенсирована.

У резерва универсального обслуживания есть еще одна функция – а именно, финансирование создания и функционирования базы данных перенесенных абонентских номеров. Вопрос о том, из каких источников будет исполняться эта функция, пока тоже никак не урегулирован.

Также стоит обратить внимание на предлагаемый законопроектом объект налогообложения для налога на операторов сети связи общего пользования. Объектом признаются операции, касающиеся оказания услуг связи абонентам и иным пользователям в сети связи общего пользования. Под это определение попадают не только услуги связи, но также иные сервисы. Поэтому возникает вопрос: не пытается ли инициатор проекта обложить налогом даже имеющие косвенное отношение к услугам связи операции? В свете развития конвергенции услуг и появления цифровых продуктов перечень облагаемых налогом услуг может существенно увеличиться. К тому же предлагаемая формулировка объекта налогообложения вступает в противоречие с определением налоговой базы, к которой относятся доходы, полученные от оказания услуг связи абонентам и иным пользователям.

Подведем итоги. Во-первых, налог на операторов сети связи общего пользования должен заменить отчисления в резерв универсального обслуживания, сохранив базу уплаты, сроки, период и ставку. Налоговая нагрузка на операторов при этом не увеличивается (при условии изменения формулировки для объекта налогообложения и не принимая во внимание усложнение администрирования налога). Во-вторых, требуется внести некоторые поправки в законодательство. А именно: исключить из закона «О связи» положения об отчислениях в резерв универсального обслуживания; утвердить новый механизм формирования резерва универсального обслуживания взамен упраздняемого; привести в соответствие формулировки объекта налогообложения и налоговой базы – во избежание двоякого толкования объема услуг, с доходов от которых необходимо рассчитывать и уплачивать налог.

ОРГАНИЗАТОР

МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ARMY

МЕЖДУНАРОДНЫЙ ВОЕННО-ТЕХНИЧЕСКИЙ ФОРУМ «АРМИЯ-2019»

25–30 ИЮНЯ
ПАТРИОТ ЭКСПО

WWW.RUSARMYEXPO.RU

ВЫСТАВОЧНЫЙ ОПЕРАТОР

МКВ

МЕЖДУНАРОДНЫЕ КОНГРЕССЫ И ВЫСТАВКИ

ОФИЦИАЛЬНЫЙ БАНК ФОРУМА

Промсвязьбанк

ГЕНЕРАЛЬНЫЙ СПОНСОР

РОСОБОРОНЭКСПОРТ

ГЕНЕРАЛЬНЫЙ ФИНАНСОВЫЙ ПАРТНЕР

НОВИКОМБАНК

ОФИЦИАЛЬНЫЙ СПОНСОР

Концерн ВКО Алмаз - Антей

ПРИ ПОДДЕРЖКЕ

Ростех

Резервы роста

Яков ШПУНТ

Спутниковая система связи в России является практически безальтернативным средством распространения телевизионного сигнала и доступа в Интернет для труднодоступных районов и на подвижных платформах. В то же время реализация программ цифровизации открывает новые ниши для применения спутниковой связи – в частности, обеспечение M2M-взаимодействия. Получается, что на российском рынке спутниковых коммуникаций, несмотря на все сложности, есть не только заделы для сохранения позиций, но и перспективы для дальнейшего роста.

Положение в отрасли спутниковой связи обсудили участники организованной ComNews XI Международной конференции «Satellite Russia & CIS: Цифровые услуги на всех орбитах». Мероприятие собрало около 300 участников, которые представляли российских и зарубежных операторов спутниковых систем связи, органы государственной власти, научные и учебные учреждения, а также институты развития. Конференция прошла под слогоном «Цифровые услуги на всех орбитах» и была посвящена планам реализации федеральной целевой программы (ФЦП) развития космических информационных технологий «Сфера», перспективам запуска и эксплуатации мультиорбитальных группировок, а также систем дистанционного зондирования Земли (ДЗЗ), что открывает широкие возможности не только для использующих их государственных органов, но и для бизнеса.

Заместитель руководителя Федерального агентства связи (Россвязь) Игорь Чурсин в приветственном слове напомнил о роли, которую телекоммуникации играют в процессе цифровой трансформации. Он отметил значимость спутникового сегмента для обеспечения работы транспортных коридоров, что немыслимо без организации связи с подвижными платформами – судами, самолетами, поездами, автомобилями. Среди стоящих перед отраслью вызовов представитель Россвязи отметил глобальное снижение темпов экономического роста, сложности с частотным ресурсом, конкуренцию с глобальными игроками рынка, а также использование экономических и технологических санкций в качестве инструмента глобальной конкуренции.

Игорь Чурсин проинформировал участников конференции, что федеральная целевая программа развития спутниковой связи будет интегрирована в ФЦП развития космических информационных технологий «Сфера».

Подробнее о ФЦП «Сфера» рассказал первый заместитель генерального директора по развитию орбитальной группировки и перспективным проектам госкорпорации «Роскосмос» Юрий Урличич. Программа «Сфера» станет катализатором развития космического приборостроения, серийного производства космических аппаратов, ракетостроения. Сервисы, которые планируется запустить в рамках «Сферы», будут способствовать сквозной цифровизации и полной информационной связности. При этом ставится задача добиться окупаемости инициативных внебюджетных проектов. В программу будут включаться все проекты, которые докажут рентабельность и техническую реализуемость. Помимо этого Роскосмос планирует, что программа будет включать спутники «Экспресс» (оператор – ГПКС) и «Ямал» (оператор – ГКС), создание которых начнут заказывать в 2020 году, группировку на высокоэллиптической орбите «Экспресс-РВ» (ГПКС) и спутники ДЗЗ «СМОТР» (ГКС), систему ГЛОНАСС, систему спутникового IoT/M2M «Марафон»,

Фото: СТАНДАРТ

Заместитель руководителя Федерального агентства связи Игорь Чурсин отметил, что более 3 млн российских граждан живет там, где предоставление широкополосного доступа к Интернету возможно только через спутник

Первый заместитель гендиректора госкорпорации «Роскосмос» Юрий Урличич пообещал, что как только «Эфир» покажет привлеченную внебюджетную составляющую, Роскосмос включит эту группировку в программу «Сфера»

Фото: СТАНДАРТ

Заместитель генерального директора по развитию и эксплуатации систем связи ГПКС Евгений Буйдинов подчеркнул, что геостационарные спутниковые системы, в отличие от низкоорбитальных, уже подтвердили свою жизнеспособность

Фото: СТАНДАРТ

систему спутникового ШПД «Скиф», системы космической ретрансляции нового поколения «Луч» и персональной спутниковой связи «Гонец», а возможно, и низкоорбитальную группировку «Эфир», которая позиционируется как прямой конкурент OneWeb. Бюджет «Сферы» пока не утвержден.

Тем не менее Юрий Урличич упомянул, что программа будет реализована на основе смешанного государственного и частного финансирования: «Мы готовы работать со всеми, кто захочет сотрудничать, используя любые формы партнерства».

Первый заместитель генерального директора АО «Газпром космические системы» (ГКС) Петр Корвяков рассказал о долгосрочной программе развития, которая реализуется в компании и включает в себя запуск восьми спутников связи «Ямал» в период с 2019 года по 2035 год и шести спутников ДЗЗ «СМОТР» в период с 2022 года по 2035 год. На май 2019 года запланирован запуск спутника «Ямал-601», который уже прошел приемку. Сборочное производство космических аппаратов, которое ГКС строит в Щелково, также имеет все шансы войти в периметр «Сферы»: здесь могут быть построены многие перспективные спутники, которые станут частью программы.

Заместитель генерального директора по развитию и эксплуатации систем связи ФГУП «Космическая связь» (ГПКС) Евгений Буйдинов остановился на том, что комплексная орбитальная группировка на геостационарной и высокоэллиптической орбитах может обеспечить равный для всех регионов страны доступ к услугам связи и вещания, а также поможет решить задачи обеспечения безопасности и государственного управления. «Для реализации таких масштабных и технически сложных проектов требуется налаженное взаимодействие федеральных органов исполнительной власти и предприятий ведомственной принадлежности. ФЦП является тем «инструментом», который позволит организовать должное взаимодействие. Мы считаем целесообразным включение мероприятий по развитию и созданию систем спутниковой связи в ФЦП «Сфера», – заявил Евгений Буйдинов.

Старший менеджер по продажам услуг фиксированной связи и передачи данных SES Networks в России и СНГ Тимур Сарсенов рассказал о работе и планах развития негеостационарной спутниковой группировки, которая позволяет предоставлять услуги высокоскоростного доступа в Интернет по всему миру. Он особенно подчеркнул, что пока это единственный коммерчески успешный пример подобного проекта.

Участники конференции обсудили и другие перспективные направления развития спутниковой связи. Глава представительства, региональный директор Hughes Network Systems Константин Ланин рассказал об опыте компании по выходу на латиноамериканские рынки. По его словам, оказание услуг в этих странах сопряжено с трудностями и потребовало учесть целый комплекс факторов, среди которых низкий платежеспособный спрос, широкое распространение практики коллективного использования оборудования, а также слабая осведомленность потенциальных абонентов. Несмотря на все сложности, темпы роста бизнеса Hughes Network Systems в Бразилии, Колумбии, Перу, Чили и Эквадоре оказались очень высокими, и спутниковый доступ в Интернет в этих странах успешно вытесняет устаревший DSL, отметил Константин Ланин.

Директор по продажам в России и СНГ ООО «Иридиум Коммьюникешенс» Дмитрий Тарасов рассказал о подвижной спутниковой связи нового поколения Certus Next. Новое оборудование Iridium позволит обеспечивать широкополосный доступ в Интернет из любой точки Земли, не исключая открытый океан.

Региональный директор Thales Alenia Space Ашот Бакунц обратил внимание участников конференции на то, что срок активного существования спутников составляет минимум 15 лет, за которые происходит несколько смен поколений оборудования. Это обстоятельство обостряет конкуренцию спутниковой связи с оптоволоконной и мобильной, в перспективе включая 5G.

«Ситуация в отрасли непростая. Имеющиеся мощности VSAT явно избыточны, что ведет к снижению цен, которое достигает 60%, – считает генеральный директор ООО «Истар» Павел Баканов. – Тем не менее спрос на услуги для M2M и IoT может стать драйвером роста рынка спутниковой связи. Отмечу, что широкое распространение получило резервирование магистральных каналов связи для корпоративных заказчиков, мобильных операторов и вещателей, а также организация связи на мобильных платформах. Активно развивается рынок услуг виртуальных операторов (Virtual Network Operator, VNO)».

Технический директор ООО «Гилат Сателлайт Нетворкс (Евразия)» Михаил Пыхов остановился на перспективах негеостационарных спутниковых систем. Среди очевидных преимуществ он назвал высокую пропускную способность таких спутниковых каналов, что открывает возможности для полноценной конкуренции спутниковых систем с ВОЛС и сетями 5G. Однако есть и обратная сторона таких проектов: «Необходимо выводить на разные орбиты большие спутниковые группировки. При этом из-за необходимости организации сетевого взаимодействия между спутниками сложнее становится конфигурация космических аппаратов. Существенно усложняется и управление лучами. Кроме того, серьезной проблемой для операторов является высокая стоимость абонентских терминалов, что сужает целевую аудиторию и требует пересмотра бизнес-модели», – предупреждает Михаил Пыхов.

Партнерами и спонсорами конференции выступили

АО «Газпром космические системы» (ГКС), ФГУП «Космическая связь» (ГПКС), SES Networks, СПАО «Ингосстрах», Hughes Network Systems, Gilat Satellite Networks Ltd., Thales Alenia Space, ООО «Истар», ООО «Иридиум Коммьюникешенс» (Iridium), АО «Амтел-Связь», АО «Информационный космический центр «Северная Корона», МОКС «Интерспутник» и ГК AltegroSky

Материалы конференции

Фото: СТАНДАРТ

Тимур Сарсенов,
старший менеджер по продажам услуг фиксированной связи и передачи данных SES Networks в России и СНГ

Спутниковый канал на скорости оптики

Я представляю оператора единственной коммерчески успешно работающей негеостационарной спутниковой группировки, которая позволяет предоставлять услуги высокоскоростного доступа в Интернет по всему миру. Наша спутниковая система O3b, находящаяся на средней околоземной орбите, уже используется для оказания услуг клиентам. Что касается готовящейся к запуску группировки mPOWER, базирующейся на спутниках второго поколения, то это не просто слайды с красивыми обещаниями. Ее создание профинансировано, и мы находимся на стадии производства аппаратов.

В 2014 году мы вывели на среднюю околоземную орбиту первые восемь спутников группировки O3b и в том же году дополнили ее еще четырьмя аппаратами, что позволило поднять производительность, устойчивость и надежность предоставляемых сервисов. Сформировав бизнес-единицу SES Networks, мы создали и ввели в эксплуатацию гибридные решения, позволяющие использовать мощности как спутников SES, расположенных на геостационарной орбите, так и аппаратов O3b. Сегодня нам доступны такие преимущества расположенных на разных орбитах спутниковых систем, как: низкая задержка сигнала, высокая пропускная способность, глобальное покрытие, высокая доступность сервисов. Все это позволило значительно улучшить качество предоставляемых услуг. В 2018 году были запущены еще четыре аппарата первого поколения. Нам известны сильные и слабые стороны нашей гибридной системы, и мы использовали эти знания и уникальный опыт для формирования требований к mPOWER.

Главным преимуществом группировки O3b является масштабируемость. Оценив то, как быстро раскупаются имеющиеся спутниковые емкости, 4 апреля 2019 года мы запустили еще четыре спутника, что позволит нам в ближайшее время ввести в эксплуатацию 40 дополнительных пользовательских лучей. Мы видим, как быстро меняется рынок, и, используя существующую спутниковую группировку, стараемся соответствовать требованиям клиентов. При этом мы не планируем останавливаться на достигнутом: в нынешних условиях спутниковая система должна быть интеллектуальной и автоматически адаптироваться под меняющиеся требования. Такой будет O3b mPOWER, доступность которой планируется обеспечить во втором квартале 2022 года.

Мы начнем с вывода семи спутников на экваториальную орбиту (8 тыс. км), на которой расположены аппараты O3b. Это позволит обеспечить полное покрытие зон между 50 параллелями южной и северной широты. Также будет обеспечена полная интеграция системы с существующими наземными и спутниковыми сетями SES. За счет перехода к новой системе, в которой каждый спутник имеет до 5 тыс. лучей с электронным управлением, емкость каждого космического аппарата серии mPOWER будет в 10 раз превышать емкость любого из действующих спутников. Это шаг в новую эру сетевых услуг.

Еще одним важным фактором является то, что наша спутниковая инфраструктура оптимизирована для работы с провайдерами облачных услуг. Группировка O3b сертифицирована Microsoft для предоставления сервисов Azure и IBM для доступа к услугам IBM Cloud. Отмечу, что мы можем предоставлять выделенный канал передачи данных Layer 2 от облачного провайдера до потребителя. В нашей новой группировке предусмотрен целый комплекс улучшений, в том числе адаптация скорости доступа под нужды приложения за счет гибкого перераспределения емкости в прямом и обратном каналах. В этом заключается ее коренное отличие от тех систем, где используются традиционные спутниковые технологии доступа с ассиметричной скоростью передачи. Используя O3b, сервис-провайдеры могут управлять своими спутниковыми каналами так же, как и каналами наземной инфраструктуры.

O3b mPOWER способна удовлетворять различные потребности корпоративных клиентов. В частности, система может быть использована как для передачи больших объемов информации, так и для подключения удаленных сайтов среднего и малого размеров. Она дает возможность работать с любым количеством шлюзов, а также устанавливать их там, где это необходимо (например, если этого требует законодательство).

Удаленные терминалы сети будут поддерживать технологию SD WAN, что обеспечивает высокую доступность услуги и позволяет приоритезировать трафик в зависимости от потребностей приложения.

Мы уверены в успехе системы O3b mPOWER.

Фото: СТАНДАРТ

Юлия Бабкина,
начальник управления маркетинга
АО «Газпром космические системы»:
«На рынках США и Латинской Америки стоимость доступа в Интернет через спутник и DSL практически совпадает. Но в России DSL-решения втрое дешевле, и спутниковым операторам сложно с ними конкурировать»

Фото: СТАНДАРТ

Андрей Гриценко,
генеральный директор
АО «Информационный космический центр «Северная Корона»:
«Наша разработка САПР «Альбатрос» используется для анализа, расчета и моделирования спутниковых систем различного назначения. Применение данного инструмента повышает скорость доступа в Интернет в пять-шесть раз на том же оборудовании и снижает воздействие атмосферных явлений на качество сигнала»

Фото: СТАНДАРТ

Михаил Глинка,
директор департамента продаж операторских и корпоративных решений
ФГУП «Космическая связь»:
«Существует пять угроз для сетей VSAT в России: активное развитие ВОЛС, которые приходят в отдаленные регионы; появление негеостационарных систем; конкуренция с операторами мобильной связи; сокращение количества VSAT-проектов; падение маржинальности услуг»

Фото: СТАНДАРТ

Никита Демиденко,
директор по продажам в России и странах СНГ
VT iDirect Inc.:
«Нам необходимо достичь среднеевропейского уровня покупательной способности населения, на что в ближайшие годы рассчитывать не приходится. Люди не готовы тратить на Интернет половину своего дохода. А B2G- и B2C-рынки очень инерционны, и там не готовы менять работающее оборудование»

Олег Тимошенко,
директор по развитию
ГК UHP Networks:
«Темпы роста нашего бизнеса в России заметно скромнее, чем на зарубежных рынках, прежде всего из-за стагнации в B2B-сегменте. Но есть и большой отложенный спрос»

Фото: СТАНДАРТ

Фото: СТАНДАРТ

Андрей Панкратов,
заместитель генерального директора
по внешнеэкономической деятельности
АО «ГКНПЦ им. М. В. Хруничева»:
«России надо предлагать услуги запуска, аналогичные тем, что предлагает Китай. А они включают полный комплекс услуг и финансирование на весьма привлекательных условиях. Так мы сможем существенно расширить рынок запуска»

Денис Стафеев,
генеральный директор
ООО «Гилат Сателлайт Нетворкс (Евразия)»:
«В B2G-секторе развитие идет высокими темпами. Однако доступ на этот рынок многим операторам если не полностью закрыт, то заметно затруднен»

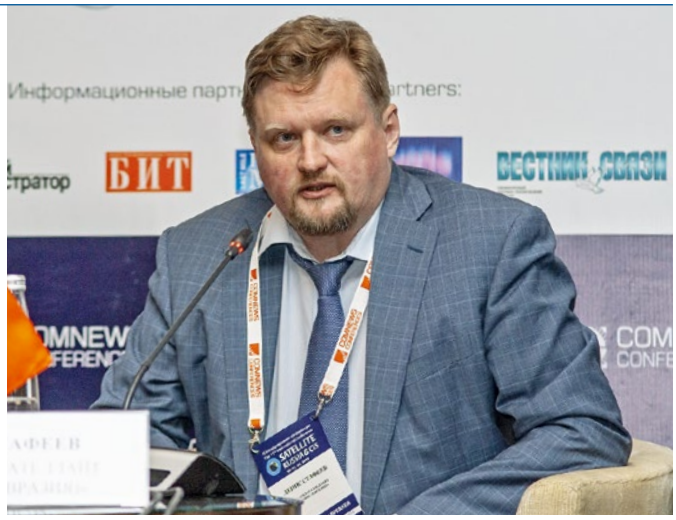


Фото: СТАНДАРТ

Фото: СТАНДАРТ

Сергей Степаненко,
технический директор
ГК AltegroSky:
«Падение заказов на новые спутники – очень серьезный негативный симптом, равно как и уход с рынка мелких игроков. Сейчас растут только такие сегменты как доступ для подвижных платформ и коллективный доступ. Не стоит забывать и о том, что люди, обделенные Интернетом, как правило, обделены и доходами»

Фото: СТАНДАРТ

Игорь Смирнов,
старший вице-президент
Marsh Space Projects:
«Без предоставления карты рисков проекта вам не видать инвестиций. Но у большинства российских операторов не организовано управление рисками»

Фото: СТАНДАРТ

Владимир Глебский,
директор отдела развития региональных проектов МОКС «Интерспутник»:
«Наша программа развития бизнеса, принятая 8 апреля 2019 года, предполагает выделение льготного финансирования для проектов в сфере спутниковой связи на сумму до $750 тыс. по ставке от 0% до 3% годовых»

Фото: СТАНДАРТ

Евгений Гетц,
генеральный директор
ООО «Центр поисковых исследований ОАО «ИСС»:
«Сценариев использования данных ДЗЗ для нужд бизнеса много. Например, есть методики, позволяющие определить оборот торгового центра по количеству автомобилей на его парковках, и предоставляемые на их базе услуги востребованы»

Фото: СТАНДАРТ

Владимир Гершензон,
генеральный директор
ООО «Лоретт»:
«Как минимум два российских ведомства – МЧС России и Росгидромет – полностью прекратили закупки данных ДЗЗ у зарубежных операторов»

Критическая «цифра»

Игорь АГАПОВ

Значение и роль критических коммуникаций расширяются. Помимо надежного инструмента связи для обеспечения деятельности особо важных государственных и коммерческих структур, они выполняют роль телекоммуникационной среды для оказания новых цифровых сервисов в области безопасности, производства и в других сферах. Кроме того, традиционная функция связи в рамках критических коммуникаций претерпевает трансформацию благодаря внедрению перспективных технологий. Все это требует поиска новых технологических и организационных форм для создания таких коммуникаций.

Вопросы традиционных и новых применений критических коммуникаций, а также проблемы технического перевооружения в этой сфере обсуждались на VII Федеральной конференции «Critical Communications Russia: Цифровые технологии для обеспечения связи и безопасности государства, общества, бизнеса», организованной ComNews. Участие в конференции приняли около 200 представителей государственных органов власти, отраслевых объединений, инновационных компаний, служб гражданской защиты и экстренного реагирования, оперативных медицинских служб, разработчиков и интеграторов ИКТ-решений, операторов связи и сетей оповещения.

Старший офицер отдела управления информационных технологий и связи МЧС России Александр Москвин остановился на роли критических коммуникаций в решении государственных задач, связанных с предупреждением чрезвычайных ситуаций и защитой от них. «Цифровые технологии – важнейший инструмент взаимодействия государства и граждан в области общественной безопасности. Очень значимые вопросы – надежная передача сигналов оповещения и связь для вызова экстренных служб. Не менее важным является обеспечение работоспособности общедоступных и специализированных сетей связи во время чрезвычайной ситуации. Решая эти и другие задачи, цифровые технологии позволяют консолидировать ресурсы всех органов власти для предупреждения и ликвидации чрезвычайных ситуаций», – сказал Александр Москвин.

Председатель правления The Critical Communication Association (TCCA) Младен Вратонич подчеркнул, что широкополосный доступ обеспечивает разнообразные возможности для критических коммуникаций, однако еще предстоит пройти долгий путь до того, когда этот вид коммуникаций будет полностью переведен на широкополосные технологии. «В 2019-2020 годах TCCA планирует провести стандартизацию функций ШПД на базе спецификаций 3GPP и разработать способы их применения в критических коммуникациях. В этот же период ожидается старт внедрения ШПД в качестве дополнительного сегмента в системах критических коммуникаций. В 2022-2023 годах начнутся широкое развертывание решений ШПД для критических коммуникаций и разработка

Фото: СТАНДАРТ

Председатель правления The Critical Communication Association (TCCA) Младен Вратонич считает, что до полного перехода критических коммуникаций на беспроводной ШПД еще предстоит пройти долгий путь

Фото: СТАНДАРТ

Старший офицер отдела управления ИТ и связи МЧС России Александр Москвин подчеркнул, что цифровые технологии – важнейший инструмент взаимодействия государства и граждан в области общественной безопасности

Директор по развитию бизнеса российского подразделения Ericsson Александр Романов полагает, что решения критических коммуникаций на базе частных LTE-сетей позволяют заменить дорогостоящие сети TETRA и DMR

Фото: СТАНДАРТ

сервисных моделей. До 2025-2030 годов большинство операторов сетей TETRA будут продолжать использовать этот стандарт, осуществляя постепенный переход на ШПД с обязательным обеспечением голосовой связи. Вопрос о том, каким будет общий эффект от применения ШПД в критических коммуникациях, остается открытым, и ответ на него зависит от методов и путей практического внедрения широкополосных технологий», – заявил Младен Вратонич.

Участники дискуссии подробно остановились на гибридных (конвергентных) сетях критических коммуникаций как на одном из возможных этапов полного перехода к широкополосным технологиям. Главный визионер и соучредитель Mentura Group Сами Хонканиеми так охарактеризовал возможности гибридных сетей TETRA/LTE: «На базе таких сетей можно организовать предоставление сервисов, основанных на передаче голоса и данных. При этом возможно совместное использование сетей общего пользования (LTE) и специализированных сетей профессиональной подвижной радиосвязи (ППРС) TETRA. Такой подход обеспечивает сочетание преимуществ беспроводного ШПД и надежности систем критических коммуникаций. Широкое использование передачи данных в такой модели позволяет повысить эффективность критических коммуникаций. С точки зрения пользователей технологии LTE и TETRA в гибридных сетях могут применяться раздельно или на основе совмещения сервисов в одном гибридном двухмодовом абонентском устройстве».

Председатель совета директоров АО «МС-Спецтелеком» Юрий Горшков описал подход к созданию конвергентных сетей с применением стандарта LTE-450. «Системы критических коммуникаций на базе технологии LTE могут развертываться в диапазоне частот 450 МГц, который по своим характеристикам хорошо подходит для этой цели. В таких сетях можно осуществить конвергенцию с технологией профессиональной подвижной радиосвязи DMR, для чего уже разработаны и выпускаются многомодовые абонентские терминалы, которые могут быть одновременно зарегистрированы в сетях LTE и DMR», – отметил Юрий Горшков.

Директор по развитию бизнеса российского подразделения Ericsson Александр Романов рассказал, что решения с использованием частных сетей LTE хорошо подходят для крупных предприятий и организаций, а их основное преимущество заключается в том, что такие решения позволяют уйти от использования дорогостоящих сетей, основанных на стандартах TETRA, DMR и других. «С технологической точки зрения LTE-сети обеспечивают более высокую скорость передачи данных и быстрое установление соединения. Немаловажным фактором является возможность присоединять инфраструктуру LTE к другим сетям связи. С точки зрения критических коммуникаций, в частных сетях LTE можно осуществлять групповые голосовые вызовы по схеме push-to-talk, что является привычным и удобным для профессиональной подвижной радиосвязи. Эта особенность дает возможность применять частные сети LTE для критических коммуникаций в области общественной безопасности (правоохранительные, пожарные, экстренные медицинские и другие службы)», – поделился с участниками конференции Александр Романов.

На мероприятии также были представлены примеры практической реализации систем критических коммуникаций с использованием различных технологических решений. Управляющий директор Zefonar Advisory, бывший комиссар по чрезвычайным ситуациям австралийского штата Виктория и национальный директор Австралийской программы оповещения о чрезвычайных ситуациях Майкл Хэллоуэс рассказал о принципах создания в 2012 году системы экстренного оповещения населения о ЧС в Австралии: «Во-первых, используемые в системе технические решения должны обеспечивать доступ к ней абонентов всех сетей мобильной связи. Кроме того, для получения сообщения о ЧС не должны требоваться какая-либо регистрация в системе или согласие абонента. Очень важно, чтобы оповещение было целенаправленным с точки зрения территории его распространения, а также чтобы система оповещения получала информацию о доставке сообщения на каждый телефон в зоне ЧС, что позволит определять количество людей, находящихся в зоне ЧС и подтверждать их информированность о ситуации».

Доцент Академии государственной противопожарной службы МЧС России Андрей Страхолис обратил внимание на специфику развертывания и эксплуатации систем критических коммуникаций в зоне ЧС. «В организации критических коммуникаций во время ЧС самым уязвимым местом является канал связи, по которому осуществляется предоставление необходимых сервисов. Поэтому обеспечение надежного канала связи – ключевой момент для эффективных критических коммуникаций, когда сети связи общего пользования могут быть значительно повреждены или совсем выведены из строя. Эта задача может решаться за счет развертывания подвижных базовых станций беспроводной широкополосной связи, с помощью которых будут оказываться услуги абонентам всех структур, участвующих в ликвидации чрезвычайной ситуации. Таким образом достигается двойная цель – обеспечение связи в условиях выхода из строя существующих на территории ЧС телекоммуникационных сетей и исключение взаимных помех радиоэлектронными средствами различных служб, работающих на месте чрезвычайной ситуации», – сказал Андрей Страхолис.

Партнерами конференции выступили

ФГУП «Российские сети вещания и оповещения» (РСВО), АО «МС-Спецтелеком», Ericsson, АО «Информационный космический центр «Северная Корона», ООО «Научно-технический центр «Протей», ПАО «Саратовский электроприборостроительный завод им. Серго Орджоникидзе», Viavi Solutions, ООО «Диджитал Кантри Нэт» (DP Net)

Материалы конференции

Сергей Сергеев,
начальник отдела разработки аналитических систем ФГУП «РСВО»:
«Системы комплексной безопасности на промышленных и других важных объектах включают в себя разнообразные компоненты – от систем контроля и управления доступом до систем оповещения о ЧС. Интеграция работы этих подсистем требует создания ИТ-инструментов интеллектуального управления»

Фото: СТАНДАРТ


Фото: СТАНДАРТ

Денис Сладких,
директор представительства в РФ и странах СНГ Viavi Solutions:
«Для критических коммуникаций особенно важны повышение осведомленности эксплуатанта сети о ее состоянии и возможность проактивного принятия решений по управлению сетью. Специальной задачей является контроль состояния инфраструктурных объектов для обеспечения непрерывности связи»

Андрей Гриценко,
генеральный директор АО «Информационный космический центр «Северная Корона»:
«Сети LTE обеспечивают «безобрывную среду» для критических коммуникаций в отличие от сетей профессиональной подвижной радиосвязи TETRA и DMR, которые очень подвержены влиянию помех со стороны радиоэлектронных средств других сетей, вплоть до полных перерывов связи на отдельных участках»

Фото: СТАНДАРТ


Фото: СТАНДАРТ

Илья Иванов,
руководитель проектов ПАО «Саратовский электроприборостроительный завод им. Серго Орджоникидзе»:
«Локализация в России производства оборудования DMR зарубежной разработки – это эффективный путь решения задач цифровизации экономики страны в части критических коммуникаций, так как локализованное оборудование может получить статус российского происхождения»

Фото: СТАНДАРТ

Евгений Опескин,
генеральный директор
ООО «Диджитал Кантри Нэт»:
«Построение сетей связи на базе однородного коммутационного оборудования отечественного производства позволяет операторам связи упростить управление сетью и сократить одномоментные капитальные затраты за счет использования расчетов с производителем по модели разделения доходов»

Фото: СТАНДАРТ

Владимир Фрейнкман,
директор по маркетингу
и системным исследованиям
ООО «НТЦ «Протей»:
«Возможность приоритезации определенных категорий трафика в частных ведомственных сетях LTE позволяет приблизить такие сети по функциональным параметрам к характеристикам, необходимым в критически важных коммуникациях, причем на базе оборудования российских производителей»

Фото: СТАНДАРТ

Александр Минов,
генеральный директор
АО «Национальный исследовательский институт технологий и связи»:
«В стандартах 3GPP для технологии 4G описаны архитектура и сервисы критических коммуникаций широкополосных систем связи в интересах общественной безопасности и борьбы с последствиями стихийных бедствий. В перспективе это будет сделано и для технологии 5G»

Фото: СТАНДАРТ

Феликс Касаткин,
директор
СПб ГУП «АТС Смольного»:
«В ситуации ЧС или особого периода нет гарантии сохранения работоспособности зарубежного оборудования профессиональной подвижной радиосвязи по различным причинам – как по причине того, что могут проявиться его незадокументированные функции, так и вследствие невозможности привлечь зарубежных представителей к обслуживанию оборудования»

Логистика на автомате

Игорь АГАПОВ

Ежегодные инвестиции во внедрение роботизированных систем в сфере логистики, включая организацию розничной торговли, уже составляют десятки миллионов долларов. В перспективе логистические системы могут стать лидирующим направлением роботизации. Чтобы реализовать этот потенциал, необходимо найти наиболее эффективные пути и средства роботизации логистической сферы.

Логистические системы уже находятся среди лидеров по объему продаж в сегменте профессиональных сервисных роботов, продолжая наращивать присутствие на рынке. Еще в 2016 году, по данным Международной федерации роботизации (International Federation of Robotics, IFR), мировые поставки таких систем в денежном выражении составили $1 млрд и были на втором месте после медицинских систем ($1,6 млрд). При этом объем поставок сельскохозяйственных роботов составил $984 млн, что было практически равно поставкам логистических. Смена лидера произошла уже по итогам 2017 года, когда поставки роботизированных систем для логистики составили $2,38 млрд, медицинских – $1,91 млрд, сельскохозяйственных – $966 млн. В 2018-м и последующих годах IFR прогнозирует опережающий рост поставок логистических роботов, в результате чего выручка от их продаж в 2018-2021 годах почти вдвое превысит показатель ближайшего «конкурента» – медицинских роботов: $21,39 млрд против $11,86 млрд.

Прогноз мировых поставок роботизированных профессиональных сервисных систем (тыс. шт., 2017-2020)

Вид систем	Объем поставок
Логистические, включая логистику внутри помещений и беспилотные средства доставки вне помещений	189,7
Роботы для связей с общественностью и развлечений	66,1
Военные и охранные системы	46,7
Механизированные экзоскелеты	41,0
Сельскохозяйственные системы	27,8
Медицинские системы	10,7
Персональные помощники	8,9
Профессиональные системы уборки/очистки помещений и территории	6,1
Строительные системы	3,2
Мобильные платформы общего назначения	2,3
Прочие	1,5

Источник: International Federation of Robotics (IFR)

Такой рост сегмента роботизированных логистических систем связан с прямым и понятным эффектом от их использования.

Руководитель Исследовательского центра проблем регулирования робототехники и ИИ (АНО «Робоправо»), заместитель руководителя рабочей группы Госдумы РФ по регулированию робототехники, искусственного интеллекта и киберфизических систем, советник юридической фирмы Dentons Андрей Незнамов уверен, что результаты автоматизации в сфере транспортно-логистических систем могут быть очень значительными: «Автоматизация перевозок грузов делает процесс дешевле, быстрее и надежнее, поэтому внедрение соответствующих систем может внести большой вклад в общее экономическое развитие каждой страны, в том числе России».

Руководитель департамента разработки беспилотных транспортных средств ООО «Когнитив» (Cognitive Technologies) Юрий Минкин придерживается похожей точки зрения. «Разработка автоматических транспортно-логистических систем необходима для повышения эффективности производства, сокращения количества производственных процессов и времени на их осуществление. Роботизация логистики уже происходит, многие компании располагают автоматизированными складами, а остальным рано или поздно придется «подтягиваться» – иначе они проиграют конкурентную борьбу», – подчеркивает эксперт.

Робологистические особенности

Автоматические транспортно-логистические системы, по словам исполнительного директора Национальной ассоциации участников рынка робототехники (НАУРР) Алисы Конюховской, состоят из двух неразрывно связанных компонентов: «В современной робототехнике выделяются сегменты складской и «большой» логистики, которая включает в себя обработку грузовых потоков и перемещение грузов на значительные расстояния. С точки зрения доступности отдельных технологий, к процессу автоматизации логистики уже сегодня могли бы присоединиться многие организации и предприятия. Другое дело, что для этого требуется разработать единые комплексы транспортно-логистических решений с использованием различных технологий роботизации. Таких решений пока мало, и их внедрение – дело будущего».

Менеджер проектов отдела «Производство. Торговля. Транспорт» Accenture Russia Юлия Шутихина описывает подходы к созданию решений для автоматизации логистики. «Важно, чтобы решение соответствовало конечным целям. Не всегда бизнесу нужен технически сложный продукт, для внедрения которого требуются серьезные

Фото: СТАНДАРТ

По словам исполнительного директора Национальной ассоциации участников рынка робототехники (НАУРР) Алисы Конюховской, к процессу автоматизации логистики могли бы присоединиться многие предприятия, но для этого нужно разработать единые комплексы транспортно-логистических решений

Фото: СТАНДАРТ

Руководитель АНО «Робоправо», замруководителя рабочей группы Госдумы РФ по регулированию робототехники, искусственного интеллекта и киберфизических систем Андрей Незнамов уверен, что эффект от автоматизации транспортно-логистических систем может быть весьма значительным, так как это делает процесс дешевле, быстрее и надежнее

инвестиции. В каких-то случаях основная выгода может лежать не в сфере транспортно-логистического планирования, а, например, в области интеграции с внешними участниками процесса. Соответственно, акцент должен быть на разработках в этом направлении. Также стоит обратить внимание на оптимальность бизнес-процесса. Если процесс не выстроен, на выходе можно получить не сокращение трудозатрат на логистические операции, а их увеличение в связи с большим количеством сценариев, требующих нестандартного подхода к их отработке. Очень важно при автоматизации начинать с проработки будущего бизнес-процесса, учитывая стратегию развития компании и лучшие практики, – рассуждает Юлия Шутихина. – Ведь зачастую сотрудники выполняют какие-то действия не потому, что они необходимы, а потому, что так сложилось исторически и никто своевременно не инициировал коррекцию процесса. В связи с постоянными изменениями рынка и законодательства, с появлением новых технологий, процессы необходимо пересматривать на регулярной основе – необходимо искать дополнительные возможности по их улучшению».

Руководитель проектов ООО «РобоСиВи» (RoboCV) Максим Фомин остановился на роботизации внутрискладской логистики, дающей такие результаты, как повышение экономической эффективности логистических операций; снижение уровня травматизма, аварийности и порчи имущества; сокращение вероятности возникновения нештатных ситуаций и повышение стабильности операций. «Особую роль здесь играет беспилотный складской транспорт. Помимо указанных общих эффектов от роботизации, беспилотный транспорт должен заменить человека на опасных, тяжелых и вредных производствах. Также роботы позволят сократить число лиц, имеющих доступ на производства и склады, где требуется соблюдение тайны (производственной, государственной, военной и т. д.)», – говорит Максим Фомин.

Совладелец и коммерческий директор агрегатора внутригородских B2B-перевозок ООО «Логософт» (Vezubr) Андрей Савин указывает на необходимость создания полнофункциональных логистических ИТ-решений. «Эффективная внутригородская логистика требует автоматизации всех этапов, а не только отдельных элементов цепочки поставок. Ряд ИТ-разработчиков уже создают алгоритмы, которые позволяют планировать и оптимально распределять между исполнителями тысячи заказов единовременно. Качество планирования можно сразу оценить в списке и на карте. Качественные маршрутизация и утилизация транспорта минимизируют количество рейсов, что снижает время пустого пробега транспорта или ожидания клиента. В крупных городах России зарегистрировано примерно 1,3 млн автомобилей грузоподъемностью от 1,5 тонн до 5 тонн. Только 17% этих транспортных средств принадлежат крупным и средним компаниям, а 83% находятся в руках мелких или частных предпринимателей и водителей. Их потенциал используется неэффективно. До 70% времени эти машины не перевозят груз, а ожидают заказов. Вот почему автоматизация должна быть направлена именно на снижение периода ожидания», – считает эксперт.

Беспилотники для логистики

Юрий Минкин напоминает, что с точки зрения логистики беспилотные грузовые транспортные средства могут быть двух категорий – для транспортировки грузов внутри складов или предприятий и для внешних перевозок. «Безусловно, для автоматизации логистической системы важны оба направления, но второе – более сложное для реализации. Развитие беспилотного грузового транспорта происходит поэтапно: от автоматизации отдельных функций автомобиля, которая уже реализуется, к абсолютной беспилотности, до которой предстоит проделать долгий путь в несколько лет. Для этого нужно решить много принципиальных технических вопросов – в частности, касающихся автоматического движения в сложных погодных и дорожных условиях, а также надежности автоматических систем управления. Все это в свою очередь требует проведения длительных и тщательных испытаний. Отдельный вопрос – появление надежных и недорогих периферических датчиков и бортовых вычислителей для автоматических систем управления беспилотными автомобилями. Еще несколько лет назад это было большой проблемой, но сейчас такие решения уже существуют», – отметил руководитель департамента Cognitive Technologies.

По оценке генерального директора ООО «Трафт» (Traft) Артура Мурадяна, использование беспилотных транспортных средств (БПТС) завершает автоматизацию логистики, которая полном ходом идет на складах и крупных производствах. «Уже во многом автоматизирована

64

Фото: СТАНДАРТ

Главный конструктор по инновационным автомобилям ПАО «КАМАЗ» Сергей Назаренко полагает, что роботизация транспорта необходима для полной автоматизации систем логистики, что принесет промышленным компаниям серьезные экономические преимущества


Фото: Vezubr

Совладелец и коммерческий директор ООО «Логософт» (Vezubr) Андрей Савин указывает, что эффективная логистика требует автоматизации всех этапов, а не только отдельных элементов цепочки поставок, и ряд ИТ-разработчиков уже создают алгоритмы, которые позволяют оптимально распределять между исполнителями тысячи заказов


Фото: СТАНДАРТ

По оценке генерального директора ООО «Трафт» (Traft) Артура Мурадяна, использование беспилотных транспортных средств завершает автоматизацию логистики, которая идет на складах и крупных производствах, и здесь важен масштаб: для получения экономии нужно внедрять беспилотники сотнями

диспетчеризация заказов, их прием и обработка, практически завершена автоматизация и оцифровка транспортного документооборота. Иными словами, автоматизировано почти все вокруг грузового транспорта – осталось автоматизировать происходящее в его кабине. И здесь главный вопрос – в эффекте масштаба. В том, удастся ли выйти на необходимый масштаб при экспериментах с БПТС. Сам по себе один беспилотник не даст никакой экономии обслуживающей его компании. Для получения экономии на топливе, на увеличенном интервале технического осмотра, на фонде оплаты труда нужно, чтобы в автопарке перевозчика были даже не десятки, а сотни беспилотников. Но далеко не все готовы к таким кардинальным экспериментам, предпочитая начать как раз с единичных внедрений, – отмечает Артур Мурадян. – Очевидно одно: БПТС помогут логистической отрасли окончательно перейти на прогнозную работу. Пиковые нагрузки, связанные с сезонностью или ажиотажным спросом продукции, будут прогнозироваться заранее, автоматические погрузчики и беспилотные грузовики будут ожидать погрузку и выгрузку у нужной площадки, роботы на погрузке будут работать сообща и без потери времени, связанной с соблюдением техники безопасности людьми».

Главный конструктор по инновационным автомобилям ПАО «КАМАЗ» Сергей Назаренко полагает, что роботизация транспорта является необходимой частью автоматизации систем логистики. «Основным эффектом от автономизации движения транспортных средств является снижение количества ДТП и повышение эффективности перевозок. Что касается роли беспилотных грузовиков и прочих автоматических транспортных средств (погрузчиков, внутрискладских транспортеров) в организации логистических систем промышленного и другого коммерческого назначения, то она заключается в обеспечении полной роботизации таких систем. Это принесет промышленным компаниям серьезные экономические преимущества, а также значительно вырастет производительность транспорта», – уверен Сергей Назаренко.

«Беспилотные транспортные средства, еще недавно казавшиеся чем-то из области фантастики, – уже реальность. Целый ряд компаний инвестирует в их разработку – например, DAF Trucks, Daimler Trucks, Iveco, MAN Truck & Bus, Scania, Volvo, – отметила Юлия Шутихина. – Горнодобывающая компания Rio Tinto использует автономный транспорт для внутренней логистики, решая таким образом проблему дефицита кадров в Западной Австралии. Грузовой парк компании на 20% состоит из автономных транспортных средств, а в прошлом году Rio Tinto начала тестирование беспилотного поезда. Пока наиболее перспективным видится применение беспилотников для обеспечения движения между складами (шаттлинг), находящимися на одной территории или близко друг от друга. Предприятия уже сейчас могут обеспечить необходимую для шаттлинга дорожную инфраструктуру и поддерживать ее на должном уровне».

Андрей Незнамов подчеркивает, что роль роботизации автомобильного транспорта в общей структуре логистических систем очень велика: «Дело в том, что процессы сортировки, погрузки и разгрузки занимают существенно меньше времени, чем перемещение грузов между объектами. Кроме того, сам процесс перевозки по своей сути хорошо поддается автоматизации, ведь движение грузового автомобиля по длинной трассе требует от водителя во многом автоматизированных навыков. Поэтому, разумеется, для полноценной роботизации логистически-транспортных систем необходима автоматизация как сортировки, учета и контроля грузовых потоков, так и грузового транспорта».


Фото: Cognitive Technologies

Руководитель департамента разработки беспилотных транспортных средств ООО «Когнитив» (Cognitive Technologies) Юрий Минкин подчеркивает, что многие компании уже располагают автоматизированными складами, а остальным придется «подтягиваться» – иначе они проиграют конкурентную борьбу

Роботизация по-нашему

Специалисты отмечают, что роботизация логистических систем развивается в России как в учетно-складском, так и в транспортном сегментах, однако в этом процессе есть ряд нерешенных проблем.

По мнению Алисы Конюховской, для нашей страны это направление особенно актуально в связи с большими территориями и объемами перевозок. «Что касается роботизированных систем «большой» логистики с внешними перевозками грузов, то для их внедрения требуется соответствующая модификация нормативной базы. Насколько существенным станет вклад беспилотных грузовиков в общее развитие автоматических транспортно-логистических систем, будет зависеть от того, как именно будут выглядеть такие системы на практике. Пока реализованных проектов роботизации в области «большой» логистики в России нет. Как правило, роботизированные системы

развиваются в сегменте внутрискладских и внутрицеховых логистических операций», – констатирует исполнительный директор НАУРР.

Андрей Незнамов также указывает на необходимость совершенствовать нормативную базу для внедрения беспилотного транспорта. «В развитии автоматического грузового транспорта в России по-прежнему есть большие проблемы с нормативным регулированием. Не вполне понятен правовой статус беспилотных транспортных средств: даже не внедрение, а само тестирование беспилотников с нормативной точки зрения затруднено. Поэтому правовые аспекты создания и внедрения беспилотных грузовиков могут стать самой большой проблемой. Однако допустить этого нельзя. Дело в том, что такие особенности России, как большие территории и протяженные маршруты доставки грузов, делают беспилотный грузовой транспорт очень перспективным направлением развития экономики», – заявил замруководителя рабочей группы Госдумы РФ.

Артур Мурадян видит те же проблемы развития беспилотного транспорта в стране: «В России развитие БПТС остается на том же уровне, что и год назад: законодательные вопросы их применения на дорогах общего пользования до сих пор не решены. Обсуждался пересмотр Венской конвенции о дорожном движении, которая запрещает людям покидать кабину автоматического транспорта, однако вопрос так и остался открытым. Поправки в правила дорожного движения, нормы уголовного и гражданского кодексов РФ, в кодекс об административных правонарушениях и законы о страховании также не внесены, хотя пакет документов и предложений направлен правительству еще летом 2017 года». Он отметил, что сейчас компания «Трафт» занимается автоматизацией «последней мили» доставки грузов, а также ведет ряд проектов, связанных с тестированием метода платунинга, когда один управляемый грузовик ведет за собой вереницу беспилотных. «В начале следующего года мы планируем провести тестовый заезд на трассе Москва – Санкт-Петербург, которую компания выбрала для комплексного эксперимента еще в 2016 году», – рассказал генеральный директор «Трафта».

Другие российские компании тоже продолжают работы по созданию систем для автономного автомобильного транспорта.

Сергей Назаренко поделился результатами, достигнутыми его компанией: «В 2017-м и 2018 годах специалисты научно-технического центра «КАМАЗа» создали опытные образцы грузовых автомобилей с прототипами собственных систем автономного движения. В 2018 году состоялся выезд автомобилей в автономном режиме, приуроченный к открытию Крымского моста».

Юрий Минкин рассказал, что Cognitive Technologies создает системы искусственного зрения и комплексные решения для автоматизации разных функций транспортных средств: «Например, наше решение для автоматического торможения уже поставляется на производство серийных автомобилей. В опытной эксплуатации находятся решения для автоматических тракторов и уборочных комбайнов. Наш проект по разработке беспилотного грузовика на базе автомобиля «КАМАЗ» завершен: мы решили поставленные задачи по отработке технологий автоматизации движения. Решения о продолжении проекта пока нет».

Максим Фомин поделился опытом роботизации внутрискладских перевозок: «Компания RoboCV является разработчиком систем интеллектуального автопилотирования для погрузочной техники. Мы разрабатываем и внедряем на площадках клиентов роботизированную складскую и производственную технику для перемещения грузов на палетах и тележках. И по опыту скажу, что сейчас российские компании заметно повышают темпы автоматизации складов и производств».

Инструмент борьбы с хаосом

Яков ШПУНТ

Говорят, что если тайна становится известной по крайней мере четверым людям, то низведение ее до уровня просто информации – вопрос времени. В современном мире, где данные хранятся в различных информационных системах, верная настройка прав доступа является залогом того, что критичная информация не попадет не в те руки. Решению этой задачи призваны помочь системы управления доступом к данным (Identity Management, IdM).

Начало 2000-х годов ознаменовалось тем, что количество и сложность систем достигло того уровня, что актуализация прав доступа к ним с помощью штатных средств стала делом долгим и трудным, по крайней мере в крупных компаниях. Этим начали пользоваться нечистые на руку сотрудники для реализации разного рода схем, направленных на получение доходов. Постепенно такая практика стала массовой, притом что сами злоумышленники долгое время оставались незамеченными.

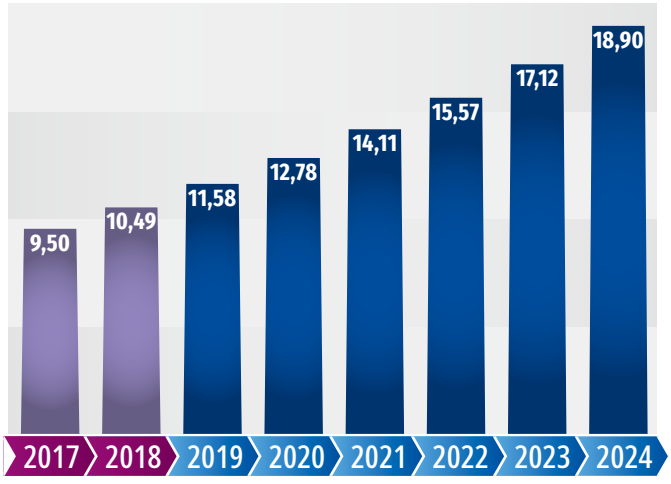
И результаты не заставили себя ждать. Так, в США массовый характер приобрели искажения корпоративной отчетности – с целью сохранить бонусы топ-менеджмента даже тогда, когда финансовые показатели компаний не были блестящими. «Подобный скандал произошел с компанией Enron (одна из крупнейших компаний США в сфере энергетики). В результате инвесторы понесли миллиардные убытки», – напоминает генеральный директор ООО «Один АйДиЭм» (1IDM) Роман Федосеев. Данный инцидент был наиболее крупным, но далеко не единственным.

Тогда же остро встала проблема, связанная с тем, что учетные данные уволенных сотрудников продолжают оставаться действующими. Также очень часто администраторы забывали отзывать права доступа у представителей внешних компаний – у подрядчиков, контрагентов, аудиторов, покупателей и заказчиков. В итоге такие учетные данные часто использовали и используют злоумышленники для проникновения в инфраструктуру компаний. Сюда же можно отнести всякого рода технологические учетные записи в разного рода системах и программно-аппаратных комплексах: их либо забывали отключать, либо не меняли пароли, выданные по умолчанию. Такие учетные записи также активно используют злоумышленники. Самым крупным инцидентом, где был применен такой сценарий, стала кража реквизитов более 100 млн платежных карт в результате атаки на американскую розничную сеть TJX в 2008 году.

Также в начале нулевых вскрылась деятельность Генриха Кибера, занимавшего весьма скромный пост в банке LGT Treuhand, который является фактически карманным банком князя Лихтенштейна. Как известно, эта страна – офшорная зона, где до недавнего времени бережно хранили банковскую тайну. Генрих Кибер обнаружил среди тех, кто пользовался услугами банка, личностей, связанных с организованной преступностью, терроризмом и просто налоговых уклонистов. Всего удалось собрать данные о без малого 6 тыс. подозрительных лиц, информацию о которых он продал правоохранительным органам нескольких стран. Только от налоговой службы ФРГ Кибер получил €4 млн. Также сотрудники немецкого ведомства организовали эвакуацию ценного информатора из Лихтенштейна. На основе собранных Кибером данных более 600 человек были привлечены к ответственности. Впрочем, от спецслужб ряда других стран, в том числе Испании, Италии, Колумбии, Франции, Генрих Кибер получил не меньше, чем от немецких налоговиков. Данный инцидент вызвал грандиозный международный скандал. Со стороны Лихтенштейна выдвигались обвинения в подрыве суверенитета этого карликового государства.

«Копирование информации – процесс немудреный, но довольно трудоемкий, требующий немалых временных затрат. То, что эти действия Кибера не вызвали никаких подозрений, по меньшей мере странно. Равно как и то, что они не были заблокированы на техническом

Прогноз динамики мирового рынка систем идентификации и управления доступом (Identity and Access Management, IAM) ($ млрд)



Источник: Global Market Insights

Фото: «Один АйДиЭм»

По мнению генерального директора ООО «Один АйДиЭм» (1IDM) Романа Федосеева, увеличению количества пользователей IdM в России способствует усиление конкуренции во всех сферах экономики, рост уровня цифровизации компаний, а также то, что в борьбе за инвестиции их деятельность становится все более прозрачной

Фото: «Солар Секьюрити»

Руководитель направления Solar inRights ООО «Солар Секьюрити» Дмитрий Бондарь отмечает, что количество проектов в сфере IdM за последние десять лет увеличилось на порядок, в том числе за счет популяризации решений усилиями вендоров

уровне», – прокомментировал инцидент эксперт международной Ассоциации аудита и контроля информационных систем (Information Systems Audit and Control Association, ISACA) Хендрик Колеманс. При этом оказалось, что предъявить лицам, по чьей вине Кибер смог совершить свой «подвиг», попросту нечего. Тем более что в то время разграничение прав доступа в инфраструктуре крупной компании с технической точки зрения если и было разрешимой задачей, то только теоретически. Так назрела необходимость в создании решений, которые автоматизировали бы процесс управления правами пользователей в корпоративной сети, – Identity Management (IdM).

Рождение IdM

Непосредственным предвестником появления данного класса систем стало принятие американского акта Сарбейнза Оксли (Sarbanes-Oxley Act, SOX) в 2002 году, действие которого распространялось не только на американские компании, но и на все фирмы, чьи ценные бумаги зарегистрированы в США.

«Данный нормативный акт не предъявляет требований к информационной безопасности компаний напрямую, однако содержит целый ряд положений относительно средств внутреннего контроля, целостности значимой финансовой информации, а также возможности аудита, – так оценивает влияние SOX на индустрию Роман Федосеев. – Первые IdM-системы появились именно как инструмент учета, контроля и аудита идентификационных данных пользователей информационных систем и их полномочий в части доступа к финансовым документам».

Руководитель направления Solar inRights ООО «Солар Секьюрити» Дмитрий Бондарь прямо связывает зарождение рынка IdM с необходимостью выполнять требования SOX в области управления идентификацией и доступом к критически важной информации. Правда, по его оценке, реально работающие продукты появились лишь спустя два года, в 2004 году. «Есть заказчики, которые приходят к нам после случившегося инцидента, связанного со злоупотреблениями правами доступа. Это обстоятельство часто является хорошим обоснованием для руководства в пользу внедрения IdM-решений. В целом же к осознанию необходимости автоматизации доступа компании приходят в тот момент, когда контролировать права доступа сотрудников вручную уже не представляется возможным», – так оценивает главные предпосылки к внедрению IdM-систем Дмитрий Бондарь.

Обозреватель Anti-Malware.Ru Александр Хонин описал схему работы IdM: «Система подключается к различным информационным ресурсам компании через коннекторы, и в последующем весь процесс управления учетными данными и правами доступа осуществляется посредством установленной IdM-системы. Как правило, схема реализуется с помощью следующих компонентов: сервер IdM; база данных IdM; коннекторы (для подключения к конечным информационным системам и ресурсам); консоль администратора; консоль различных групп пользователей».

«Фактически IdM-система является дублирующей по отношению к штатным средствам разграничения доступа на уровне СУБД или бизнес-приложения», – говорит руководитель группы информационной безопасности технологического консалтинга Oracle в России и СНГ Андрей Гусаков. Но при этом, по словам эксперта, использование IdM привносит унификацию управления всеми учетными данными, кросс-системное разграничение обязанностей, ведение истории изменений, применение средств самообслуживания (например, для сброса пароля или создания заявки). «Поэтому наличие IdM-системы важно для крупных организаций и для компаний, стремящихся максимально автоматизировать бизнес-процессы», – именно к этому, по мнению Андрея Гусакова, сводится роль типичной IdM-системы.

Такой инструментарий заметно повышает продуктивность работы ИТ-специалистов. «Представьте, что у вас на предприятии используется десять бизнес-систем, каждая со своей логикой управления учетными записями и доступом. И банальные действия по принятию на работу нового сотрудника или его увольнению превращаются в рутинную и долгую процедуру «хождения» по этим бизнес-системам с целью создать/удалить в них нужных пользователей и их права. Не говоря о том, что по законам жанра человеческий фактор даст о себе знать в полный рост: бывают случаи, когда кто-то что-то забыл отозвать или, наоборот, не предоставил. Условно, если администратор бросит все дела и будет создавать нового пользователя в десяти системах с нужными правами, то он потратит на это пару часов. В таких случаях система IdM/IAM показывает свою эффективность и полезность, ведь с ее помощью эти процессы автоматизируются и проходят по большей части без участия человека, при этом время на выполнение той же операции – несколько секунд», – иллюстрирует преимущества использования IdM коммерческий директор ООО «Аванпост» Александр Санин.

«IDM помогает исключить влияние человеческого фактора и автоматизировать процесс управления доступом и паролями к системам. Она по заданным параметрам меняет пароли доступа к разным информационным системам компании», – дополняет руководитель направления информационной безопасности АО «Бэлл Интегратор» Алексей Майоров.

Руководитель отдела решений информационной безопасности ООО «ФОРС – Центр разработки» Андрей Гридин предупреждает, что когда количество идентификационных данных и механизмов управления ими велико,


Фото: «Аванпост»

Коммерческий директор ООО «Аванпост» Александр Санин связывает повышение интереса к IdM-решениям с интенсивным изменением ИТ-ландшафта компаний: чем динамичнее меняется сфера ИТ, тем более актуальными становятся процессы централизованного управления доступом


Фото: «ФОРС – Центр разработки»

Руководитель отдела решений информационной безопасности ООО «ФОРС – Центр разработки» Андрей Гридин полагает, что росту интереса к средствам управления правами доступа способствует то, что они являются источником данных для других систем: например, в системах мониторинга событий информационной безопасности IdM может дополнять события данными о сотруднике

технические ошибки просто неизбежны. Он напоминает, что администраторам для предоставления доступа требовалось неоднократно выполнять рутинные операции (вводить ФИО, подразделение, должность, логин, права доступа и т. п.), и процесс усугублялся тем, что процедура предоставления доступа могла растягиваться на несколько дней. «А ответ на простой вопрос «к каким системам имеет доступ сотрудник, и с какими правами?» иногда требовал привлечения специалистов нескольких подразделений», – вспоминает Андрей Гридин.

По оценке начальника отдела систем управления идентификационными данными ООО «Информзащита» Александра Черных, в России практический интерес к IdM-решениям начал появляться примерно спустя пять лет после первых внедрений на Западе. Однако по-настоящему активно процесс внедрения такого рода решений начался совсем недавно, чему способствовал рост их функциональности и появление зрелых продуктов от отечественных поставщиков.

«Если в компании 50 баз данных и 10 тыс. человек, то управление паролями и доступом к ним возможно только в автоматизированном режиме», – делает вывод Алексей Майоров.

От IdM к IGA

К концу нулевых обнаружились недостатки IdM-систем первого поколения. При назначении прав обычно использовалась ролевая модель, но верно определить эти роли не всегда просто. Тем более что на первой волне экономического кризиса компании массово сокращали штаты, и в этих условиях ролевая модель просто ломалась, поскольку обязанности одного уволенного сотрудника часто перераспределялись между другими. А там, где текучка кадров традиционно велика (розничная торговля и банковская сфера), выстраивание ролей становилось и вовсе неразрешимой задачей.

С подобными сложностями столкнулись и российские компании. Это обстоятельство стало главной трудностью в ходе внедрения IdM-системы оператором «ВымпелКом», как отметил на одной из конференций руководивший в то время профильным подразделением компании Дмитрий Устюжанин. Впрочем, сложности не помешали успешно завершить проект. Но во многих других компаниях внедрение часто проваливалось уже на ранних этапах формирования ролевой модели или при попытках применить ее к каким-то системам. Бывало и так, что IdM-система просто не справлялась с теми ролями пользователей, что были разработаны, и все приходилось начинать сначала. В итоге проекты длились, без преувеличения, годами.

«Современные решения способны подстраиваться под потребности заказчиков. С момента появления IdM на рынке мы наблюдали трансформацию систем данного класса в сторону управления идентификацией и правами доступа (Identity and Access Management, IAM), а от IAM – к управлению правами доступа и администрированию (Identity Governance & Administration, IGA)», – так описывает эволюцию систем управления доступом Александр Черных.

К основным новшествам систем нового поколения директор по развитию ООО «Аванпост» Олег Губка относит появление гибких процессов сертификации и ресертификации/аттестации доступа, а также инструментов, позволяющих выявить и устранить конфликты полномочий (это необходимо для обеспечения принципа разделения ответственности, когда один человек не может обладать набором полномочий, позволяющим единолично выполнить критичную для бизнеса операцию, что часто является регуляторным требованием).

Широкое распространение облачных технологий не оказало серьезного влияния на системы управления правами доступа. По мнению Алексея Майорова, защищать облачную базу немного сложнее, но никаких трудозатрат и финансовых затрат это не несет: «Разве только настройки становятся немного специфичнее (например, меняются маршрутизация и IP-адрес). Но это не забота рядового пользователя».

Дмитрий Бондарь считает, что управление пользовательскими правами доступа для размещенной во внешнем облаке системы осуществляется посредством еще одного дополнительного коннектора, и для IdM это по сути просто еще одна информационная система.

Андрей Гридин полагает, что меняется лишь способ управления, и то при условии, что облачное решение предоставляет дополнительные возможности (интерфейс или API) по управлению учетными записями и правами доступа.

Андрей Гусаков предупреждает, что необходимо тщательно изучать вопросы, связанные с разграничением ответственности с поставщиком услуги. Однако, по мнению представителя Oracle, с точки зрения пользователя вообще ничего не меняется.

А вот появление новых движков работы с данными специалисты оценивают не столь однозначно. «Инструменты, применяемые в современных IdM-решениях, позволяют благодаря специальным интеграционным модулям наладить взаимодействие практически с любой информационной системой, – полагает Александр Черных. – Исключением здесь могут быть только платформы, используемые для хранения и обработки неструктурированных данных. В этом случае должны использоваться иные средства защиты – например, базирующиеся на анализе поведения пользователей».

Дмитрий Бондарь более оптимистичен: «Задача управления доступа к информационным ресурсам, таким как папки и документы, стояла перед IdM практически всегда, и она так или иначе решается в рамках проектов: где-то

сводится к ролям/профилям, где-то решается через специализированный функционал управления информационными ресурсами».

«К новым движкам работы с данными логично отнести стандарты федеративного и кросс-доменного управления, а также возможность обращения за IdM-услугами через REST-сервисы, работающие по модели распределенной по сети архитектуры. Oracle понимает их важность и обеспечивает возможность работы своих решений с OpenID Connect, OAuth2, HTTP cookies, JWT-based tokens, SAML, SCIM, RESTful APIs и другими стандартными протоколами. Их применение позволяет значительно ускорить процесс внедрения и адаптации новых бизнес-сервисов различными клиентами», – дополняет Андрей Гусаков.

Блестящее будущее

По оценкам аналитиков ИБ-рынка, именно сегмент средств управления доступом является одним из самых быстрорастущих на российском рынке. И тому есть несколько причин, среди которых расширение предложения, в том числе от российских вендоров, чьи продукты лучше адаптированы под специфику используемых у нас систем. Например, только отечественные продукты поддерживают системы, работающие поверх СУБД PostgeSQL, а именно этот сервер баз данных популярен в проектах по импортозамещению. Плюс ко всему, использование российских разработок снимает проблему политических рисков, с которыми некоторые организации уже столкнулись.

Традиционно системы управления доступом были ориентированы на рынок крупных компаний, с количеством рабочих мест от 10 тысяч. Но практический интерес к таким системам начал появляться и у предприятий более скромных размеров, а им крупные вендоры ничего предложить не могли. Флагманские продукты были для небольших компаний слишком сложными, дорогими и перегруженными невостребованными функциями. Кроме того, многие зарубежные вендоры не имеют представительств в России и по их продуктам невозможно найти специалистов.

Руководитель дирекции информационных технологий ООО «НТВ-Плюс» Дмитрий Мозжегоров рассказал о проекте по автоматизации процесса управления учетными записями и правами доступа пользователей с использованием платформы 1IDM: «Мы рассматривали несколько вариантов решений – как российских, так и зарубежных разработчиков. Был сформирован ряд ключевых критериев, предъявляемых к IdM-системе, в том числе стоимость владения, скорость внедрения и доступность специалистов по ее доработке и сопровождению. Решение 1IDM в полной мере отвечает всем нашим требованиям: оно разработано на базе отечественной платформы 1С, система гибкая и имеет открытый код, так что в случае отказа от одного подрядчика мы сможем безболезненно передать ее сопровождение другому. И наконец, решение легко интегрируется с системами других поставщиков». По словам Дмитрия Мозжегорова, на реализацию проекта ушло около двух месяцев. «Чуть больше времени потребовалось на внутреннюю коммуникацию – на объяснение особенностей работ и описание преимуществ, которые получат сотрудники службы безопасности и управления кадрами. Сначала мы сформировали единое информационное поле для взаимодействия представителей разных подразделений, затем приступили к выбору подрядчика и технической реализации проекта», – добавил руководитель дирекции «НТВ-Плюс».

С другой стороны, российские продукты часто критикуют за «сырость», сложности с адаптацией под нужды заказчика и проблемы с пресейлом. Именно этими факторами руководитель отдела информационной безопасности банка «ДельтаКредит» Всеслав Соленик объяснил то, что ни один из российских продуктов не смог удовлетворить требованиям в ходе проекта по внедрению IdM-системы в банке. Поэтому в итоге было выбрано зарубежное решение.

Фото: «Бэлл Интегратор»

Руководитель направления информационной безопасности АО «Бэлл Интегратор» Алексей Майоров убежден, что если в компании со штатом в 10 тыс. сотрудников 50 баз данных, то управление паролями и доступом к ним возможно только в автоматизированном режиме

«Порой мы видим живой интерес и от совсем некрупных организаций, в штате которых насчитывается 300-500 сотрудников. Связано это в первую очередь с интенсивным изменением ИТ-ландшафта компаний. Чем динамичнее меняется ИТ, тем актуальнее становятся процессы централизованного управления доступом. Все прекрасно это понимают, иначе будет хаос», – отметил Александр Санин.

«Ситуация на российском рынке такова, что конкуренция во всех сферах экономики усиливается, при этом растет уровень цифровизации компаний. Все это на руку производителям IdM-решений и их партнерам. Кроме того, в борьбе за инвестиции деятельность компаний становится более прозрачной, что также увеличивает вероятность роста пользователей IdM», – полагает Роман Федосеев.

Начинает играть свою роль и появление регуляторных требований. «В рамках обеспечения безопасности значимых объектов критической информационной инфраструктуры РФ утвержден приказ ФСТЭК России №239, где в перечне организационных и технических мер содержатся идентификация и аутентификация, а также управление доступом», – напоминает Александр Черных.

Повысилась и информированность потенциальных заказчиков. «Если сравнивать количество проектов в сфере IdM, реализуемых сейчас и десять лет назад, то их количество увеличилось на порядок. На мой взгляд, этот рост обусловлен популяризацией темы усилиями вендоров. Сейчас компаниям уже не нужно объяснять, что это за системы и для чего они нужны», – уверен Дмитрий Бондарь. Также, по мнению руководителя профильного подразделения «Солар Секьюрити», до сих пор действует эффект отложенного спроса, возникший после снижения бюджетов на острой фазе кризиса в 2014-2016 годах.

По мнению Андрея Гусакова, на российском рынке главным фактором роста спроса на средства управления доступом является повышение зрелости отечественных компаний. Именно ее отсутствие, по оценке Алексея Майорова, было главным тормозом при внедрении такого рода систем. Основной точкой роста представитель «Бэлл Интегратора» считает крупные территориально распределенные компании, прежде всего это банки и телекоммуникационные операторы.

Андрей Гридин полагает, что росту интереса к средствам управления правами доступа способствует то, что они являются источником данных для других систем: «Например, в системах мониторинга событий информационной безопасности IdM может дополнять события данными о сотруднике, которому принадлежат учетные записи, а при мониторинге инфраструктуры – статистику по изменению количества учетных записей для оценки состава лицензий».

Секреты массового пользования

Игорь АГАПОВ

Персональные данные в электронном виде все шире используются государственными и коммерческими структурами для решения разнообразных задач – например, при предоставлении услуг в режиме онлайн. При этом перечень используемых данных постоянно растет. Такие тенденции обусловливают усиление угроз компрометации персональных данных и их утечек. Одновременно практика показывает, что не существует какого-то одного метода надежной защиты данных, и требуется комплексный подход к решению этой задачи.

Новые электронные системы, в которых используются персональные данные (ПДн), появляются чуть ли не каждый день. Причем их масштаб постоянно растет: такие системы все чаще охватывают граждан целых стран, а порой приобретают глобальные размеры, как это происходит, например, с базами данных о пользователях крупных социальных сетей или электронных торговых площадок.

Россия не остается в стороне от этого процесса. Данные о гражданах собирают, хранят и обрабатывают самые разные коммерческие и государственные структуры – от магазинов и школ до операторов связи, банков и структур исполнительной власти. Согласно закону «О персональных данных», такими данными считается «любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу». Таким образом, в нашей стране в электронном и физическом обороте уже находится огромный массив персональных данных, а в перспективе он увеличится многократно. В этой связи планируется создание всеобщих баз данных обо всем населении России. В частности, речь идет о едином федеральном информационном ресурсе или о так называемом едином электронном реестре населения. Концепция этого реестра утверждена правительством РФ в июле 2017 года на основании указа президента РФ Владимира Путина. Затем, в июне 2018 года правительство подготовило проект соответствующего закона, но он пока еще не внесен на рассмотрение в Государственную думу.

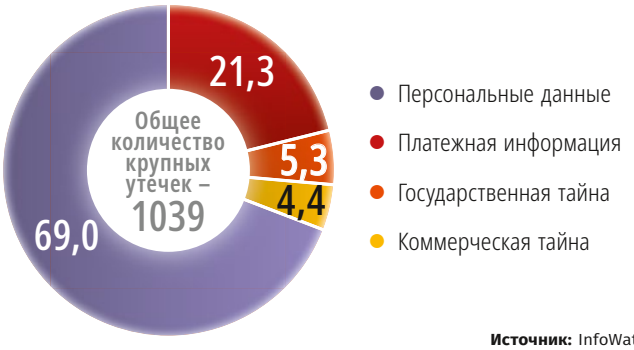
Правительственная концепция предусматривает, что в реестре будут содержаться данные свидетельств о рождении; документов, удостоверяющих личность; документов, удостоверяющих право физических лиц осуществлять определенную деятельность (дипломов, лицензий и т. д.); сведения о постановке на учет в налоговых органах, о регистрационном учете по месту жительства или месту пребывания; сведения о регистрации в системах обязательного пенсионного, медицинского, социального страхования. Другими словами, реестр станет источником практически исчерпывающих данных о гражданине с точки зрения его отношений с государством.

Другая система персональных данных всероссийского масштаба – уже создаваемая Единая биометрическая система (ЕБС), первоначально предназначенная для распознавания личности граждан по биометрическим признакам при обращении в финансово-кредитные организации (банки) с перспективой использования этих данных и в других сферах.

Начальник управления информационных систем Департамента информационных технологий (ДИТ) города Москвы Владимир Бугров полагает, что рост количества собираемых данных и содержащих их систем создает предпосылки для их недобросовестного использования. «Безусловно, большое количество персональных данных, обрабатываемых в информационной системе, может послужить дополнительным стимулом для недобросовестных граждан в организации атак на ресурсы с целью хищения информации, ее искажения или удаления», – говорит Владимир Бугров.

Директор по консалтингу АО «ИнфоВотч» (InfoWatch) Мария Воронова видит прямую зависимость уровня угроз персональным данным от роста объема этих данных в информационных системах различного назначения и роста количества таких систем. «С ростом объема собираемых данных и количества систем, в которых они обрабатываются, растут и риски, связанные с возможной компрометацией ПДн граждан. При этом отмечается очевидная тенденция к созданию единых систем больших данных (big data): Единая система идентификации и аутентификации (ЕСИА), Единая система госуслуг, системы регистраций и записи актов гражданского состояния. При подобной централизации

Структура утечек конфиденциальных данных в мире за I полугодие 2018
(Доля в общем количестве утечек, %)



Источник: InfoWatch

крайне важно обеспечить достаточный уровень информационной безопасности этих систем, и речь идет не только о сохранности конфиденциальности данных, но также об их целостности (защита от модификации) и доступности», – поясняет Мария Воронова.

Опасность укрупнения

Специалисты отмечают, что появление все более крупных баз данных само по себе так или иначе увеличивает их уязвимость.

Председатель коллегии адвокатов «Вашъ юридический поверенный» Константин Трапаидзе считает это очевидным: «Разумеется, вероятность утечки персональных данных возрастает по мере того, как увеличивается количество данных, которые кто-то зачем-то собирает, и количество систем, где такие данные обрабатываются и хранятся. Понятно, что чем больше мест, откуда можно что-то украсть, тем вероятнее, что это будет украдено».

Владимир Бугров считает, что прямой линейной зависимости роста угроз компрометации персональных данных, обрабатываемых в информационной системе, от роста их количества нет. «Это связано с тем, что угрозы зависят не от самого объема данных, а от структуры информационной системы, от используемых в системе технологий и оборудования, от особенностей взаимодействия систем между собой и Интернетом, используемых мер по защите этих систем», – рассуждает начальник управления ДИТ Москвы.

Ведущий аналитик департамента информационных технологий ЗАО «КРОК инкорпорейтед» Анастасия Федорова также говорит о последствиях увеличения масштабов баз данных. «Если в организациях налажены процессы по обеспечению безопасности обрабатываемых данных, то большинство возникающих угроз, в том числе связанных с возрастанием объемов обрабатываемых данных и увеличением числа самих информационных систем (ИС), решаются превентивно. Однако часто бывает так, что рост ИС и их интеграция приводят к тому, что контроль за обрабатываемыми данными, функционирующими средствами защиты и настройками ослабляется. Этим и могут воспользоваться злоумышленники», – отмечает Анастасия Федорова.

Тему укрупнения баз продолжает эксперт по защите информации ЗАО «Производственная фирма «КСБ Контур» Анастасия Алехина: «Уровень угрозы персональным данным зависит в первую очередь от возможностей злоумышленника, а чем больше персональных данных хранится в системе, тем больше она интересует преступников. Спрос порождает возможности, что повышает актуальность угрозы. Что касается роста количества информационных систем, то если правильно обеспечивать их безопасность, это наоборот усложняет доступ нарушителя к данным. Ведь теперь злоумышленнику надо взломать не один рубеж обороны, чтобы получить доступ ко всем данным, а несколько».

Инженер по облачным решениям и информационной безопасности ООО «Связь ВСД» (Linxdatacenter) Борис Меркулов согласен с тем, что уровень угроз персональным данным прямо пропорционален количеству самих данных и систем их обработки. «Чем больше систем появляется, тем выше вероятность компрометации данных, которые в них хранятся. Особенно часто такие утечки касаются финансовых и медицинских данных граждан. Недавний громкий случай – утечка базы с персональными данными и фотографиями заемщиков из Южного, Уральского и Приволжского федеральных округов и всеми их заявками на кредиты. Нередки случаи утечек и из государственных информационных систем. Свежая история – утечка данных по платежам за штрафы ГИБДД и задолженности по исполнительным производствам службы судебных приставов. Причем если сами происшествия часто становятся известны широкой публике, то о наказании за подобные утечки мы, как правило, ничего не знаем. Пару лет назад мы все слышали об утечке данных из Пенсионного фонда, а результатов проверки обнародовано так и не было. К сожалению, подобные новости сегодня уже никого не удивляют», – сетует Борис Меркулов.

Фото: «КРОК»

Ведущий аналитик департамента информационных технологий ЗАО «КРОК инкорпорейтед» Анастасия Федорова подчеркивает, что для защиты персональных данных необходим комплексный подход и соблюдение требований безопасности на всех стадиях жизненного цикла информационных систем, акцент на один из компонентов защиты может привести к компрометации данных

Данные под ударом

Виды угроз персональным данным, как и пути неправомерного доступа к ним разнообразны.

Мария Воронова перечисляет наиболее значимые из них: «Прежде всего это компрометация данных. При этом наиболее популярный вид незаконного использования персональных данных – перепродажа с целью совершения мошеннических действий. Например, применяя приемы социальной инженерии, мошенник под видом банковского работника обманным путем вынуждает гражданина совершить какое-либо действие с банковской картой или счетом. Также распространено использование паспортных данных (в том числе скан-копий паспорта) для оформления микрозаймов или для регистрации номеров у операторов связи. Причем эти же номера, как правило, в дальнейшем могут быть использованы для совершения мошеннических действий».

Анастасия Алехина уверена, что значимы все угрозы, которые несут в себе нарушение целостности, доступности и конфиденциальности данных. «Для каждой информационной системы персональных данных находятся актуальные угрозы, которые часто не совпадают с угрозами для других информационных систем. Например, если информационная система отключена от Интернета, а все данные передаются через flash-накопитель, то угрозы, связанные с сетью, можно не рассматривать. Вместо этого нужно сосредоточиться на том, чтобы к информационной системе могли подключаться только определенные flash-накопители и был невозможен запуск вредоносного программного кода со съемных носителей», – поясняет эксперт «КСБ Контура».

Анастасия Федорова обращает внимание на то, что все угрозы могут быть разделены на несколько видов. «Если мы говорим о защищаемых внутренних информационных системах и ресурсах компаний, которые находятся в зоне интересов злоумышленников, то это могут быть прямые атаки на ПДн и системы защиты (логические атаки на прикладное ПО, выявление и эксплуатация уязвимостей и др.). Примером служит недавняя утечка данных пользователей из социальной сети Facebook, когда с помощью вредоносных расширений для браузеров злоумышленники смогли собрать личную информацию десятков миллионов человек, включая личные сообщения. В целях получения нужной информации злоумышленники широко применяют социальную инженерию и фишинг, а иногда и подкуп привилегированных пользователей таких систем. Сетевые сервисы активно развиваются, формируя новые угрозы безопасности информации, что также приводит к утечкам

Фото: ДИТ

Начальник управления информационных систем Департамента информационных технологий (ДИТ) города Москвы Владимир Бугров считает, что рост угроз компрометации персональных данных, обрабатываемых в информационной системе, не зависит напрямую от роста их количества, так как угрозы зависят не от объема данных, а от структуры информационной системы

персональных данных. Например, одна российская компания забыла закрыть некоторые разделы корпоративного сайта от индексации, в результате чего все резюме, когда-либо отправленные соискателями работы в компании через веб-форму на этом сайте, стали отображаться при запросах в поисковых системах», – рассказал аналитик компании «КРОК».

По мнению Бориса Меркулова, не вполне корректно делить угрозы на более или менее значимые. «Для каждой информационной системы выстраивается индивидуальная модель угроз. Компетентные специалисты-эксперты в области защиты информации оценивают абсолютно все возможные угрозы. Получается, что это практически полностью экспертная оценка, поэтому есть возможность варьировать уровень защищенности, понижая или повышая его при необходимости. Это плохо, и в будущем еще сыграет свою роль. Кроме того, в текущих моделях угроз отсутствуют многие потенциальные уязвимости, которые могут содержаться в системах, имеющих прямое или косвенное отношение к защищаемой ИС. Иными словами, возможен запуск цепной реакции, которая может привести к компрометации целевой системы. Не стоит забывать и о человеческом факторе. На сегодняшний день это самый значимый вид угрозы не только персональным, но и в целом любым данным в организациях», – делится взглядом на проблему специалист по информационной безопасности Linxdatacenter.

Константин Трапаидзе также указывает на человеческий фактор как на один из источников угроз персональным данным. «Оставляя в стороне технические причины утечек персональных данных, можно с уверенностью сказать, что главная причина утечек – банальное воровство данных недобросовестными сотрудниками компаний и организаций с целью нажиться за счет их продажи. Все мы знаем случаи, когда в Интернете появлялись предложения купить целые базы данных телефонных абонентов, пациентов лечебных учреждений, граждан, зарегистрировавших автомобили в ГИБДД, и так далее. При этом такая ситуация вовсе не означает, что с действиями недобросовестных сотрудников нельзя бороться: это вполне реальная задача, для решения которой нужна соответствующая воля руководства компаний и учреждений», – заявил глава юридической компании.

Безличная безопасность

В качестве одного из способов снизить угрозу утечки персональных данных заинтересованные компании и организации называют их обезличивание (деперсонализацию), когда данные «привязаны» не к имени и фамилии человека, а к условному номеру, который уже соотносится с именем субъекта данных. Однако эксперты считают, что возможности такого способа защиты весьма ограничены.

Владимир Бугров указывает, что в настоящее время законодательство оговаривает, в каких случаях необходимо обезличивание персональных данных. «Например, при публикации судебных решений. Такой подход не позволяет использовать обезличивание как полноценный инструмент защиты ПДн. При этом обезличивание данных как средство защиты может только снизить риски причинения вреда конкретным гражданам. Однако лишь в том случае, если произошла утечка только обезличенных данных и неизвестны алгоритмы, по которым обезличивание проводилось, а также нет никакой дополнительной информации, по которой можно восстановить ПДн», – поясняет сотрудник ДИТ Москвы.

Анастасия Федорова характеризует особенности обезличенных баз персональных данных и обозначает условия, когда их безопасность может быть нарушена.

«При обезличивании персональные данные «разбиваются» на несколько логических баз, содержащих только часть данных субъекта, по которым его невозможно идентифицировать. Чаще всего такие базы между собой связываются внутренними идентификаторами. В случае компрометации одной из таких баз, риски для субъекта данных (гражданина) значительно минимизируются. Однако если будут скомпрометированы механизмы, применяемые для обезличивания, и большая часть данных из баз, злоумышленник получит возможность ретроспективно восстановить полные данные субъекта и использовать их в своих целях», – отмечает менеджер «КРОКа».

Борис Меркулов полагает, что декларируемая некоторыми информационными системами деперсонализация данных граждан вряд ли может снизить уровень угроз их компрометации. «Деперсонализация практически никак не влияет на безопасность персональных данных. Обезличенные ПДн не перестают быть персональными данными, и их необходимо защищать точно так же, как и персональные данные в обычном формате. Может показаться, что деперсонализация снижает уровень угроз, но это не так. При компрометации информационной системы злоумышленнику обычно доступен алгоритм деперсонализации и обратного восстановления, используя который можно вернуть персональные данные к предыдущему состоянию. Деперсонализация защищает ПДн на уровне базы данных, но никак не на уровне информационной системы в целом», – подчеркивает специалист Linxdatacenter.

Мария Воронова говорит, что обезличенное хранение увеличивает уровень защищенности персональных данных, но не является панацеей. «Суть этой процедуры заключается в том, что кусочки информации, составляющие обезличенные данные, разносятся по разным системам или базам данных. Связка осуществляется исключительно по ключу (ID). То есть каждый отдельный хранящийся фрагмент – это обезличенные данные, но если собрать все вместе – это вновь персональные данные. Таким образом, злоумышленнику для получения всей информации потребуется залезть уже не в одну систему, а в множество систем, что сделает более трудоемким нелегитимный доступ к данным», – отметила эксперт InfoWatch.

Как остановить утечки

Специалисты приводят целый перечень мер, которые можно применять для защиты персональных данных.

Анастасия Федорова подчеркивает, что необходим комплексный подход и соблюдение требований по обеспечению безопасности на всех стадиях жизненного цикла информационных систем. «Как показывает практика, чрезмерный акцент на один из компонентов обеспечения защиты может привести к компрометации и утечке данных. При создании информационных систем, в которых будут обрабатываться персональные данные, необходимо использовать безопасные методы программирования и разработки ПО,

а также регулярно тестировать сформированный код на уязвимости и закладки. Исходя из этих принципов, «КРОК» реализует все необходимые работы – от разработки организационно-правовых мер защиты до проектирования и внедрения технических средств защиты информации», – пояснила ведущий аналитик департамента информационных технологий компании.

Об обязательности комплексного подхода к защите персональных данных говорит и Владимир Бугров: «Утверждение о том, что какие-то методы защиты ПДн более эффективны, а какие-то менее – некорректно. Защита персональных данных достигается только за счет комплексного подхода к обеспечению безопасности информации. Организационные меры без применения технических средств защиты информации не будут эффективны в современных системах, как и использование исключительно технических средств без выстраивания регламентов работы в системе и обеспечения ее безопасности. Особую роль в обеспечении защиты информации играет осведомленность сотрудников в области информационной безопасности».

Мария Воронова описывает стандартный комплекс мер, необходимых для защиты данных. «Во-первых, это разграничение легитимного доступа к данным: к системам, где хранятся персональные данные и другая чувствительная информация, должны иметь доступ только те сотрудники, которым это необходимо в соответствии с должностными обязанностями. Во-вторых, защита информационных систем и инфраструктуры от проникновения извне. В-третьих, использование систем контроля информационных потоков и защиты от утечек (DLP-системы). В-четвертых, обучение сотрудников и граждан так называемой кибергигиене – правилам безопасного обращения с персональными данными. Для достижения нужного результата группа компаний InfoWatch предлагает все необходимые услуги и продукты. Наш флагманский продукт – решение для предотвращения утечек информации (DLP) и защиты организаций от внутренних угроз информационной безопасности InfoWatch Traffic Monitor», – сообщила директор по консалтингу InfoWatch.

У Бориса Меркулова – свой перечень необходимых мер защиты. «Наиболее эффективные меры – использование антивирусной защиты, периодическое сканирование уязвимостей, сканирование сети, контроль парольной политики, использование защищенного канала связи при передаче ПДн за пределы контролируемой зоны, защита среды виртуализации, если мы говорим об облаках, и, конечно же, резервное копирование. Другие меры защиты могут быть избыточными и не имеют особого смысла при компрометации чего-либо из вышеперечисленного», – считает инженер по облачным решениям и информационной безопасности Linxdatacenter.

На важность юридических методов защиты персональных данных обратил внимание Константин Трапаидзе, который считает, что к традиционно обсуждаемым техническим и организационным мерам следует добавить защиту персональных данных правовыми средствами. «Я имею в виду, что граждане должны требовать компенсации за нанесенный им ущерб вследствие компрометации персональных данных, а ответственность за это, включая материальную, должны нести не только физические лица, непосредственно похитившие данные, но и юридические лица, хранившие эти данные и не обеспечившие их надежную защиту. В целом приходится констатировать, что по мере распространения цифровизации всех отраслей экономики и социальной жизни гражданам придется учиться жить в мире, где любые их персональные данные в любой момент могут стать известны любому другому человеку. И очень важно, чтобы и граждане, и общество, и государство формировали культуру защиты данных правовыми средствами», – резюмирует председатель коллегии адвокатов «Вашъ юридический поверенный».

Доверие и управляемость

Яков ШПУНТ

Переход в публичное или гибридное облако требует от коммерческих компаний и государственных организаций смены подходов к обеспечению безопасности. Это актуально еще и в связи с тем, что традиционная парадигма корпоративного сетевого периметра полностью себя исчерпала. В ответ на эти вызовы формируются подходы, позволяющие добиваться приемлемого уровня безопасности и соответствовать нормам отраслевого и государственного регулирования, – в частности, к ним относится концепция программно определяемого периметра. Одновременно с этим трансформируются и сами средства защиты, адаптируясь к меняющимся угрозам и мигрируя в виртуальные и облачные среды.

Использование облачных сервисов в ИТ-инфраструктуре стало распространенной практикой на предприятиях любого масштаба и практически во всех странах. Переход в облако позволил решить множество проблем, связанных с эффективностью использования ИТ. Например, проблему обязательного перелицензирования ПО, вопрос дефицита кадров, проблему избыточных мощностей, которые востребованы только в отчетный период, а в остальное время простаивают, занимая место в серверных. Но есть и обратная сторона процесса: широкое использование облаков и смежных технологий ставит перед потребителями новые вызовы с точки зрения обеспечения информационной безопасности (ИБ).

Директор по технологиям группы компаний «ФОРС» Андрей Тамбовский напомнил, что развитие облаков шло наперекор логике развития ИТ, предполагающей, что технологическое решение сначала апробируется в корпоративном сегменте, затем адаптируется для нужд компаний среднего и малого бизнеса и только потом попадает на рынок конечных потребителей. Целевой аудиторией облачных сервисов изначально были конечные пользователи, затем – микро- и малый бизнес, и только потом их начали адаптировать для нужд B2B- и B2G-сегментов. Данное обстоятельство, по мнению Андрея Тамбовского, породило недоверие к облачным сервисам со стороны крупного бизнеса и государственных органов. И только авторитет крупных корпораций, которые вышли на этот рынок, способствовал преодолению недоверия. Такие поставщики облачных услуг успешно проходят сертификацию на соответствие нормам различных отраслевых и национальных стандартов в области безопасности, включая PCI DSS, ISO 27001, а также аттестацию на соответствие российским и мировым нормам по защите персональных данных.

Однако сертификация не всегда гарантирует надежность компаний, которые предоставляют облачные услуги, используя устаревшие подходы к обеспечению информационной безопасности. Так, в текущем году стало известно, что Facebook хранила регистрационные данные десятков миллионов пользователей своих сервисов в текстовых файлах, доступ к которым легко могли получить практически все желающие. Представители интернет-компании заявили, что проблема была устранена, но впоследствии повторялись инциденты, когда такая информация попадала к злоумышленникам.

Несколько лет назад пользователи DropBox столкнулись с массовыми атаками спамеров: их адреса попали к злоумышленникам из внутренней базы компании DropBox, которая хранилась в открытом виде. В период с 8 по 15 апреля 2014 года было зафиксировано массовое заражение троянцем – вымогателем файлов, пересылаемых через онлайн-диск Mail.Ru, незащищенный на тот момент от вредоносного ПО.

Эти и подобные инциденты дают основание для недоверия облачным услугам. Так, в ходе конференции «Саммит по информационной безопасности 2019» управляющий директор, начальник центра киберзащиты департамента безопасности ПАО «Сбербанк» Сергей Валуйских подчеркнул, что проблема доверия к поставщику облачных услуг по-прежнему стоит остро, в том числе потому что от него сложно добиться внятных ответов на многие вопросы. Обеспечение защиты в облачных средах требует серьезной смены подходов к ИБ в целом. Сами облачные ресурсы часто представляют собой черный ящик, в работе которого многие аспекты скрыты от потребителя. И при использовании таких сервисов если не исчезает, то серьезным образом размывается то, что принято называть корпоративным сетевым периметром.

Типичные примеры теневого ИТ
(% ответивших)

Макросы для офисных приложений	19
Несанкционированная установка ПО	17
Несанкционированное использование облачных сервисов	16
Несанкционированная доработка модулей ERP-систем	12
Несанкционированная доработка систем бизнес-аналитики	9
Несанкционированное приобретение аппаратных и программно-аппаратных комплексов	6
Неучтенное использование сервисов VoIP	5
Неучтенная ИТ-поддержка	5
Неучтенные ИТ-проекты	3
Использование собственных устройств	3

Источник: Palo Alto Network

Фото: СТАНДАРТ

Директор департамента информационной безопасности ООО «Оберон» Андрей Грузинов убежден, что само понятие периметра информационной безопасности устарело и использовать его в современных реалиях нецелесообразно

Фото: Check Point Software Technologies

Руководитель направления по защите от киберугроз Check Point Software Technologies в России и СНГ Алексей Белоглазов подчеркивает, что в основе облачной безопасности должна лежать модель взаимной ответственности поставщиков облачных услуг и их заказчиков

Не умер, но трансформировался

Разговоры о размывании традиционного корпоративного периметра идут уже более десяти лет. Первым шагом к этому стал переход от использования настольного корпоративного ПК к портативному. Компьютеры стали подключать к сети компании не только из офиса, но также из любой точки мира, при этом могли использоваться незащищенные Wi-Fi-сети – например, публичные. Положение усугубляется тем, что до сих пор сетевые соединения защищают нечасто. По данным исследования, проведенного ООО «Код безопасности» в марте 2019 года, VPN для удаленного подключения к корпоративной сети не используют треть российских пользователей.

Директор департамента информационной безопасности ООО «Оберон» Андрей Грузинов приводит такой пример: «Сотрудник компании утром работал из дома, а днем приехал в офис и работал внутри беспроводной сети компании. После обеда он пошел на встречу в ближайшее кафе и подключился к корпоративной сети через публичный Wi-Fi. Вечером – улетел в командировку и по пути в аэропорт работал через Wi-Fi в вагоне аэроэкспресса. В аэропорту он тоже подключился к корпоративной сети через местный Wi-Fi. Все это разные сети, с разными политиками безопасности, но одно оставалось неизменным – сотрудник всегда находился внутри сети своей компании».

Появление в корпоративной практике облачных сервисов еще больше размыло понимание сетевого периметра. Руководитель направления по развитию продукта АО «ИнфоВотч» (InfoWatch) Александр Коробко уверен, что традиционный подход к периметру теряет актуальность в условиях, когда бизнес арендует облачные сервисы, подключает к своим услугам новых контрагентов, открывает сотрудникам доступ к CRM-системам с личных устройств.

Андрей Грузинов еще более радикален в оценках: «Само понятие периметра информационной безопасности устарело и нецелесообразно использовать его в современных реалиях. Более того, мы не знаем, что же такое периметр информационной безопасности».

Руководитель направления по защите от киберугроз Check Point Software Technologies в России и СНГ Алексей Белоглазов считает, что говорить об исчезновении периметра преждевременно, – скорее, речь идет о его трансформации и усложнении. «Теперь мы говорим не только о внешнем и внутреннем периметрах, но также о периметрах на границе и внутри облачной инфраструктуры между различными сервисами и микросервисами. Актуальной становится задача микросегментации: между виртуальными машинами (IaaS), такими микросервисами, как контейнеры (PaaS), на уровне рабочих станций и мобильных устройств (SaaS)», – говорит он.

Заслуженный системный инженер Cisco Михаил Кадер уточняет, что само понятие «периметр» изменилось: «Это уже не граница сети, а защита обрабатываемых и хранимых данных вне зависимости от того, где они находятся. Обрабатываем данные на смартфоне – периметр пришел туда, обрабатываем данные в облаке – значит, здесь тоже периметр».

Выступая на «Саммите по информационной безопасности 2019», консультант по информационной безопасности Palo Alto Networks Денис Батранков обратил внимание на то, что в любом случае традиционные продукты, такие как межсетевые экраны, в сложной инфраструктуре работают все хуже: они не показывают реальное состояние сети и слишком часто требуют анализа событий в ручном режиме.

Следствием размывания сетевого периметра стало появление в 2013 году концепции программно определяемого периметра (Software Defined Perimeter, SDP). Она объединяла аутентификацию устройства, доступ на основе идентификации и динамически создаваемые возможности подключения. Менеджер проектов аналитического агентства Anti-Malware.Ru Олег Иванов уверен, что интеграция трех этих составляющих открывает новые возможности для защиты инфраструктуры, которые неспособны дать традиционные инструменты поддержки безопасности. «Предварительная аутентификация в сочетании с предварительной авторизацией позволяет создавать сети, скрытые от неизвестных хостов. При этом обеспечивается доступ для авторизованных пользователей. Ключевым аспектом SDP является то, что предварительная аутентификация и предварительная авторизация происходят до того, как будет инициировано соединение протокола управления передачей (TCP) между пользователем и защищенным приложением. Более того, пользователю разрешен доступ только к авторизованным приложениям. Это помогает устранить угрозу «бокового перемещения» от скомпрометированных устройств», – рассказал Олег Иванов.

Концепции SDP соответствуют программно-аппаратные комплексы сетевой безопасности большинства крупных поставщиков, включая Check Point, Cisco, Huawei, Palo Alto Networks, и этот перечень постоянно растет. Так, Михаил Кадер напоминает, что все современные инфраструктурные продукты и продукты информационной безопасности поддерживают доступ через программные интерфейсы (Application Programming Interface, API) – частные или организованные по принципу REST (Representational State Transfer). По словам заслуженного системного инженера Cisco, это дает возможность оперативно менять политики безопасности в рамках всей инфраструктуры: от периметра на мобильных устройствах до периметра внутри облачных сред.

Денис Батранков обращает внимание на важность глубокой идентификации трафика, особенно в нынешних условиях, когда более 80% всех данных, передаваемых через Интернет, зашифровано. По его мнению, идентификация помогает лучше контролировать пользователей и приложения, с которыми они работают, что в свою очередь

Фото: Palo Alto Networks

Консультант по информационной безопасности Palo Alto Networks Денис Батранков считает, что практика использования нескольких облаков продолжит расширяться, и будет крайне трудно добиться полной управляемости такой инфраструктуры без использования инструментов с функциональностью SDP

позволяет избежать перехвата учетных данных с применением фишинговых сценариев (когда пользователя заманивают на поддельную страничку идентификации), а также предотвращает попытки воспользоваться украденными логинами и паролями.

Александр Коробко тоже считает, что организациям не стоит концентрироваться только на традиционной концепции защиты сетевого периметра, а нужно применять и другие подходы к ИБ – например, обеспечивать защиту сред и устройств, проводить мониторинг бизнес-процессов, организовывать управление ИБ-решениями через единую консоль.

Теневое облако

Серьезной проблемой является то, что облачные сервисы используются неконтролируемо: об их подключении ИТ- и ИБ-подразделения не всегда ставятся в известность. По данным исследования Cisco, 98% облачных сервисов используется сотрудниками без ведома профильных подразделений. Часто бывает и так, что те или иные облачные услуги являются дополнением к используемому ПО. Например, младшие версии Microsoft Office, которые тесно интегрированы с облачным диском OneDrive. Так что облачные сервисы практически с самого начала своей истории прочно заняли место в том, что называется «теневые ИТ», которые являются одним из главных источников проблем и неприятностей, в том числе в сфере безопасности. По данным исследования Gartner, с теневыми ИТ связана треть успешных взломов.

При этом, как отметил генеральный директор и сооснователь ООО «МобилитиЛаб» Сергей Орлик, сотрудники со своих корпоративных рабочих мест, как правило, обращаются к тем облачным ресурсам, которыми они обычно пользуются, – к электронной почте и файлообменным сервисам. Причем эти сервисы могут использоваться в том числе в служебных целях. И соответственно, ни о каком соблюдении корпоративных политик безопасности при обращении к сервисам, предназначенным для индивидуальных пользователей, не может быть и речи.

Александр Коробко также предупреждает, что облака часто становятся инструментом в руках злонамеренных инсайдеров. «Часто ИТ- и ИБ-службы не осведомлены об использовании облаков и не знают точно, какой информацией обмениваются сотрудники с помощью этих сервисов. Чем больше таких сервисов используют сотрудники, тем выше риск утечки информации. Пользователь может отправить на личный аккаунт рабочие документы, чтобы поработать из дома, не задумываясь, например, о защищенности используемого облачного файлообменника или о том, что его аккаунт не защищен сильным паролем. Бывают ситуации, когда такие сервисы используются в схемах сговора как промежуточное звено за пределами контроля организации», – говорит представитель InfoWatch. По данным мониторинга утечек InfoWatch за 2018 год на web- и облачные среды пришлось 72,7% всех утечек информации из компаний и госучреждений.

Алексей Белоглазов обращает внимание еще на два очень серьезных риска: «Во-первых, переключаясь между корпоративными и личными сервисами в течение дня, пользователь перестает осознавать, где он ведет корпоративную беседу, и ему очень легко подсунуть фишинг-страницу. Поэтому, когда злоумышленники осознают, что корпоративная система серьезно защищена, они начинают атаковать пользователей через личную почту. Через этот канал они могут как установить зловреды, так и украсть учетную запись пользователя. Например, от лица администратора компании злоумышленники присылают форму для подтверждения учетной записи – и сотрудник вводит логин и пароль, которые крадет злоумышленник. Во-вторых, люди не задумываются над тем, что хранят конфиденциальные данные на внешних неуправляемых ресурсах – и в итоге никто не несет ответственность за их утечку, не контролирует защиту данных на этих сервисах со стороны компании. Например, сотрудник перенес контакты контрагентов в Google Docs, которым пользуется с ПК и смартфона на базе ОС Android. А потом – скачал скомпрометированную игру, из-за чего злоумышленник

Распределение утечек по каналам передачи данных (%)

Источник: InfoWatch

Фото: СТАНДАРТ

По словам заслуженного системного инженера Cisco Михаила Кадера, все современные инфраструктурные продукты и продукты информационной безопасности поддерживают доступ через API, что дает возможность оперативно менять политики безопасности всей инфраструктуры – от периметра на мобильных устройствах до периметра внутри облачных сред

может установить троянца и перехватить доступ к ресурсам Google – а следовательно, к личным данным в базе».

Впрочем, Михаил Кадер полагает, что не стоит драматизировать ситуацию: «Если люди соблюдают «цифровую гигиену» и им в этом помогают департаменты ИТ и ИБ (с помощью технических средств и обучения), то риски становятся управляемыми. Если кто-то решил украсть данные из компании, то он это сделает и без облачных сервисов. Более того, без облачных сервисов гораздо проще «не оставить следов». Это подтверждается и аналитиками, так, согласно результатам исследования Gartner от ноября прошлого года, причины 95% инцидентов безопасности, связанных с облаком, были вызваны проблемами внутри компаний – потребителей услуг.

Однако применение средств, поддерживающих концепцию SDP, купирует угрозу, исходящую из теневого облака. Подводя итоги успешных проектов на «Саммите по информационной безопасности 2019», Денис Батранков отметил, что системы с соответствующей функциональностью позволяют разделить облачные сервисы на три группы: разрешенные, допустимые с ограничениями и неразрешенные. «Причем системы сами выявляют сервисы, которые используются в компании, и оценивают уровень их опасности согласно тому, с какими узлами они «общаются». Среди неразрешенных сервисов, скорее всего, окажутся не только те, которые явно передают информацию на сторону, но и такие, чье назначение даже с натяжкой нельзя отнести к необходимым по работе, – например, онлайн-игры, онлайн-кинотеатры или радиостанции, которые распространены намного шире, чем принято считать», – отметил специалист Palo Alto Networks.

Александр Коробко, основываясь на опыте InfoWatch, полагает, что в обеспечении безопасности при работе с облачными сервисами хорошо помогают так называемые облачные брокеры – Cloud Access Security Broker (CASB). «Такой брокер может обеспечить контроль сразу нескольких десятков облачных сервисов, анализировать корреляцию событий и взаимодействовать с третьими системами – например, с DLP-системой, которая предотвращает утечки данных. У нас по такому принципу осуществлена интеграция InfoWatch Traffic Monitor с брокером от Microsoft для хранилищ Office 365», – рассказал он.

Управляемо – значит, безопасно

Даже если использование облачных сервисов санкционировано ИТ- и ИБ-службами, это не гарантирует защиты от возможных проблем. У этого есть целый ряд причин. Во-первых, поставщики облачных услуг часто арендуют мощности у сторонних компаний, далеко не всегда интересуясь подробностями их работы. Во-вторых, сами заказчики используют несколько облаков, и такая практика стремительно набирает популярность. Наконец, настройки облака во многих аспектах сложнее, чем настройки традиционной инфраструктуры. Все это порождает серьезные проблемы с управляемостью, а значит, и с безопасностью.

Сергей Валуйских отметил, что поставщики услуг скрывают, на чем базируется их инфраструктура и каким образом она защищается, что не способствует доверию и пониманию в отношениях с ними, особенно в такой зарегулированной области, как банковская.

Алексей Белоглазов обращает внимание на то, что поставщики услуг защищают только свою инфраструктуру, тогда как за сохранность данных отвечает сам заказчик: «Согласно отчету Check Point 2019 Security Report, 30% ИТ-специалистов возлагают ответственность за обеспечение безопасности на поставщиков облачных услуг. Однако провайдер не говорит о том, что он защищает сами данные, – эта ответственность ложится на плечи заказчиков. В основе облачной безопасности должна лежать модель взаимной ответственности, и граница этой ответственности зависит от самого облака». Однако заказчики об этом часто забывают, что создает проблемы. Представитель Check Point привел пример: «До недавнего времени хранилище S3 на Amazon формировалось по умолчанию доступным для чтения в Интернете. И если администратор не менял настройки по умолчанию и забывал включать шифрование этого хранилища, то любой желающий мог получить доступ к данным. В итоге 7% хранилищ на Amazon были по ошибке опубликованы в Интернете, а 35% оказались незашифрованными. Как итог – персональные и финансовые данные миллионов граждан утекли в Сеть».

Александр Коробко также указывает на то, что часто причиной утечек становится открытая консоль Kubernetes, через которую злоумышленники получают доступ к хранилищу в результате ошибок пользователей.

Вместе с тем, далеко не все согласны, что инфраструктура поставщика услуг представляет собой черный ящик. «Риски «неподконтрольности» инфраструктуры у облачных провайдеров не больше, а скорее даже меньше, чем у корпоративных ЦОДов, операторы которых часто вынуждены использовать самостоятельно написанные средства автоматизации различных задач», – полагает Михаил Кадер.

Однако важно уточнить, что многие провайдеры IaaS открыто публикуют описания решений и услуг на сайтах. «Правда, те из них, кто ориентирован на западный рынок, некоторые услуги считают «опциональными» и ограничиваются их декларированием, – отмечает Александр Коробко. – В России клиенты чаще проверяют заявления поставщиков, много внимания уделяя вопросам безопасности и требованиям регуляторов».

Начальник управления информационной безопасности ПАО «Северсталь» Сергей Гусев также подчеркнул важность использования единого интерфейса управления для нескольких сервисов, отсутствие которого серьезно повышает риски допустить критичные ошибки в их конфигурировании, чреватые разного рода инцидентами.

Денис Батранков отметил, что защита сервисов от одного поставщика не представляет серьезной проблемы. «Вместе с тем практика использования нескольких облаков широко распространена и будет расширяться, и добиться полной управляемости такой инфраструктуры без использования инструментов с функциональностью SDP крайне трудно, – считает консультант по информационной безопасности Palo Alto Networks. – Кроме того, современные системы позволяют обогащать данные, которые предоставляет поставщик услуг, – например, журналы событий».

Однако результаты тестирования новейших систем обеспечения безопасности показывают, что сервисы, на которых происходит обогащение данных, как правило, расположены за пределами России, что может доставить различные сложности и чревато множеством рисков. На данный момент единственное исключение представляет собой решение от Huawei.

Дата
Название
Место
Организаторы
Контакты

4-6 июня
ANGA COM 2019
Германия, Кельн
ANGA Services
Тел. +49 221 998 0810

4-6 июня
Datacloud Global
Монако, Монте-Карло
BroadGroup
Тел. +44 0 207 779 7366

6-8 июня
Петербургский международный экономический форум 2019
Россия, Санкт-Петербург
Росконгресс
Тел. +7 812 680 0000

10-11 июня
XI Международный ИТ-форум с участием стран БРИКС и ШОС
Россия, Ханты-Мансийск
Администрация Ханты-Мансийского автономного округа – Югры
Тел. +7 346 795 8045

10-14 июня
London Tech Week
Великобритания, Лондон
Informa Telecoms & Media
Тел. +44 0 207 017 5000

11-13 июня
5G World 2019
Великобритания, Лондон
KNect365
Тел. +44 0 203 377 3279

11-13 июня
Identity Week
Великобритания, Лондон
Terrapinn Holdings
Тел. +44 0 118 984 3209

14 июня
Бизнес-форум «Smart City & Region: Цифровые технологии на пути к «умной стране»
Россия, Сочи
ComNews
Тел.: +7 495 933 5483, +7 967 136 2260

17-19 июня
Internet of Things Conference 2019
Германия, Мюнхен
Software & Support Media Group
Тел. +49 069 630 0890

18-21 июня
IoT Week
Дания, Орхус
IoT Forum
info@iotforum.org0

19-20 июня
European Spectrum Management Conference
Бельгия, Брюссель
Forum Europe
Тел. +44 0 292 078 3021

20 июня
V Федеральный ИТ-форум электроэнергетической отрасли России – «Smart Electro: Цифровая трансформация электроэнергетического сектора»
Россия, Москва, отель «Хилтон Гарден Инн Москва Красносельская»
ComNews
Тел.: +7 495 933 5483, +7 967 136 2260

23-26 июня
International Telecoms Week
США, Антанта
Capacity Conferences
Тел. +44 0 207 779 8646

25-27 июня
CEBIT Russia 2019
Россия, Москва, технопарк «Сколково»
Технопарк «Сколково», Deutsche Messe
Тел. +7 495 956 0033

25-28 июня
Российский международный энергетический форум
Россия, Санкт-Петербург
ЭкспоФорум-Интернэшнл
Тел. +7 812 240 4040

25-30 июня
V Юбилейный международный военно-технический форум «Армия-2019»
Россия, Московская область, г. Кубинка, КВЦ «Патриот»
Министерство обороны РФ
Тел. +7 495 640 5500

26 июня
Конференция «Диверсификация предприятий оборонно-промышленного комплекса отрасли связи» в рамках форума «Армия-2019»
Россия, Московская область, г. Кубинка, КВЦ «Патриот»
Министерство обороны РФ, ComNews
Тел. +7 495 933 5483

27 июня
Конференция «Умные технологии» на службе Вооруженных Сил РФ» в рамках форума «Армия-2019»
Россия, Московская область, г. Кубинка, КВЦ «Патриот»
Министерство обороны РФ, ComNews
Тел. +7 495 933 5483

26-27 июня
VIII Среднерусский экономический форум. «Цифровой регион»
Россия, Курск
АК&М
Тел. +7 499 132 6130

26-28 июня
MWC Shanghai
Китай, Шанхай
Ассоциация GSM
Тел. +86 213 103 3860

План конференций

июнь – октябрь 2019

	Название	Дата	Место проведения
Smart City & Region Сочи	Бизнес-форум «Smart City & Region: Цифровые технологии на пути к «умной» стране» Сочи	14 июня	Отель Swissotel Resort Sochi Kamelia Сочи, Курортный пр., д. 89
SMART ELECTRO	IV Федеральный ИТ-форум энергетической отрасли России «Smart Electro: Цифровая трансформация энергетического сектора»	20 июня	Отель «Хилтон Гарден Инн Москва Красносельская», Москва, Верхняя Красносельская ул., д. 11а, стр. 4
ARMY 2019 Диверсификация предприятий оборонно-промышленного комплекса отрасли связи	Конференция « Диверсификация предприятий оборонно-промышленного комплекса отрасли связи»	26 июня	Конгрессно-выставочный центр «Патриот» Московская обл., г. Кубинка
ARMY 2019 «Умные технологии» на службе Вооруженных Сил Российской Федерации	Конференция «Умные технологии» на службе Вооруженных сил РФ»	27 июня	Конгрессно-выставочный центр «Патриот» Московская обл., г. Кубинка
	V Федеральный ИТ-форум нефтегазовой отрасли России «Smart Oil & Gas: Цифровая трансформация нефтегазовой индустрии»	12–13 сентября	Отель «Хилтон Санкт-Петербург Экспофорум», Санкт-Петербург, Петербургское шоссе, д. 62, стр. 1
Лучшие ИТ-проекты для нефтегазовой отрасли	Церемония награждения победителей XI конкурса «Лучшие ИТ-проекты для нефтегазовой отрасли»	12 сентября	Отель «Хилтон Санкт-Петербург Экспофорум», Санкт-Петербург, Петербургское шоссе, д. 62, стр. 1
Smart City & Region Севастополь	Бизнес-форум «Smart City & Region: Цифровые технологии на пути к «умной» стране» Севастополь	26 сентября	Технопарк «ИТ КРЫМ», Севастополь, ул. Руднева, д.41
SMART AGRO	Федеральный ИТ-форум агропромышленного комплекса России «Smart Agro: Цифровая трансформация в сельском хозяйстве»	9 октября	Отель «Хилтон Гарден Инн Москва Красносельская», Москва, Верхняя Красносельская ул., д. 11а, стр. 4

В плане возможны изменения и дополнения

стандарт

COMNEWS

Издание зарегистрировано
в Министерстве РФ по делам печати,
телерадиовещания и средств
массовых коммуникаций.
Свидетельство ПИ №77-26396
от 01 декабря 2006 г.
Учредитель и издатель
ООО «КомНьюс Груп»

РЕДАКЦИЯ
главный редактор Леонид Коник
редактор Ксения Прудникова
заместитель главного редактора
Алексей Ефименко
обозреватели
Игорь Агапов, Яков Шпунт
корректура Нина Донецких
дизайн и верстка Александр Шаров
фотограф Александр Фомкин
фото на обложку Dreamstime

РЕКЛАМА
Сергей Болдырев, Светлана Вахотина,
Ольга Вербицкая, Лилия Забирова,
Мария Шевченко

ИНФОСПОНСОРСТВО
Максут Жафяров

КАЛЕНДАРЬ ВЫСТАВОК
Ольга Егорова

РАСПРОСТРАНЕНИЕ
Татьяна Яцко

Отпечатано в типографии
«Премиум Пресс»,
Санкт-Петербург, ул. Оптиков, 4
Тираж 10 000 экземпляров

**107140, Москва, Верхняя
Красносельская ул., д. 2/1, стр. 1
Тел.: +7 495 933 5483, +7 495 933 5485
190013, Санкт-Петербург,
Московский пр., д. 22
Тел. +7 812 670 2030
info@comnews.ru**
Ваши замечания, пожелания,
идеи, пожалуйста, направляйте
по адресам редакции или
по нашему электронному адресу
info@comnews.ru
Электронная версия журнала:
www.comnews.ru

Подписка на журнал «Стандарт»

Через редакцию

Стоимость оформления подписки составляет 3630 рублей на полугодие, включая доставку по ЦФО.
Вы можете заказать любой номер журнала (при наличии остатка) с доставкой.
Стоимость одного экземпляра – 300 рублей.
Стоимость доставки по Москве и Санкт-Петербургу – 350 рублей.
Стоимость доставки в другие города можно уточнить по указанным телефонам.
Тел.: + 7 495 933 5483, + 7 495 933 5485
office@comnews.ru
Татьяна Яцко

На сайте www.comnews.ru/standart/subscription

Через партнеров группы компаний ComNews

Стоимость подписки в агентствах-партнерах можно уточнить по указанным телефонам

1. **Агентство «Роспечать»**
   На сайте www.rosp.ru/service/subscribe
2. **Объединенный каталог «Пресса России»**
   Подписной индекс 11015
   На сайте www.pressa-rf.ru
3. **Каталог «Информнаука» – подписка за рубежом**
   Тел. +7 495 787 3873
   На сайте www.informnauka.com
4. **Группа компаний «Урал-Пресс»**

Москва
Новодмитровская ул., 5а,
стр. 4, 1-й подъезд, 2-й этаж
Тел.: +7 495 961 2362, 789 8636/37
moscow@ural-press.ru

Санкт-Петербург
пр. Юрия Гагарина, 2а,
ДЦ «Гагаринский»
Тел. +7 812 677 3207
spb@ural-press.ru

Екатеринбург
ул. Мамина-Сибиряка, 130
Тел. +7 343 262 6543
info@ural-press.ru

Представительства за рубежом:

Казахстан
Петропавловск,
Интернациональная ул., д. 15, кв. 2
Тел. +7 715 252 5170
kazahstan@ural-press.ru
Семигулина Ольга

Германия
13581 Berlin,
Seeburger Strasse 87
Тел. +49 303 389 0115
frg@ural-press.ru
Waldemar Besler

Полный список представительств на сайте www.ural-press.ru/contact

5. **Интернет-магазин подписки на журналы MyMagazines.ru**
   Тел. +7 921 374 5706
   На сайте www.mymagazines.ru

Организаторы АТРП ВГТРК ТЕЛЕВИДЕНИЕ И РАДИО НАТ НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ ТЕЛЕРАДИОВЕЩАТЕЛЕЙ

При поддержке Минкомсвязь России

Профессиональный Всероссийский молодежный
научно-технический конкурс разработок в области
кинопроизводства, телерадиовещания и телекоммуникаций

ПЕРВЫЙ ШАГ

Финал
29-31 мая, Томск

#СДЕЛАЙ ПЕРВЫЙ ШАГ

konkurs@atrp.ru
www.atrp.tv

- **Разработки в области кинопроизводства, телерадиовещания и телекоммуникаций**
- **Студенты и аспиранты технических специальностей**
- **Денежные гранты, ценные призы, поездки на мировые выставки и конференции**
- **Авторитетнейшее жюри**

Информационные партнеры

МЕЖДУНАРОДНАЯ АССОЦИАЦИЯ СТУДЕНЧЕСКОГО ТЕЛЕВИДЕНИЯ МАСТ

ТКТ ТЕЛЕСПУТНИК BROADCASTING ТЕЛЕВИДЕНИЕ И РАДИОВЕЩАНИЕ ТЕЛЕСКОП

МЕДИА • СПУТНИК COMNEWS MediaVision

CommuniGate Pro

ПЛАТФОРМА ОБЪЕДИНЕННЫХ КОММУНИКАЦИЙ

17 000 ИНСТАЛЛЯЦИЙ

25 ЛЕТ НА РЫНКЕ

15 000 000 УЧЁТНЫХ ЗАПИСЕЙ

Электронная почта

Календари и планы

Мгновенные сообщения

Телефония

Хранилище документов

Контакт-центр

Единый программный продукт для организации всех типов связи современного бизнеса

Кросс-платформенное решение для любых ИТ-инфраструктур

Внесено в Единый реестр российских программ для ЭВМ и баз данных. Сертифицировано ФСТЭК

Годовая подписка

Стоимость 1000 рублей за 1 пользователя в год*

* телефония отдельно

Антивирус и антиспам плагины в комплекте

Участвуют компании с количеством пользователей ДО 200.

Срок проведения акции до 1 июля 2019 года.

Партнеры, реализующие решение CommuniGate Pro в специальной редакции SMB Connect:

softline® AXOFT MONT Group of companies

russia@communigate.com

www.communigate.com