

# The world of information technology

# Connect. WIT

мир информационных технологий

май-июнь 2017



Петр ЕФИМОВ,  
генеральный  
директор компании  
«Информзащита»:

«Решения  
по информационной  
безопасности  
становятся все более  
востребованными»

# ПЯТАЯ КОНФЕРЕНЦИЯ «СВЯЗЬ НА РУССКОМ СЕВЕРЕ» Москва, МТУСИ 5-6 СЕНТЯБРЯ 2017

Организатор: **Connect**  
ИТ-агентство



[www.свЯзьнаСевере.рф](http://www.свЯзьнаСевере.рф)



Тема очередного номера журнала – замещение импорта в сфере инфраструктурного программного обеспечения. Реестру российских программных продуктов больше года. Формальные критерии, по которым подтверждается происхождение продукта, служат необходимым условием включения в реестр. А достаточным условием является заключение Экспертного совета.

Реестр состоялся, но периодически попадает под огонь критики. В частности, эксперты обращают внимание на то, что большинство продуктов, включенных в список, можно использовать только на Windows и с базами данных SQL и Oracle. Насколько обоснована такая критика, рассуждают на страницах издания участники заочного круглого стола. Они же отмечают трудности, возникающие при миграции популярных в нашей стране бизнес-приложений на открытые операционные системы и СУБД.

Опыт преодоления таких проблем есть у специалистов в других странах. Например, во Франции госорганам запрещено использовать зарубежные ОС и СУБД, правительства ФРГ и Италии субсидируют миграцию ресурсов муниципальных органов власти на открытое ПО. О перспективах применения подобных механизмов у нас размышляют приглашенные эксперты.

О замещении импортного ПО в инженерных проектах авторы статей рассказывают на примере подготовки к замене иностранных продуктов, которые много лет применяются в России для проектирования воздушных судов и бортовой электроники. Что касается сегмента отечественных PLM-решений, то очевидна тенденция к консолидации локальных инструментов в определенных предметных областях в состав крупных программных комплексов.

По мере обновления нормативной базы в сфере ИТ рынок отечественного офисного программного обеспечения оживился. Заметную активность проявляют госструктуры, которым предстоит развивать ИТ-инфраструктуру на основе российских программных инструментов, на годы вперед закладывая технологическую платформу. Базовым элементом такой инфраструктуры является операционная система. Обзор предложений в сегменте отечественных ОС на базе ядра Linux сквозь призму ориентиров для выбора комплекса свободного ПО, включающего инструменты управления ИТ-инфраструктурой и офисные приложения, представлен в одном из материалов номера.

Кстати, на недавней IV конференции OS DAY обсуждались подходы к разработке отечественного ПО и операционных платформ. Выступающие отмечали, что прилагаемые в этом направлении усилия не должны приводить к снижению планки требований. Одна из опасностей кроется в том, что импортозамещение может содействовать продвижению на рынке компаний с невысокой культурой разработки. Качество ПО, по мнению участников отрасли, определяет уровень информационной безопасности.

В дни работы над этим выпуском журнала разыгралась история с WannaCry. По одной из версий, «червь» вырвался на просторы Сети по ошибке его создателей. Аргументы в пользу такого сценария привел эксперт «Лаборатории Касперского», он же обратил внимание на пикантность ситуации. Авторы «червя» не могут прислать ключ дешифровки своим жертвам, поскольку у них нет информации о том, какие ключи какой жертве соответствуют. Оказывается, и у разработчиков вирусов случаются проблемы – не всегда удается сдержать прорыв вредоносных, не готовых к распространению.

Хакерские атаки 2017 г. ударили по многим странам, добрались до компьютеров российских силовых ведомств и телеком-компаний, а сбои в компьютерных сетях (недавний случай с авиагаванью в Великобритании) в очередной раз продемонстрировали всему миру, что привычный ритм жизни зависит теперь и от надежности систем, гарантий информационной безопасности. Готовы ли российские разработчики ответить на такие вызовы времени? За ответом на этот вопрос редакция обратилась к Петру Ефимову, одному из основателей Группы компаний «Информзащита» и генеральному директору одноименного системного интегратора. Петр Валентинович поделился любопытным наблюдением: сейчас все меньше рассказывают о том, как далеко летают ракеты, и все больше о том, что происходит в цифровом поле. Специализация в сфере ИБ становится востребованной. Дополнительные аргументы на этот счет, в том числе в условиях замещения импортных программных продуктов, вы найдете и в других материалах выпуска. Внимательного и полезного вам чтения!

**С уважением,  
Светлана АРЯНИНА,  
Connect**



— ИНТЕРВЬЮ НОМЕРА —

- 4 **Петр ЕФИМОВ:** «Решения по информационной безопасности становятся все более востребованными»  
Интервью с основателем Группы компаний «Информзащита» и генеральным директором компании «Информзащита»

— ПАНОРАМА —

- 12 Создание и внедрение ИТЗ в жизненном цикле продукции ОПК  
Итоги Второй научно-практической конференции «Управление созданием научно-технического задела в жизненном цикле высокотехнологичной продукции – 2017»
- 18 **Александр КУЗЬМЕНКО:** «Код» решения проблем управления ЖЦ существует  
Интервью с генеральным директором компании «ЛМ Софт»
- 20 Наука безопасности операционных платформ  
Репортаж с IV научно-практической конференции OS DAY
- 22 На PHDays обсуждали проблему периметра безопасности  
Репортаж с седьмой PHDays – конференции и конкурса CTF для специалистов информационной безопасности
- 24 В витрине отрасли на выставке «Связь-2017»  
Итоги 29-й международной выставки информационных и коммуникационных технологий «Связь-2017»

- 28 Доступность финансовых услуг  
Репортаж с 21-го форума «Информационные технологии в финансовом секторе»

— ТЕМА НОМЕРА —

- 30 Больше, чем ОС  
Обзор рынка отечественных операционных систем  
**Алексей СМИРНОВ**, советник генерального директора, «Базальт СПО»
- 34 Российская отрасль СУБД продвигается на «слонах»  
По материалам компании Postgres Professional
- 40 О замещении иностранного ПО в инженерных проектах  
**Сергей АВТОМАНОВ**, ведущий инженер, ФГУП «ГосНИИАС»  
**Александр ПОПОВ**, ведущий инженер, ФГУП «ГосНИИАС»
- 44 К импортозамещению ERP крупные предприятия подходят особенно аккуратно  
**Алексей КАЗАРЕЗОВ**, директор ЦИТК «Парус»



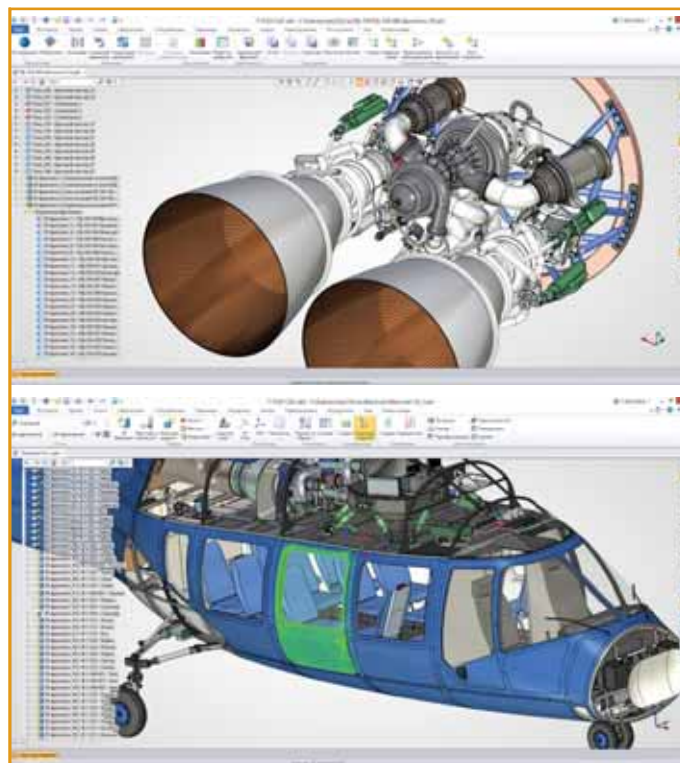
- 46 Круглый стол с экспертами  
Замещение импорта в сфере инфраструктурного ПО:  
риски, проблемы и алгоритмы решений

**— БИЗНЕС, ТЕХНОЛОГИИ, УПРАВЛЕНИЕ —**

- 54 PLM с прицелом на замещение импорта  
**Игорь КОЧАН**, директор по маркетингу,  
ЗАО «Топ Системы»
- 58 АСУПП: что первично?  
**Игорь РЕШЕТНИКОВ**, основатель и руководитель  
MES-центра, к. т. н.

**— ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ —**

- 62 Доверенные ПАПы  
**Валерий АНДРЕЕВ**, заместитель директора  
по науке и развитию,  
ЗАО ИВК, к. ф.-м. н.



- 66 Актуальные вопросы защиты  
государственных информационных систем  
в период перехода на импортозамещающие  
технологии  
**Сергей ОВЧИННИКОВ**, директор по маркетингу  
Центра защиты информации,  
ГК «Конфидент»
- 70 Импортозамещение ИТ- и ИБ-решений  
в ОПК  
**Андрей ПРОЗОРОВ**, руководитель  
экспертного направления, компания Solar Security

**— ИНФОКОММУНИКАЦИИ —**

- 74 Информационно-телекоммуникационные  
системы в глобализованном мире  
**Игорь ДУЛЬКЕЙТ**, к. т. н., ОмГТУ

**— СПУТНИКОВЫЕ ТЕХНОЛОГИИ —**

- 80 Спутниковая связь для Интернета вещей  
**Александр МИНОВ**, генеральный директор  
АО «Национальный исследовательский институт  
технологий и связи»  
**Александр БАБИН**, заместитель генерального  
директора АО «Национальный  
исследовательский институт технологий и связи»  
по работе с государственными органами,  
к. т. н.

- 86 НОВИНКИ РЫНКА ИКТ



# Петр ЕФИМОВ:

## «Решения по информационной безопасности становятся все более востребованными»

Хакерские атаки в мае 2017, ударившие по многим странам, а также затронувшие компьютеры российских силовых ведомств и телекоммуникационных компаний, еще раз напомнили миру, что информационная безопасность сегодня становится одним из важнейших факторов, обеспечивающих нормальную жизнь современного общества. Готовы ли российские разработчики ответить на вызовы времени? Как относятся к проблемам информационной безопасности российские компании? С этими и другими злободневными вопросами мы обратились к Петру Валентиновичу Ефимову, одному из основателей Группы компаний «Информзащита» и генеральному директору крупнейшего системного интегратора в сфере информационной безопасности компании «Информзащита».



– Петр Валентинович, расскажите об основных результатах и достижениях компании по итогам прошедшего года. Насколько удачным был для компании 2016 г.?

– Прежде чем переходить к нашим результатам, я сразу бы хотел уточнить, что речь пойдет о достижениях всего холдинга, а не только системного интегратора «Информзащита». Если в 2015 г. у нас был рост совокупной выручки на 28% (в сравнении с 2014 г.), то в прошедшем 2016 г. нам удалось вырасти на 31%, что составляет 6867 млн руб.

Понятно, что результаты нашей работы измеряются не только деньгами – нас больше интересует качественная оценка. Разумеется, нам всегда хочется больших достижений – видимо, в этом и заключается философия развития бизнеса, однако результаты прошедшего года нас вполне удовлетворяют. Как команда профессионалов, мы ставили перед собой планы по повышению качества услуг в области защиты информации, развитию наших компетенций и экспертизы. В 2016 г. нам удалось достичь поставленных целей, в этом году мы продолжим развитие. Также хорошие показатели были получены и нашим производителем – я говорю сейчас о разработчике программных

и аппаратных средств компании «Код безопасности».

**– Какие из направлений вы развивали активнее всего в 2016 г.? И на какие направления будете делать упор в будущем?**

– 22 года назад, когда мы начинали работать, мир был гораздо проще. За прошедшие два десятилетия произошел головокружительный скачок в области «диджитализации» жизни. Инновации воплотились в реальность, и все сферы жизни получили цифровое сопровождение. Поэтому, когда мы сегодня говорим об информационной безопасности, следует понимать, что она теперь занимает в нашей жизни если не доминирующее положение, то определенно одно из важнейших. Угрозы, связанные с информационной безопасностью, стали гораздо ощутимее, реальнее. Честно говоря, 20 лет тому назад мы порой скептически относились к тем угрозам, которые могли возникнуть в цифровом мире, но недавний пример хакерской атаки в мае этого года лишний раз показывает, к каким последствиям приводят вирусные эпидемии.

Вместе с удобством, мобильностью и платежами в один клик, которые подарил нам скачок в развитии технологий, человечество получило угрозу личной информационной безопасности: сегодня уже никто не может сказать, что его это не касается.

Современные атаки, имея целью финансовое обогащение, получение преимуществ в конкурентной борьбе или решение политических задач, становятся все более массовыми, вследствие этого затрагивают не только предполагаемую жертву атаки, но и критически важные области простых людей. Так, в Великобритании атака парализовала больничную сеть, и пациенты не смогли вовремя получить медицинскую помощь. Такие же примеры можно привести с транспортом, мобильными операторами и многими другими областями жизни, когда косвенной жертвой становится обыватель.

Направленность последних атак показывает, что под угрозой находятся и такие системы жизнеобеспечения, как энергетика, силовые структуры. Например, в России многие люди в регионах не смогли вовремя получить водительские удостоверения из-за сбоя в работе системы сервисов ГИБДД. Страшно подумать, что могло бы произойти, если бы атака затронула критически важные объекты инфраструктуры.

Именно поэтому в «Информзащите» создан Центр промышленной безопасности, который реализует сложные проекты по защите АСУТП и критической инфраструктуры крупных производственных компаний. Кроме того, Центр по противодействию мошенничеству не оставляет без внимания направление, связанное с защитой банковской деятельности, выполняет проекты по созданию и внедрению антифрод-систем, защищает от целенаправленных атак.

Информационные технологии несколько смещаются в сторону централизации ресурсов: облачные вычисления, анализ больших данных, повсеместное использование мобильных устройств. На мобильных устройствах размыта грань между персональной и служебной информацией, что порождает дополнительные проблемы для обеспечения корпоративной безопасности. Эти явления породили спрос на новые решения в области информационной защиты.

По всем этим ключевым направлениям мы ведем работу как интегратор – стараемся предлагать заказчикам оптимальные и лучшие на рынке решения.

Помимо этого явно обозначился спрос на аутсорсинг в ИБ. Если раньше заказчик хотел владеть продуктом, то сегодня хочет получить профессиональную услугу. Этот выбор объясняется просто: услуга позволяет снижать операционные затраты на поддержку решения и содержание дорогостоящего персонала в штате и, главное, избавляет от капитальных затрат на закупку оборудования и ПО.

«Информзащита» одной из первых создала Security Operation

Center (SOC) – эта история началась больше 10 лет назад. И, кстати, на тот момент наш заказчик еще не был готов к такой услуге – люди не соглашались отдавать на аутсорсинг или переводить в модель сервисного обслуживания безопасность. А сегодня ментальность немного поменялась: у нас все больше заказчиков, которые готовы передать управление информационной безопасностью в «чужие руки». Понятно, что это не просто чужие руки, а руки профессионалов, и безопасность компании передается под определенные SLA, под четко прописанные обязательства.

Естественно, что на данном этапе развития сервисная модель пока не может вытеснить классическую, но ее доля будет становиться больше с каждым годом.

Возвращаясь к началу нашего разговора, отмечу следующее: в апреле, сразу же после публикации на WikiLeaks очередной порции «разоблачений» (утечки из наработок АНБ и ЦРУ), мы разослали своим заказчикам информационную справку, дали им точные рекомендации, что необходимо в оперативном порядке проверить в ИТ-инфраструктуре, какие коррективы внести. У нас на обслуживании находится целый ряд систем, среди которых есть и критически важные, которые благополучно пережили майские атаки. Если бы с ними что-то случилось, это бы сразу заметила вся страна.

**– Каков отраслевой состав клиентов «Информзащиты»? В чем специфика их требований на текущий момент?**

– Если говорить об отраслевом составе, то он у нас настолько широкий, что мне легче будет пойти от обратного и сказать, кто нами еще не охвачен в должной степени. В числе наших заказчиков слабо представлен сектор SMB – малые и средние предприятия. Их бизнес не регламентируется законодательно так подробно, как деятельность государственных структур или компаний финансовой отрасли. Поэтому вопрос важности

информационной безопасности в этом случае должен быть самостоятельно осознан в первую очередь владельцами.

Государственные учреждения выполняют все требования регуляторов (ФСТЭК, ФСБ), поэтому уровень их защищенности априори высок, а вот в сфере частного бизнеса ничто не заставит собственника капитала потратить деньги, если у него не будет четкого осознания необходимости поддержки должной степени информационной безопасности собственного бизнеса.

И такое осознание рисков в сфере малого бизнеса пока не наступило. Конечно, некоторые более продвинутые бизнесмены понимают необходимость обеспечения ИБ: они понимают, что могут потерять и какую цену следует заплатить для нейтрализации риска. Другие же считают, что терять им нечего, что цифровой мир не несет им большой угрозы. Но последние события говорят об обратном.

Если же вернуться к вопросу об отраслевом составе, то исторически мы работаем с государственными структурами, с силовыми ведомствами. На втором месте по объему продаж и количеству проектов находится финансовый сектор. Сразу замечу, что специфика предоставления услуг для банков и для предприятий государственного сектора различна.

С банками мы ведем несколько интересных крупных проектов, связанных с противодействием мошенничеству – фрод операционный и карточный. А также предлагаем решения для борьбы с фродом в энергетике и нефтяной отрасли. Там, где есть соприкосновение с автоматизированными системами, где возможно искажение учета, изменение показаний датчиков и другие злоупотребления, там появляется поле для фрода и соответственно для нашей деятельности по предотвращению этих угроз.

Есть у нас клиенты в телекоммуникационном секторе, в атомной энергетике, транспорте, оптовой и розничной продаже, страховании, промышленности и т. д.

Если 10–15 лет назад информационная безопасность финансировалась по остаточному принципу, примерно как маркетинг и реклама, то сейчас без раздела ИБ ни один ИТ-проект просто не рассматривается.

**– Как импортозамещение вписывается в рыночную стратегию вашей компании?**

– На мой взгляд, тема импортозамещения возникла в России слишком поздно. Эти вопросы мы поднимали намного раньше, до всех событий последних лет, связанных с западными санкциями и обострением международной обстановки. Уже пятнадцать лет назад было понятно, что государство должно помогать своим российским разработчикам развивать продукты и решения, помогать находить рынок сбыта как внутри страны, так и за ее пределами. Как, например, в США и Европе. Во-первых, они жестко защищают свои рынки. Во-вторых, ИБ – это очень чувствительная для государства тема. Так что пускать «чужого» производителя и, что не менее важно, исполнителя работ по информационной безопасности на свои рынки никто не позволяет.

А в России в этом чувствительном секторе могли работать любые зарубежные компании, и долгое время никто не защищал от них свой рынок. В условиях отсутствия предпочтений от государства нашим производителям ПО было очень трудно конкурировать со сложившимися западными вендорами и показывать хорошие результаты.

Конечно, хорошо, что у нас возникли такие компании, как «Лаборатория Касперского», хорошо, что «Информзащита» в сложные годы смогла выстоять. Однако подобных компаний в России не так много. Поэтому политика импортозамещения – это очень правильный шаг со стороны государства. В результате, например, объем выручки нашего разработчика программных и аппаратных средств «Кода безопасности» в прошлом году вырос на 70% – это большая цифра.

И наши отечественные решения заказчики сейчас выбирают не по принципу «на безрыбье и рак рыба» – нет, продукты российских компаний становятся конкурентоспособными и востребованными.

Понятно, что такие вопросы, как импортозамещение «железа» и ПО, не могут решаться моментально. Вообще, создание хорошего продукта требует длительного цикла – от одного года, когда уже имеются хорошие наработки, и до трех-пяти лет, когда работа ведется с нуля. Чтобы бизнес начал инвестировать в разработку отечественных продуктов, он должен быть уверен в том, что они будут востребованными на рынке сегодня и завтра – это и должна гарантировать политика импортозамещения.

**– Каких российских продуктов вам не хватает для полного отказа от иностранных решений? Какова доля иностранных продуктов в ваших проектах сейчас?**

– Иностранные решения присутствуют сегодня в нашей продуктовой линейке. Здесь необходимо понимать, что мы, с одной стороны, должны предлагать своему заказчику сбалансированное, качественное решение, которое подходит конкретно ему. С другой стороны, мы живем в правовом поле и должны учитывать все те ограничения, которые возникли на сегодняшний день. Импортозамещение совсем не означает запрета всех импортных продуктов. Да, по тем классам продуктов, которые есть у российских разработчиков и которые достигли зрелости, мы должны ориентироваться на отечественные решения. Для этого, собственно говоря, и был создан Реестр отечественного программного обеспечения в Минкомсвязи.

Естественно, что доля импортных решений в нашей продуктовой линейке в настоящее время постепенно сокращается. Кстати, лакмусовой бумажкой для регистрации успехов политики импортозамещения может выступать наш Учебный центр, сосредоточенный только на курсах, связанных



с информационной безопасностью. В прошлом году объем курсов по решениям российских вендоров вырос на 40%. Как вы понимаете, обучение – это далеко не перво-степенная статья расходов в любой компании. Если происходит сокращение бюджета, то начинают всегда подрезать рекламу, маркетинг и обучение. Соответственно, наши заказчики готовы сейчас тратить деньги на обучение только по тем продуктам, которые они используют на практике, а это, как выясняется, российские решения.

Если же говорить о том, продуктов какого класса нам не хватает, то я бы указал на решения по выявлению мошенничества. Недостает нам также решений по анализу безопасности конфигурации сетевой инфраструктуры, управлению безопасностью мобильных устройств. Хотя, если быть точным, то по мобильным устройствам есть неплохие решения у российских разработчиков. В частности, у нашего производителя «Кода безопасности» есть ряд наработок в области MDM (Mobile Device Management).

Также сегодня не хватает инструментов, которые могли бы обеспечивать защиту информации в сфере Big Data. Работа с неструктурированными данными предполагает получение некоего итогового анализа – при этом мы сталкиваемся со следующей ситуацией. Сами по себе данные, как правило, не являются секретными – они обычно берутся из открытых источников, а вот те выводы, та аналитика, которую вы получаете на основе больших данных, могут таить в себе серьезные угрозы при открытии их в публичном пространстве. Этот непростой вопрос сейчас поднимают некоторые ИТ-компании, но пока что я не встречал ни одного законченного решения, позволяющего решить эту проблему.

Да и в сфере облачных технологий на сегодня закрыты далеко не все вопросы, связанные с безопасностью данных клиентов.

Еще одна новая проблемная область – это Интернет вещей, который развивается очень быстро



и уже сегодня стал в России вполне осязаемой вещью. А вот когда по нашим дорогам поедут беспилотные автомобили, проблемы безопасности станут критически важными. Понятно, что в этой сфере вопросов пока больше, чем ответов.

По другим категориям российские продукты представлены

достаточно широко, и здесь уже на первый план выходят задачи заказчика, особенности его инфраструктуры. Если смотреть продажи «Информзащиты» за прошлый год, то объем продуктов отечественных вендоров составил около 70% в сравнении с решениями зарубежных вендоров.



– В вашей группе компаний есть собственный производитель «Код безопасности». Как часто вы используете его продукты в своих проектах? В каком направлении вам хотелось бы совершенствовать продуктовую линейку этого производителя?

– В проектах наших заказчиков используем продукты «Код безопасности» достаточно часто и вовсе не в силу каких-либо табу на применение решений от сторонних производителей. Более того, бывают ситуации, когда мы используем в своих проектах продукты его прямых конкурентов.

Но, разумеется, во всех тех случаях, когда продукты «Код безопасности» применимы, мы предпочитаем продукцию своего производителя.

Понимаете, продукция «Код безопасности» закрывает много проблем – это очень удобно, когда от одного вендора вы получаете защиту каналов, систему обнаружения вторжения, межсетевые экраны (если говорить о сетевых продуктах). Далее, «Код безопасности» предоставляет целый набор продуктов класса Endpoint security, которые позволяют защищать конечные устройства (рабочие станции и др.), причем делать это полноценно и всесторонне. Есть, например, такой продукт, как Secret Net (Secret Net Studio 8.1), который существует как торговая марка уже 24 года, и все эти годы указанное решение постоянно развивается.

Также в «Коде безопасности» разрабатывается и к настоящему времени находится уже в хорошем рабочем состоянии новое решение для защиты мобильных устройств. И все эти решения интегрируются в единую консоль, так что для администратора информационной безопасности частной компании или государственной организации создаются комфортные условия: он работает с набором продуктов от одного вендора, управляет ими через единую консоль, оперирует одними и теми же терминами.

«Код безопасности» также проводит и уникальные разработки – они, конечно же, менее масштабны по применению. Речь идет о работах, связанных с применением электронной цифровой подписи. В больших системах, например финансовых, существует необходимость многочисленных проверок электронной цифровой подписи, а эта процедура требует значительной вычислительной мощности, потому на большом объеме транзакций необходимы специализированные движки, которые позволяют быстро и эффективно решать узкий спектр задач.

**– В составе холдинга «Информзащита» есть Учебный центр. Насколько его стратегия поменялась в связи с импорто-замещением? Увеличилась ли потребность у ваших клиентов в подготовке кадров для обслуживания российских продуктов? Появились ли в Учебном центре новые курсы в связи с развитием технологий и отрасли? Какие?**

– Хочу сразу же подчеркнуть, что наш Учебный центр целиком и полностью существует на рыночных принципах – он работает на спрос. Сам Учебный центр формировать этот спрос не может – он лишь откликается на запросы клиентов. Чтобы заказчик захотел произвести обучение кадров по какому-то курсу, у него, как минимум, должна появиться в компании соответствующая информационная система, должны быть ответственные за эксплуатацию системы – только тогда может родиться потребность в повышении квалификации кадров.

Да, у нас есть и набор авторских курсов, которые позиционируются как некое расширение кругозора специалиста ИБ, однако в основном Учебный центр идет в кильватере спроса. Продукты в сфере ИБ становятся с каждым годом все сложнее, так что эксплуатировать их по документации, как это делалось раньше, теперь попросту невозможно – нужно профессиональное обучение работе с конкретными продуктами, что и делает наш центр.

**– Насколько влияют на ситуацию с квалифицированными кадрами новые требования по подготовке специалистов в сфере информационной безопасности?**

– Если посмотреть на то, что было 15 лет назад, то тогда кафедры по ИБ в России можно было пересчитать по пальцам. Первая кафедра, с которой мы сотрудничали и которой в свое время помогали, появилась в МИФИ. Вторая кафедра, которую мы обеспечивали тогда методическими материалами, открылась

в РГГУ. Естественно, была своя кафедра и в МГТУ им. Н.Э. Баумана – мы помогли им средствами информзащиты.

Сейчас ситуация изменилась коренным образом: вузов, которые готовят специалистов по профилю «защита информации», стало гораздо больше. И я надеюсь, что со временем у них обучение и по качественному показателю станет приемлемым. Причем уже сегодня имеется достаточное количество учебных заведений, которые выпускают хорошо подготовленных специалистов. Естественно, мы продолжаем тесно сотрудничать с ведущими вузами.

**– Какова стратегия вашей компании в области защиты промышленных систем и объектов критической инфраструктуры?**

– Следует отметить, что сама тематика информационной безопасности промышленных систем появилась сравнительно недавно, и мы здесь были одними из первых. Офисные системы построены по одним и тем же принципам, они работают на единых протоколах, используют одни и те же операционные системы, одним словом, сделаны «по шаблону». Грубо говоря, при различных конфигурациях они сложены из одних и тех же кубиков.

Совсем другое дело – АСУТП. В них используются другие протоколы, причем по большей части эти протоколы являются проприетарными, и все промышленные системы очень сильно отличаются друг от друга. Например, если вы посмотрите на структуру АСУТП в машиностроении и энергетике, то увидите, что это просто разные системы. Единственное, что их объединяет – это само название АСУТП.

Вопросы безопасности промышленных систем мы начали поднимать на высоком уровне уже давно. Удалось достичь создания неких рабочих групп и комиссий по выработке специализированных требований, в которых эксперты «Информзащиты» принимают самое активное участие. Мы убеждены в том, что все должно

начинаться с нормативной базы, чтобы предупредить вкусовщину и разброд мнений.

Что же касается работы с нашими конкретными заказчиками, то здесь «Информзащита» исповедует исключительно индивидуальный подход к каждой промышленной системе.

Сейчас в этой области (АСУТП) существует острая нехватка высококвалифицированных кадров, поэтому нам пришлось создать некий симбиоз тех, кто хорошо знает саму АСУТП, и тех, кто знает сферу безопасности, – только вместе эти специалисты могут решать проблемы.

Сложнее всего тиражировать компетенции специалистов – над этой непростой проблемой сейчас и работаем.

**– Что «Информзащита» предлагает промышленности для защиты своей информации и инфраструктуры?**

– Сегодня именно в этой области чувствуется нехватка продуктов и решений высокого уровня, причем я говорю не только о нехватке отечественных продуктов – импортные решения тоже далеки от того, что заказчик хотел бы получить. Как я уже отметил ранее, до недавнего времени не существовало даже самого класса таких продуктов – для защиты АСУТП. Второй момент: все подобные решения не являются типовыми – это означает «индивидуальный пошив» для каждого заказчика, что всегда оказывается дороже стандартных решений.

Как я уже говорил, в рамках нашей компании выделено подразделение «Центр промышленной безопасности». До этого команда существовала в рамках отдела, нарабатывавшего в течение нескольких лет методики, проводила исследовательскую деятельность.

Большая сложность здесь заключается в том, что, когда имеешь дело с промышленными объектами, невозможно смоделировать систему заказчика на стендах. Например, сейчас в Сервисном центре «Информзащиты» для стандартизированных офисных систем



развернуто множество сервисных стендов и тестовых зон. Здесь можно смоделировать практически любую ситуацию и отработать план действий, схему реагирования на инцидент. А когда дело касается АСУТП, то смоделировать какую-то ситуацию невозможно как по финансовым соображениям, так и по необходимой инфраструктуре. То есть большинство проектов по защите промышленных систем могут выполняться только на территории заказчика.

Сейчас Центр промышленной безопасности «Информзащиты» имеет в своем составе экспертов с уникальными компетенциями в области информационной и промышленной безопасности, а также с опытом реализации сложных проектов по защите АСУТП.

У нас есть методики, опыт и отличная команда.

**– Насколько текущая ситуация на рынках – российском и международном – является благоприятной для вашего бизнеса?**

– Только сегодня я обсуждал с коллегами последнюю вирусную атаку. Может быть, это прозвучит не совсем этично, но я приведу такое сравнение. Когда идет эпидемия какой-то болезни, то у врачей появляется больше работы. Из этой аналогии следует, что нашей компании будет чем заняться.

Но давайте посмотрим на эту ситуацию немного шире. Международная обстановка сегодня, скажем так, беспокойная. Постоянно одна страна обвиняет другую в хакерских атаках на объекты

своей ИТ-инфраструктуры. Надо быть очень наивным, чтобы полагать, что наши объекты однажды не окажутся под ударом со стороны зарубежных хакеров. Да, мир стал жестче.

Обратите внимание, нам все меньше рассказывают о том, как далеко летают ракеты, и все больше о том, что происходит в информационном (цифровом) поле. Исходя из этого наша специализация становится все более востребованной, как и наши продукты. Угрозы выросли, выросли и риски, и с этой ситуацией приходится разбираться.

А в связи с дальнейшим развитием информационных технологий проблем с безопасностью ИТ-систем будет становиться только больше. ■

## «Галактика» адаптировала веб-аналитику Yandex для промышленных задач

Корпорация «Галактика» оптимизировала работу с «Яндекс.Метрика» для своих клиентов. Специалисты нашли различные возможности использования технологии веб-аналитики ClickHouse (Yandex) для анализа экономической деятельности предприятий. Технология сможет применяться как в системах планирования ресурсов предприятия класса ERP (Enterprise Resource Planning), так и в системах бизнес-анализа и поддержки принятия решений класса BI (Business Intelligence). ClickHouse – это система управления базами данных, которая изначально разрабатывалась для веб-аналитики «Яндекс.Метрика». ClickHouse позволяет обрабатывать огромные объемы данных (свыше двух терабайт в секунду), сохраняя отказоустойчивость, и делает это гораздо быстрее других решений, представленных на мировом рынке. Чтобы выиграть для пользователей бизнес-приложений время, корпорация «Галактика» оптимизировала технологию Yandex. Для ее оценки специалисты использовали 13 млн собственных бухгалтерских проводок и рассчитали средствами ClickHouse оборот по счетам и поток денежных средств. Результат оказался убедительным. Если в традиционной учетной системе аналогичные задачи

решаются за минуты, то в макете с использованием ClickHouse – за секунды. Решение позволяет бизнес-пользователю работать с отчетами в интерактивном режиме. Например, быстро переключаться с просмотра остатков средств на начало месяца к анализу оборота в разрезе счетов-субсчетов и т. д. За короткий сеанс работы пользователь может просчитать несколько вариантов управленческого решения и выбрать оптимальный. «Ключевой ресурс бизнеса сегодня – время. Способность компании к быстрым решениям и действиям позволяет увеличивать ее прибыль. Мы работаем над оптимизацией программного кода собственных разработок и ищем наиболее быстрые и эффективные технологии сторонних компаний, чтобы сэкономить время наших пользователей. Оптимизация системы управления базами данных ClickHouse, на наш взгляд, достигла этой цели», – прокомментировал член правления корпорации «Галактика» Сергей Петров. Заинтересованные пользователи ERP и BI-решений могут поработать с данными в тестовом макете «Галактики» и убедиться, насколько быстро справляется ClickHouse с типичными бизнес-задачами.

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

## Китайское рекламное агентство распространяет зловред

Команда Threat Intelligence компании Check Point Software Technologies обнаружила чрезвычайно активную китайскую вредоносную кампанию, от которой пострадали уже более 250 млн компьютеров по всему миру. В каждой четвертой российской компании заражен хотя бы один компьютер. Распространяемый зловред Fireball поражает браузеры, превращая их в зомби. У Fireball две основные функции: одна заключается в способности запускать любой код и скачивать любые файлы на компьютер жертвы, а другая позволяет управлять веб-трафиком пользователя, чтобы генерировать прибыль от рекламы. В настоящее время Fireball устанавливает плагины и дополнительные конфигурации для увеличения рекламного трафика, однако он может легко превратиться в распространителя любого другого зловредного ПО. Кампанией управляет крупнейшее маркетинговое агентство Rafotech, расположенное в Пекине. Rafotech использует Fireball, чтобы управлять браузерами жертв и менять поисковые системы и стартовые страницы, установленные по умолчанию, на фейковые поисковики, которые просто перенаправляют запросы на yahoo.com или Google.com. Поддельные поисковики способны собирать персональную информацию пользователей. Fireball также может шпионить за жертвами, доставлять любые зловреды и запускать

любой вредоносный код на инфицированных машинах. Fireball попадает на компьютер жертвы обычно в связке с другим ПО, которое скачивает пользователь. По данным аналитиков Check Point, инфицировано более 250 млн компьютеров по всему миру. По данным Check Point, процент заражения корпоративных сетей еще выше: около 20% от общего числа всех корпоративных сетей в мире. Другим показателем высокой степени распространения является популярность поддельных поисковых систем Rafotech. Согласно аналитической системе Alexa, 14 из этих поддельных поисковых систем входят в число 10 000 наиболее популярных веб-сайтов, причем некоторые из них иногда попадают и в 1000 лучших. С технической точки зрения Fireball демонстрирует высокую степень мастерства его создателей: он способен избегать обнаружения, содержит многоуровневую структуру и гибкий C&C и в целом ничем не уступает другим успешным вредоносным программам. Rafotech не признается в распространении поддельных поисковых систем, однако на своем сайте объявляет себя успешным маркетинговым агентством, охватывающим 300 млн пользователей по всему миру, что примерно совпадает с данными о количестве зараженных машин.

<http://www.checkpoint.com>

# Создание и внедрение НТЗ в жизненном цикле продукции ОПК

26 апреля 2017 г. в Москве прошла Вторая научно-практическая конференция «Управление созданием научно-технического задела в жизненном цикле высокотехнологичной продукции – 2017». Организаторами мероприятия выступили Военно-промышленная комиссия РФ, НИЦ «Институт имени Н.Е. Жуковского» и Институт проблем управления имени В.А. Трапезникова РАН. Партнерами конференции стали компании «ЛМ Софт», «Сименс» и «КАДФЕМ Си-Ай-Эс».

## Переход к модели «квалифицированного заказчика»

Конференцию открыл **Андрей Дутов, генеральный директор ФГБУ «НИЦ «Институт имени Н.Е. Жуковского»**. В своем вступительном слове он обрисовал общее состояние дел в области управления жизненным циклом технологий и продукции ОПК и отметил, что Центр, работая в рамках реализации указа Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации», идет по пути создания **модели «квалифицированного заказчика»**, который будет не только распределять бюджетные средства, но и иметь необходимые инструменты и ресурсы как для формирования детальных технических заданий, так и для квалифицированной приемки работ.

Затем в докладе «Методологические основы управления созданием опережающего научно-технического задела в жизненном цикле высокотехнологичной продукции» А. Дутов обозначил проблемы разработки технологий и продуктов в наукоемкой промышленности, в числе которых слабое целеполагание при формировании НТЗ, оторванность проводимых исследований

от потребностей производителей, недостаточная координация планов развития технологий, отсутствие критериев оценки результативности исследований, низкий уровень зрелости разрабатываемых технологий. Решить указанные проблемы призваны системы прогнозирования и стратегического планирования исследований и разработок, оценки их результативности, а также системы трансфера технологий, научно-технического сопровождения и системная интеграция технологий при реализации комплексных научно-технологических проектов.

Далее, конкретизируя механизм функционирования системы прогнозирования и стратегического планирования исследований и разработок, А. Дутов показал взаимодействие формирования требований (форсайт «спроса») на перспективные технологии с оценкой их возможностей (форсайт «предложения»), а также обозначил место разрабатываемых методик в стратегическом и тактическом контурах управления созданием НТЗ. Особое внимание он уделил межотраслевой интеграции как ключевому фактору создания прорывных технологий, отметив,



в частности, синергетический эффект прироста знаний и возможность снизить издержки за счет **увеличения серийности** производства наукоемкой продукции (сегодня для России запуск самолета в серию оказывается важнее рождения нового проекта), удешевления сертификации и унификации экспериментальной базы.

Выделяя направления исследований и разработок, в которых возможна межотраслевая интеграция, докладчик указал на новые виды источников энергии, средств ее хранения и преобразования на борту, новые конструкционные материалы, конструкции и производственные технологии, а также на методы и средства автоматизации управления движущимися объектами и сложными системами, в том числе основанные на принципах искусственного интеллекта, и новые методы математического моделирования, расчетов и проектирования сложных систем.

А. Дутов также говорил о необходимости разрабатывать прорывные технологии для обеспечения конкурентоспособной авиационной техники, создавать образцы, которые будут принципиально лучше существующих. По его словам, в авиационной области технологический прорыв



**Олег БОЧКАРЕВ,**  
заместитель председателя коллегии  
ВПК РФ

может быть связан с появлением полностью электрического самолета, а задачи, которые будут решаться в интересах авиастроения, актуальны и для железнодорожного транспорта, судостроения, других отраслей. При этом к ожидаемой в 2025–2030 гг. технологической революции готовиться нужно уже сегодня.

Министерство обороны РФ на конференции представлял полковник **Сергей Панков, начальник Управления перспективных межвидовых исследований и специальных**



**Андрей ДУТОВ,**  
генеральный директор НИЦ  
«Институт имени Н.Е. Жуковского»

**проектов.** Свой доклад он посвятил необходимости создавать опережающий научно-технический задел для разработки новых образцов ВВСТ как основы эффективного управления их жизненным циклом. В качестве справедливости настоящего тезиса он привел данные из зарубежной практики: открытие опытно-конструкторских работ (программ приобретения) по разработке высокотехнологичных образцов ВВСТ с незрелым научно-техническим заделом приводит к увеличению по сравнению с начальной оценкой сроков их создания в среднем в 1,9 раза, повышению стоимости разработки в среднем на 40%, а стоимости закупки финальных образцов – на 20%. Подтверждение этому – американский истребитель пятого поколения F-35 Lightning II, разработка которого началась еще в конце 1980-х гг., а окончательная стоимость, по оценкам некоторых экспертов, составляет 1 трлн долларов.

Рассматривая утвержденную министром обороны РФ «Концепцию создания НТЗ для перспективных видов вооружения и военной техники на период с 2016 по 2025 год», С. Панков отметил, что сегодня целью создания НТЗ для перспективного, в том числе нетрадиционного





**Дмитрий НОВИКОВ,**  
директор Института проблем управления имени В.А. Трапезникова РАН

вооружения является **заблаговременное решение наиболее сложных научно-технических проблем**, связанных с его разработкой. Основой этого должны стать концентрация материальных и финансовых ресурсов на межвидовом уровне, предварительная отработка и обеспечение единства концептуальных, архитектурных, схемных и технических решений, снижение уровня неопределенности и подтверждение реализуемости принципиально новых научно-технических решений. Основные задачи создания НТЗ в Концепции определены так: поиск и реализация новых, в том числе нетрадиционных форм, способов и средств решения существующих и перспективных военных и специальных задач; поиск и разработка новых принципов создания вооружения, технологий и материалов; поиск, оценка реализуемости и внедрение новейших научных, научно-технических и прочих достижений в интересах создания перспективных ВВСТ.

В качестве приоритетных направлений разработки перспективного вооружения докладчик выделил лазерное и радиочастотное оружие, оружие на основе гиперзвуковых технологий и робототехнические комплексы.



**Наталья СОБОЛЕВА,**  
компания «ЛМ Софт»

А на примере разработки технического облика и обоснования технико-экономических показателей крылатых ракет оперативно-тактического и стратегического назначения рассказал о создании и реализации научно-технического задела в ОКР по разработке перспективных ВВСТ.

В завершение первого пленарного заседания выступил **Дмитрий Новиков, директор ФГБУН «Институт проблем управления имени В.А. Трапезникова РАН»**, с докладом «Проблемы управления жизненными циклами знаний, технологий и наукоемкой продукции: межотраслевая и междисциплинарная интеграция». Он констатировал актуальность согласованного управления жизненными циклами таких элементов комплексной деятельности организационно-технических систем, как сама деятельность, продукт и изделие, являющиеся ее предметом, внешняя потребность и ресурсы, включая знания, технологии и организации.

Д. Новиков рассмотрел также типологию междисциплинарности: интердисциплинарность, трансдисциплинарность, мультидисциплинарность, кроссдисциплинарность – взаимное влияние дисциплин и синергетический



**Дмитрий КОПАНЕВ,**  
Siemens PLM Software

эффект от межотраслевого переноса прикладных результатов. Докладчик отметил, что в контексте управления наукой и использования ее результатов на практике эволюционное развитие научных дисциплин и их ответы на междисциплинарные запросы характеризуются высокой степенью истинной неопределенности результатов и времени их получения. Вместе с тем **рост уровня междисциплинарности представляется чрезвычайно привлекательным**, поскольку повышает экономическую эффективность научных исследований и разработок за счет расширения возможности передачи имеющихся результатов в новые теоретические и прикладные области.

## Проблемы импортозамещения и цифровизации в авиационной отрасли

После пленарного заседания работа конференции продолжилась в тематических секциях:

- «Интеграция управления жизненным циклом технологий и продукции ОПК» (модератор – **Владислав Клочков**);
- «Информационная поддержка процессов развития





**Александр КУЛИКОВ,**  
НИЦ «Институт имени  
Н.Е. Жуковского»

и индустриализации технологий» (модератор – **Александр Куликов**);

- «Подходы к управлению созданием НТЗ в жизненном цикле высокотехнологичной продукции» (модератор – **Павел Филиппов**).

**Дмитрий Копанев (Siemens PLM Software)** выступил с докладом, посвященным системной инженерии и обеспечению выполнения требований при разработке наукоемкой продукции начиная с ранних этапов жизненного цикла. Он начал с постулата о том, что изделие – это комплекс систем, которые некорректно рассматривать по отдельности ни при определении требований, ни при разработке. **Работа изделия – это работа его систем**, функциональность которых необходимо обеспечить, причем необходима параллельная разработка систем изделия (объекта управления) и алгоритмов систем управления, а успешность проекта критически зависит от качества, сроков и стоимости разработки самих систем.

Докладчик показал, что все это можно обеспечить с помощью технологии «Виртуальный интегрированный самолет», реализованной в виде масштабируемой комплексной имитационной

модели самолета и его систем. Эта модель верхнего уровня представляет изделие в сборе, включая все системы, функции, а также взаимосвязи между ними. Она необходима для выбора оптимальной архитектуры изделия, детализации и каскадирования требований на уровень разработчиков систем, утверждения «интерфейсных контрактов» по каждой системе, контроля выполнения требований верхнего уровня и постоянного контроля за качеством проектных решений, а также за обеспечением требуемой интеграции систем. Модели этого уровня, отметил Д. Копанев, на российских предприятиях, как правило, отсутствуют. Предприятия страны используют расчетные модели отдельных систем. Однако в отсутствие интегрирующей модели системы являются изолированными, не могут быть собраны, их интеграция не может быть проверена, а моделирование по большей части не подкреплено ни методически, ни административно.

О платформе прикладных исследований и всестороннего численного моделирования на основе платформы ANSYS рассказал **Николай Староверов, директор инженерного центра, технический директор**

**компании «КАДФЕМ Си-Ай-Эс».** Проанализировав сложность современных разработок и роль численного моделирования, он заявил, что для отраслей ОПК и авиастроения доказана оправданность инвестиций в численное многодисциплинарное моделирование. В качестве примера он привел программы модернизации высокопроизводительных вычислений и применения компьютерного моделирования Министерства обороны США (JSF F-35, гиперзвуковой аппарат HIFiRE).

Доклад **Владимира Макарова (ЦИАМ имени П.И. Баранова)** был посвящен использованию методов и средств математического моделирования и управления инженерными данными для создания многоуровневой модели авиационного газотурбинного двигателя («цифровой двигатель») как объекта формирования опережающего НТЗ. Он указал на существующую проблему разрыва уровней моделирования всего двигателя, а также сказал о том, что необходимо изменить саму ментальность инженеров, подвигнув их к использованию инновационных цифровых разработок. Технологию «цифрового двигателя» В. Макаров предложил сделать приоритетной в авиастроении.



**Михаил Лобачев (КГНЦ)** рассказал о проблемах создания и использования суперкомпьютерных технологий при проектировании высокотехнологичной продукции. Прежде всего он отметил наличие в существующих нормативных документах подмен и несоответствий понятий, которое, в частности, может привести к тому, что математическое моделирование физических процессов окажется вне нормативно-правовой базы. М. Лобачев обозначил также необходимость регламентировать вопросы финансирования, включая структуру цены и оценку трудоемкости, численного моделирования физических процессов в высокотехнологичных изделиях и имитационного моделирования сложных технических систем, без чего невозможно работать с военной приемкой. Значительное внимание докладчик уделил проблеме **недостаточной оснащенности предприятий ОПК вычислительной техникой** и использования зарубежного коммерческого и отечественного ПО, а также пакета с открытым кодом OpenFOAM. По мнению КГНЦ, требуется создание линейки (иерархии) суперкомпьютеров различной производительности и оснащения ими предприятий: 5–50 Тфлопс на отдельных предприятиях, до 500 Тфлопс в отраслевых центрах компетенции



**Юрий РАТАЙ,**  
компания «ЛМ Софт»

и уже существенно большей производительности в межотраслевых центрах (Минпромторг России, Росатом, РАН), а наиболее целесообразной представляется четырехуровневая иерархия.

В совместном выступлении **Дарья Сизоненко** и **Михаил Скулябин (КГНЦ)** рассказали о внедренной в Крыловском центре системе учета и управления результатами научно-технической деятельности.

**Наталья Соболева, руководитель отдела экспертизы проектного управления компании «ЛМ Софт»**, в докладе «Информационная поддержка процессов сквозного проектного управления в сфере создания и промышленного применения НТЗ» рассказала о функционировании созданной подсистемы технологической поддержки проектов в составе автоматизированной информационной системы проектного управления Минпромторга России, задачей которой является повышение эффективности процессов мониторинга, анализа и управления реализацией проектов на оперативном уровне. В свою очередь, разработанная «ЛМ Софт» подсистема призвана прежде всего отслеживать рост научно-технического задела, создаваемого на выделяемые министерством бюджетные средства, и его применение на предприятиях ОПК.



**Анна КАН,**  
НИЦ «Институт имени  
Н.Е. Жуковского»

Доклад **Анны Кан, начальника отдела НИЦ «Институт имени Н.Е. Жуковского»**, был посвящен созданию отечественной информационной среды поддержки разработки комплексов бортового оборудования самолетов на основе унифицированных авиационных технологических стандартов и интерфейсов. По мнению специалистов Центра, **единая информационная среда разработки** позволит контролировать стоимость разработки, сокращать издержки и контролировать выполнение сроков проекта, а также позволит взаимозаменять и повторно использовать аппаратные и программные компоненты благодаря стандартизации и унификации ключевых интерфейсов. Кроме того, такая среда даст возможность исключить двойную разработку, снизить затраты на испытания, сократить цикл разработки ПО, а также упростит интеграцию и сертификацию, ускорит поставки новой функциональности на борт воздушного судна.

## Задача на будущее: меньше технократии — больше экономики

Во втором пленарном заседании принял участие **Олег**



**Леонид КУЗНЕЦОВ,**  
ОСК

**Бочкарев, заместитель председателя коллегии Военно-промышленной комиссии РФ.**

Он проанализировал управление жизненным циклом с позиции специфических задач предприятий ОПК и отметил, что на конференции было много технократов и мало представителей бизнеса и экономистов, а именно они сейчас нужны для правильной оценки перспективности тех или иных ИТ-технологий. В связи с этим он предложил на следующей конференции **сместить акценты в сторону более полного и глубокого освещения экономической составляющей новых технологий.** О. Бочкарев также отметил, что следует рассмотреть проблемы внедрения и практического использования предложенных в ходе конференции новых подходов и методологий. Кроме того, по его убеждению, эксперты должны обратить внимание на обсуждение и выработку типового контракта жизненного цикла.

В ходе конференции генеральный директор НИЦ «Институт имени Н.Е. Жуковского» А. Дутов и директор Института проблем управления имени В.А. Трапезникова РАН Д. Новиков подписали соглашение о сотрудничестве. В рамках соглашения стороны планируют заниматься разработками новых технологий управления созданием опережающего научно-технического задела и решением задач в области управления и навигации, направленных на повышение надежности, экологичности и безопасности летательных аппаратов, беспилотных авиационных систем, двигателей и бортового оборудования.

**Леонид Кузнецов, директор департамента координации программ и проектного управления ОСК,** посвятил свой доклад программно-проектному управлению в ОСК и управлению жизненным циклом в судостроении по методу «Контрольные точки».

**Владимир Биткин (Siemens PLM Software)** рассказал



о применении системной инженерии и междисциплинарных инженерных расчетов на ранних этапах жизненного цикла.

**Константин Костромин, заместитель директора департамента управления разработкой ОАК,** вынес на обсуждение собравшихся создание национальной системы управления технологическим развитием: ее цели, задачи, критерии оценки и результаты выполнения задач.

В докладе «Методические основы управления трансфером и индустриализацией технологий в программах ЖЦ образцов ВВСТ» **Юрий Ратай, руководитель направления проектной экспертизы компании «ЛМ Софт»,** рассказал о влиянии трансфера технологий в рамках НИР на цену эксплуатации и создания изделия, полную стоимость программы и результативность технического перевооружения. Докладчик особенно подчеркнул **необходимость сквозной интеграции процессов научно-технологического и научно-инженерного развития:** фундаментальных и прикладных НИР, процессов анализа, планирования, развития технологий и др. с процессами более поздних этапов жизненного цикла ВВСТ, таких как проектирование и разработка,

технологическая подготовка производства, испытания, обеспечение боеготовности и эксплуатационной эффективности, модернизация.

В заключение с обобщающими сообщениями выступили модераторы секций. После этого **Андрей Дутов, генеральный директор НИЦ «Институт имени Н.Е. Жуковского»,** подвел предварительные итоги конференции и внес предложения для принятия резолюции.

С целью обеспечить эффективное выполнение указов Президента РФ о реализации планов (программ) строительства и развития Вооруженных Сил и модернизации ОПК в части создания систем управления полным жизненным циклом вооружения, военной и специальной техники было предложено сформулировать научно обоснованный комплекс мероприятий по совершенствованию нормативной, нормативно-правовой, технологической и материально-технической базы ОПК.

Участники конференции также посчитали целесообразным создать рабочую группу при НТС ВПК для разработки национального стандарта модели полного жизненного цикла ВВСТ и сформировать соответствующий экспертный орган. ■

# Александр КУЗЬМЕНКО: «Код» решения проблем управления ЖЦ существует»



Российские разработчики и производители высокотехнологичной продукции накапливают опыт применения методов управления жизненным циклом (ЖЦ) продукции, внедрения и использования специализированных информационных систем управления жизненным циклом. О тенденциях в названной сфере рассказывает Александр КУЗЬМЕНКО, генеральный директор компании «ЛМ Софт», решения которой применяются в Минпромторге России, организациях Роскосмоса, на предприятиях авиационной и судостроительной отраслей.

**– Каковы сегодня основные тенденции и проблемы в управлении жизненным циклом продукции высокотехнологичных отраслей в России?**

– Недавно в Москве прошла 2-я научно-практическая конференция «Управление созданием научно-технического задела в жизненном цикле высокотехнологичной продукции – 2017» при участии представителей Военно-промышленной комиссии РФ, Министерства обороны Российской Федерации, НИЦ «Институт имени Н.Е. Жуковского», Института проблем управления имени В.А. Трапезникова РАН, ОСК, ОАК, ГРЦ имени академика В.П. Макеева, других заинтересованных организаций. На конференции обсуждались актуальные проблемы управления ЖЦ высокотехнологичной продукции на начальных этапах – исследования и разработки. Приняли

участие в этом мероприятии и мы, поскольку продукты нашей компании применяются в управлении жизненным циклом высокотехнологичной продукции оборонной и гражданской промышленности и в целом тематика начальных стадий ЖЦ для нас очень интересна.

Управление ЖЦ продукции направлено в первую очередь на оптимизацию сроков, стоимости разработки и постановки на производство новых образцов продукции. Как отметил представитель Минобороны России, накоплен практический опыт перехода от стадии к стадии жизненного цикла изделий, в том числе опыт ошибок, приводящих к удорожанию работ и увеличению их продолжительности. Например, по программе самолета ДРЛО А-100 «Премьер» из-за ошибок при переходе к опытно-конструкторским работам стоимость работ увеличилась на 50%, а их продолжительность – на два года.

Замечу, что проблема ошибок при управлении ЖЦ не является исключительно российской. Примером может служить американская программа создания истребителя 5-го поколения F-35

«Лайтнинг II», в ходе которой плановые затраты на разработку самолета и плановая стоимость серийного изделия возросли в несколько раз, а общая стоимость жизненного цикла машины может превысить 1,3 трлн долл.

Поэтому совершенно логично, что еще одной важной темой, поднятой на конференции представителем Военно-промышленной комиссии, стала оценка стоимости ЖЦ продукции, на основе которой должна формироваться стоимость работ и государственных контрактов по гособоронзаказу. Соответственно было сформировано предложение включить в программу конференции следующего года тематику экономики жизненного цикла, чтобы поднять и обсудить актуальные вопросы управления стоимостью ЖЦ перспективных образцов ВВСТ.

**– С какими еще вопросами вышли на конференцию представители отраслевой науки?**

– Представителей авиационной науки и отрасли в целом волнуют вопросы создания опережающего научно-технического задела. Научно-исследовательские работы, говорят авиационные специалисты, должны быть

направлены на создание образцов, которые будут принципиально лучше предшественников. В авиации такое преимущество должно составлять 10–15%. С использованием имеющихся технологий достигнуть этих показателей невозможно. Все ждут новой технологической революции в 2025–2030 г., и готовиться к ней необходимо сейчас. Решения, принимаемые в области НТЗ сегодня, в будущем году или через два года, могут иметь трудно предсказываемые последствия в горизонте 10–20 лет.

Но дело в том, что проекты научных исследований и разработок являются наиболее рискованными, особенно на начальных стадиях. Основной задачей в этой области является снижение неопределенности условий принятия решений – в частности, за счет развития методического и программного обеспечения мониторинга, анализа и прогнозирования перспективных разработок, выявления и оценки экономических и технических факторов развития технологий. Кроме того, необходимо формировать и развивать инфраструктуру верификации, повторного использования и коммерциализации результатов интеллектуальной деятельности.

**– Насколько упомянутые проблемы представляются решаемыми? Когда можно ожидать появления программных продуктов, поддерживающих выполнение задач, стоящих перед наукой и промышленностью?**

– Как руководитель компании, специализирующейся в том числе на разработке программных продуктов, скажу, что решение любой структурированной задачи может быть описано соответствующим «кодом». И я рад сообщить, что код, обеспечивающий решение многих проблем управления жизненным циклом, уже существует и успешно нами используется.

Например, в рамках развития АИС проектного управления Минпромторга России создана

подсистема мониторинга технологической зрелости. Подсистема отвечает за отслеживание развития создаваемого за государственные средства научно-технического задела (НТЗ) и его применения в промышленности. Основным объектом управления подсистемы является технология, имеющая такую комплексную характеристику, как уровень готовности. Для оценки уровня готовности разных классов технологий применяются особые расчетные модели («калькулятор УГТ»). В целом чем выше уровень готовности, тем более зрелой и проверенной является технология. Механизм оценки УГТ является важным средством снижения рисков исследовательских программ и программ создания перспективной техники.

Программное обеспечение проектного управления с существенно расширенной функциональностью мы разрабатываем для одной из ведущих организаций Госкорпорации «Роскосмос». Во взаимодействии с предприятиями корпорации в этом году создается макет системы сбора, обработки и хранения данных для анализа и прогнозирования стоимостных показателей продукции, а также ведения единого реестра покупных комплектующих изделий, закупаемых для реализации Федеральной космической программы. Фактически речь идет о создании ПО, которое позволяет моделировать и прогнозировать затраты на всех стадиях ЖЦ продукции.

Для таких наших заказчиков, как НИЦ «Институт имени Н.Е. Жуковского», ОСК, Крыловский научный центр, в 2016 г. мы выполнили значительный объем работ по методическому обеспечению управления ЖЦ и автоматизации управления ЖЦ. Это проекты по определению путей управления созданием и использованием НТЗ в жизненном цикле продукции, по обеспечению стандартизации и качества авиационной техники, согласованности нормативного регулирования на различных

фазах жизненного цикла авиационной техники, по адаптации методов бережливого производства к российским реалиям в судостроении и разработке соответствующей нормативной базы – отраслевых ГОСТ по бережливому производству.

**– На чем сфокусировано внимание «ЛМ Софт» сегодня и по каким направлениям вы планируете развивать компетенции?**

– Мы продолжаем развитие существующей экспертизы и линейки ПО. На базе функциональности ПО для управления НСИ LM Soft MDM планируем развитие более универсальной платформы управления сложными данными.

В части поддержки проектного управления активно развиваем направление сквозного управления стоимостью ЖЦ изделий на всех этапах – от укрупненных прогнозных оценок на начальных стадиях ЖЦ до формирования иерархической структуры плановых и фактических затрат на стадиях разработки, опытных образцов и перехода к серийному выпуску продукции. Наши подходы к управлению стоимостью основаны на методах системной инженерии и обеспечении сквозного управления требованиями, структурой изделия и пакетами работ, балансировки рисков между этапами ЖЦ. Мы проанализировали и обобщили широкий спектр наработок по управлению стоимостью ЖЦ продукции, включая опыт ведущих мировых аэрокосмических и оборонных структур: NASA, Airbus, Минобороны США (USDOD) и т. п., – и готовы адаптировать полученные результаты к потребностям конкретных предприятий.

Кроме того, мы получили лицензию на образовательную деятельность, и теперь можем обеспечить полноценное обучение по ключевым аспектам управления ЖЦ продукции и использованию наших программных продуктов. ■

# Наука безопасности операционных платформ

В главном здании Российской академии наук прошла IV научно-практическая конференция OS DAY, подготовленная девятью компаниями и организациями: Институтом системного программирования (ИСП) РАН, DZ Systems, ГосНИИАСом, «Свемелом», «Базальт СПО», «Открытой мобильной платформой», «Лабораторией Касперского», «РусБИТех-Астра» и «Тайзен.ру». OS DAY обретает статус площадки, на которой формулируются и корректируются подходы к разработке отечественного ПО и операционных платформ. В конференции приняли участие свыше 200 участников, заинтересованных в развитии операционных систем, более 30 докладчиков рассказали о своих разработках. Корреспондент журнала Connect выяснил, что сегодня находится в центре внимания представителей научных институтов, разработчиков операционных платформ и производителей ПО.

Первая конференция в 2014 г. была организована усилиями Института системного программирования РАН и группой компаний DZ Systems. В этом году список соорганизаторов расширился, а мероприятие примерило формат коммуникационной площадки для теоретиков и практиков системного программирования, производителей аппаратного обеспечения и заказчиков. Три года назад на конференции обсуждали, следует ли направлять усилия на разработку операционных систем в нашей стране, в 2015-м, когда появились трудности с использованием импортного ПО, зашла речь о прикладных задачах. В прошлом году участники OS DAY обменивались опытом встраивания операционных систем в аппаратные платформы.

Лейтмотивом IV конференции OS DAY стала тема обеспечения качества операционных платформ, неотъемлемым слагаемым которого является безопасность. В настоящее время уровень информационной безопасности в значительной мере определяется качеством ПО. Ошибки в исполняемом коде приводят к потере стабильности работы программы, уязвимостям защиты, из-за ошибок в программе пользователи могут обходить средства разграничения прав доступа и т. д. На конференции отмечалось, что границы

между ошибками программистов, закладками и несанкционированными возможностями весьма размыты. Очевидно, что за безопасностью операционных систем стоят научные разработки. Осознание данного тезиса участниками рынка показывает, что отечественные компании не только нуждаются в результатах научных исследований, но и готовы за них платить.

Участие в конференции представителей различных сегментов ИТ-индустрии – отрадное и закономерное явление. По словам директора Института системного программирования РАН Арутюна Аветисяна, развивать направление разработки операционных платформ можно только в рамках сообщества, кооперации, в одиночку сил на это не хватит. Причем важно рассматривать эффективные средства разработки в комплексе, с позиций функциональности, продуктивности и удобства использования, внедрять инструменты, поддерживающие жизненный цикл разработки безопасного ПО.

Если говорить о современных вызовах в сегменте операционных платформ, то один из них связан с замещением импортных программных продуктов отечественными ради достижения технологической независимости. Прилагаемые в этом направлении усилия не должны приводить к снижению

уровня культуры разработчиков. Одна из опасностей кроется в том, что импортозамещение может содействовать продвижению на рынке компаний с невысокой культурой разработки. Нужно быть осторожными и думать об этом, заметил директор ИСП РАН Арутюн Аветисян. Еще она проблема – кадры высшей квалификации, способные осуществлять мониторинг киберугроз. Для решения задач, связанных с кибербезопасностью, нужно создавать комплексную программу исследований угроз в указанной сфере, направленную на разработку технологий и развитие кадрового потенциала.

Об основных направлениях повышения защищенности операционных систем говорил в своем выступлении на конференции заместитель директора Федеральной службы по техническому и экспортному контролю России Виталий Лютиков. Подготовленным ФСТЭК национальным стандартом защиты информации предусмотрены мероприятия, реализация которых, как ожидается, позволит свести к минимуму появление уязвимостей при разработке операционных систем. Применение стандарта носит добровольный характер, но регулятор рекомендует разработчикам и производителям операционных систем оценить необходимость его внедрения в процесс создания

продуктов. Одна из актуальных проблем сегодня продиктована тем, что внутренние процедуры реагирования на уязвимости у разработчиков не отработаны.

В течение двух дней на конференции обсуждались различные аспекты темы «операционная система как платформа». Выступления, рассказывающие о реализуемых проектах, а также большое количество вопросов из зала давали пищу для размышлений. Новой революцией в сфере ИТ руководитель управления перспективных технологий «Лаборатории Касперского» Андрей Духвалов назвал подключение всевозможных устройств к Интернету. По его прогнозам, в скором времени объем трафика, создаваемого и потребляемого такими устройствами, превысит объем трафика, создаваемого людьми. Наряду с преимуществами подключения к Сети человеку нужно быть готовым к дополнительным рискам. Обеспечить кибербезопасность в новых условиях можно при использовании ОС с интегрированными средствами защиты.

Многие выступления на конференции были посвящены перспективам создания и потенциалу операционных систем отечественного производства. Одну из них в своем кратком докладе, прозвучавшем под занавес первого дня мероприятия, представил заместитель директора по базовым информационным технологиям научно-технического предприятия «Криптософт» Валерий Егоров. Он сознательно выбрал тезисный стиль выступления, чтобы дать возможность аудитории задать уточняющие вопросы. И расчет оправдался – зал устроил докладчику коллективное интервью, которое завершилось заслуженными аплодисментами.

Компания «Криптософт» почти два десятка лет занимается разработкой многопользовательской защищенной операционной системы QP ОС, построенной по принципу монолитного ядра. Важно отметить, что данная разработка не является клоном другой операционной системы, создавалась, что называется, с нуля. QP ОС функционирует



*В зале во время работы конференции*

на платформах x86, x64, ARMv7 и MIPS64 (по словам Валерия Егорова, полноценно на первых двух). Система рассчитана для использования во встроенных решениях, в серверах (почтовых, виртуальных машин), а также в качестве системного ПО для рабочих станций. В настоящее время разрабатываются прикладные программы платформы QP ОС. Сертифицированная ФСБ России система поддерживает широкий спектр периферийного оборудования. Для нее создан полный стек заново написанных драйверов, в том числе сетевых. Производительность системы можно было оценить на стенде компании, развернутом в холле помещения, где проводилась конференция.

С докладами на конференции выступили представители университетов России и Беларуси, а также компаний Intel, Samsung, «Свемел», «НеоБит», «РедСофт». На мероприятии было объявлено о сотрудничестве компании DZ Systems и Университета Иннополис. Предметом совместной работы станет, в частности, развитие операционной системы «Фантом» на базе «Эльбруса». В планах Университета Иннополис и DZ Systems – тестирование, доработка «Фантома» и создание на этой основе экосистемы. О системе, которая

написана с нуля и не использует чужой код, в Иннополисе говорят, что это шаг вперед и с точки зрения преподавания.

Работа двухдневной конференции, посвященной созданию операционных платформ, завершилась обсуждением положений резолюции. По мнению представителей профессионального сообщества, сегодня очевидна необходимость реализации комплексной программы исследований и разработок в области системного программирования и информационной безопасности под патронажем ИСП РАН. Участие промышленных партнеров в реализации такой программы даст возможность апробировать и внедрять новые инструменты, определять дальнейшие направления разработок.

Важно обеспечить гармонизацию государственных информационных систем и их переход на отечественное офисное ПО. Одно из предложений, адресованных регуляторам и органам по стандартизации, продиктовано необходимостью отказаться от предусмотренных в государственных стандартах требований использования проприетарных форматов документов, буквально привязывающих пользователей к пакету MS Office. ■

[www.connect-wit.ru](http://www.connect-wit.ru)

# На PHDays обсуждали проблему периметра безопасности

Компания Positive Technologies провела 23 и 24 мая седьмой PHDays – конференцию и конкурс CTF для специалистов информационной безопасности. Нынешняя PHDays – это полгода подготовки, 1100 компаний-участников (из которых только 250 ИБ-компаний), 196 спикеров, 50 партнеров. За два дня форум посетило рекордное число участников – около 5000 из разных стран мира: Америки, Израиля, Кореи, Италии, Франции, Германии, Казахстана, Беларуси, Индии, Польши и, конечно, России.

Конкурс среди хакеров CTF (Capture the Flag – борьба за флаг), который уже второй год проводится в формате «Противостояния», в этот раз был максимально приближен к реальности:

в распоряжении участников был целый полигон с моделью мегаполиса, где помимо офисов, телеком-операторов, железной дороги, ТЭЦ и прочих объектов находилось множество

IoT-устройств – целый виртуальный город. К барьеру были приглашены «хакеры», «защитники» и security operation centers (SOC). В результате хакерам удалось украсть деньги из банка виртуального города, перехватить SMS, компрометирующие меры, провести успешную атаку на электростанцию, ТЭЦ и нефтеперерабатывающий завод и перехватить автомобиль с украденными деньгами, взломав систему трекинга автотранспорта. Результаты исследований будут использованы для улучшения безопасности реальных критически важных объектов.

Была затронута на мероприятии и тема эпидемии шифровальщика WannaCry, который продемонстрировал слабость современных систем защиты. Причем основная проблема даже не в технической стороне вопроса, а в процессах. Исправления к уязвимости были опубликованы за два месяца до нападения шифровальщика. За месяц до нападения хакерская группа TheShadowBrokers опубликовала эксплойт, который к тому же начал активно распространяться в конце апреля, но без шифровальщика. Евгений Климов, технический директор «Информзащиты», отметил: «После публикации эксплойтов TheShadowBrokers на такой же конференции я спросил коллег, хорошо ли они провели выходные, потому что мы круглые сутки разбирали опубликованные эксплойты и готовили рекомендации для







наших клиентов. Однако многие на профильной конференции даже и не слышали об опубликованном архиве эксплойтов!»

Кроме того, компании плохо знают свой периметр. Сергей Гордейчик, заместитель технического директора «Лаборатории Касперского», сказал: «Когда прошла атака и к нам за помощью начали обращаться компании, мы запрашивали IP-адреса периметра их корпоративных сетей. Иногда в ответ приходил адрес сети /16, в которой может быть до 16 536 адресов». Такой ответ клиентов означает, что компания просто не знает своего периметра, поэтому не может его контролировать. Именно в этом причина возникновения проблем с обнаружением побочных открытых

каналов проникновения WannaCry в корпоративные сети – через несанкционированные подключения.

Впрочем, как сообщил в эксклюзивном интервью для Connect Александр Гостев, ведущий эксперт «Лаборатории Касперского», сам WannaCry вырвался на просторы Интернета, скорее всего, по ошибке и раньше, чем этого хотели авторы «червя». Ведь тот самый домен, с помощью которого в результате остановили эпидемию, на самом деле предназначался для другого – для сбора сведений от жертв и генерирования одноразовых кошельков биткоина. Те три адреса, которые сейчас используются, были резервными на случай недоступности основного сервера. Предположительно «червь» должен был

в каждом конкретном случае генерировать уникальный кошелек и вместе с ключами шифрования пересылать его на указанный домен. Возможно, домен должен был быть в защищенной сети ToG, но во время отладки программисты вбили тестовый домен от фонаря в домене .com. Пикантность ситуации в том, что теперь авторы «червя» просто не могут прислать ключ дешифровки своим жертвам, поскольку у них нет информации о том, какие ключи какой жертве соответствуют. Таким образом, можно констатировать, что и у разработчиков вирусов тоже есть проблемы с периметром – они не всегда могут удержать внутри недоделанные вредоносные. ■

*Валерий КОРЖОВ*

# В витрине отрасли на выставке «Связь-2017»

В Москве состоялась 29-я международная выставка информационных и коммуникационных технологий «Связь-2017». По данным организаторов, крупнейшее в отрасли информационных технологий и телекоммуникаций в России мероприятие, проходившее с 25 по 28 апреля в ЦВК «Экспоцентр», собрало 325 компаний из 23 стран, в том числе 177 российских. Страной – партнером выставки в этом году стал Азербайджан. Коллективные экспозиции оформили также Китай и Тайвань. Впервые в рамках выставки «Связь-2017» состоялась международная конференция «TeleMultiMediaForum 2017: Настоящее и будущее медиапотребления в России и мире».

В этом году в выставке наряду с компаниями из Германии, Италии, Кипра, Нидерландов, Финляндии, Франции, Израиля, Индии, Китая, Южной Кореи, Японии вновь участвовали представители Испании, Польши, Украины и Беларуси. Впервые на выставке «Связь-2017» свою продукцию и решения показали компании из Ирана и Сингапура.

На церемонии открытия выставки глава комитета Госдумы по информационным технологиям, информационной политике и связи Леонид Левин отметил, насколько стремительно развиваются цифровые технологии, которые все шире проникают

в энергетику, сельское хозяйство, медицину, ЖКХ. Благодаря современным технологиям появляются новые профессии. Одной из преобладающих тенденций в сфере телекоммуникаций он назвал персонализацию получаемой пользователями информации.

Демонстрируя передовые разработки и технологии, выставка «Связь» помогает мобилизовать потенциал и ресурсы отрасли, подчеркнул глава Федерального агентства связи («Россвязь») Олег Духовницкий. Агентство участвует в выставке восьмой раз и представлено ведущими российскими госкомпаниями в области связи и ИТ, в том числе

Группой компаний «Космическая связь». Оператор продолжает работу над новыми спутниками «Экспресс-80» и «Экспресс-103». Как ожидается, в результате вывода их на орбиту через несколько лет появится возможность предложить обновленный перечень услуг.

К слову, в первый день работы выставки «Космическая связь» (ГП КС) открыло серию юбилейных бизнес-мероприятий, организованных совместно с партнерами в московском регионе, Сибири и на Дальнем Востоке. В текущем году спутниковый оператор отмечает 50-летний юбилей. В рамках проведения «Связь-2017» ГП КС представило проект по оказанию услуг спутникового ШПД в диапазоне Ка. В этом одновременно праздничном и деловом мероприятии принял участие Евгений Буйдинов, заместитель генерального директора ГП КС, который рассказал о достижениях, сделал акцент на важных для страны инфраструктурных проектах, осуществленных ГП КС. Четыре года назад компания создала уникальную сеть спутниковой связи, которая сегодня включает в себя хабы, находящиеся в Дубне, Хабаровске и Железногорске. Это позволяет спутниковому оператору работать через семь-восемь космических аппаратов и иметь полноценное покрытие, охватывающее территорию России,



Открытие выставки «Связь-2017»

ближайшую акваторию морей и океанов, а также Ближний Восток, Европу, часть Средней Азии и Дальний Восток. Кроме того, оператор «Космическая связь» реализовал крупный совместный проект с «Гидрометцентром» России, построив станции на Севере в труднодоступных регионах. Одной из отличительных особенностей этого уникального проекта является возможность для заказчика («Гидрометцентра») самостоятельно распределять спутниковый ресурс для любой станции. Сегодня наиболее актуальна услуга спутниковой видеосвязи, с помощью которой сотрудники метеостанций обучаются работе на новом оборудовании.

После церемонии открытия выставки начался Большой медиакоммуникационный форум, организованный Российской ассоциацией электронных коммуникаций (РАЭК) и АО «Экспоцентр». Заседания и дискуссии в рамках мероприятия продолжались в режиме нон-стоп. С аналитическим докладом на форуме выступил директор Российской ассоциации электронных коммуникаций Сергей Плуготаренко, который отметил вклад цифровой экономики России в общую экономику страны. По мнению докладчика, под цифровой экономикой следует понимать сегменты рынка, в которых добавленная стоимость создается с помощью цифровых или информационных технологий. Одним из аспектов исследования цифровой экономики стали вопросы медиа, в частности интернет-рекламы. Объем этого сегмента в 2016 г. эксперты оценивают в 136 млрд руб. Среди основных тенденций в этой сфере отмечается увеличение расходов на интернет-рекламу, активное использование нативной и мобильной рекламы, а также популярность блокировщиков рекламы. Область медиа и развлечений оценивается аналитиками в 63 млрд руб. Ключевой тренд заключается в том, что интернет-холдинги обходят телеканалы по влиянию на аудиторию и проценту ее охвата.



*Евгений Буйдинов представляет обзор достижений ФГУП «Космическая связь»*

В дни работы выставки состоялись переговоры между компаниями России и Китая, а также церемония подписания соглашений между МТУСИ и фирмой «1С», МТУСИ и компанией «Лаборатория Касперского». В вузе создается базовая кафедра «Корпоративные информационные системы», которая станет одним из звеньев практико-ориентированного обучения по образовательным программам на основе сертификационных курсов «1С» и будет содействовать организации образовательно-производственной площадки для совместных проектов. Базовая кафедра создается в МТУСИ на факультете информационных технологий, который, по данным рейтинговых агентств, показывает один из самых высоких уровней подготовки специалистов, востребованных на рынке труда среди столичных вузов.

Что касается соглашения по стратегическому партнерству в сфере образования с «Лабораторией Касперского», то документ предусматривает ряд совместных мероприятий, одним из которых является создание в МТУСИ научно-образовательного центра «Лаборатории Касперского». Структурное подразделение университета будет предоставлять образовательные

и информационно-консультационные услуги в области информационной безопасности не только внутри вуза, но и за его пределами, например представителям регионального сообщества.

По традиции в дни выставки прошло расширенное заседание Федерального агентства связи. С докладом на нем выступил глава «Россвязи» Олег Духовницкий. Его отчет о проделанной работе был представлен в виде мультимедийной презентации. Руководитель агентства ознакомил слушателей с основными итогами 2016 г., который для «Россвязи» прошел под знаком года образования. Этой теме во второй части заседания был посвящен также круглый стол на тему «Отраслевые вузы: вчера, сегодня, завтра». Высшие учебные заведения развивают сотрудничество с зарубежными университетами и отраслевыми компаниями. На базе университетов открыты учебные лаборатории LTE Nokia, лаборатория «Цифровая обработка сигналов» компании TexasInstruments.

Основные направления деятельности агентства по оказанию госуслуг в сфере связи – одна из тем выступления Олега Духовницкого. По его словам, количественные показатели минувшего года отражают рыночные



На церемонии открытия выставки были погашены почтовые конверты с символикой выставки «Связь-2017»

тенденции. На фоне падения спроса на услуги традиционной телефонии уменьшилось количество выданного ресурса нумерации в коде ABC. Изменения в сегменте сотовой связи продиктованы развитием дополнительных услуг на основе технологий M2M, новые небольшие операторы проявили интерес к бизнес-модели MVNO. Такими факторами объясняется двукратное увеличение ресурса нумерации в коде DEF. Еще больше возрос спрос на услуги колл-центров, что подтверждается десятикратным увеличением количества выделяемой нумерации в коде 800.

Колебания на валютном рынке и санкции отразились на падении потребительского спроса в сегменте мобильных устройств. Насыщенностью рынка эксперты объясняют не столь большое, как в предыдущие годы, желание производителей обновлять модельный ряд выпускаемых устройств. Одна из самых заметных тенденций выражается в том, что среди общего количества телеком-оборудования, задекларированного в 2016 г., треть пришлось на оборудование отечественного производства. Как стало известно на заседании, «Россвязь» зарегистрировала первые декларации на оптоволоконный кабель, состоящий

из оптических волокон российского производства.

В минувшем году Правительство РФ наделило «Россвязь» полномочиями федерального органа по сертификации технических средств обеспечения транспортной безопасности в отношении средств связи, приема и передачи информации.

Что касается развития универсальных услуг связи, то на фоне значительного недофинансирования контракта с «Ростелекомом» обсуждается перспектива изменения парадигмы универсальных услуг и контракта в целом. По согласованию с Минкомсвязи России смещены приоритеты предоставления универсальных услуг с пунктов коллективного доступа в сторону точек доступа. Глава «Россвязи» заявил, что закрытие «Почтой России» пунктов коллективного доступа в Интернет в малых населенных пунктах можно рассматривать как нарушение законодательства, согласно требованиям которого такими пунктами должны быть оборудованы поселения, насчитывающие более 500 жителей.

Во второй раз выставка «Связь» проводилась в рамках Российской недели высоких технологий, объединяющей несколько мероприятий. Одновременно в Экспоцентре проходили

XI международный навигационный форум и IX выставка «Навитех». Большое внимание организаторы уделили популяризации беспилотных технологий в России. Так, в рамках «Навитеха» некоммерческое партнерство «Содействие развитию и использованию навигационных технологий» организовало гонку дронов. В соревновании приняли участие пилоты из России, Литвы, Беларуси, Казахстана, Франции, ОАЭ и США. Состязания проходили в формате HD, что позволило передавать картинку высокого качества. Зрители могли увидеть трассу глазами пилотов. На отдельных участках 500-метрового маршрута дроны развивали скорость до 160 км/ч. Развитие беспилотных авиационных систем – стратегическое направление деятельности Некоммерческого партнерства «Содействие развитию и использованию навигационных технологий», которое ставит перед собой задачу создания условий для расширения этого рынка. К числу таких условий относится формирование законодательной и регуляторной базы, экосистемы сервисов, приложений и платформ.

На состоявшейся в рамках выставки «Связь-2017» первой международной конференции «TeleMultiMediaForum 2017: Настоящее и будущее медиапотребления в России и мире» аналитики, производители контента, представители технологических компаний, OTT-сервисов и операторов ТВ обсудили тенденции развития отрасли цифрового ТВ в контексте новых моделей медиапотребления.

Свои разработки на выставке «Связь-2017» представили такие известные зарубежные компании, как 3CX, Corning, Ekinops, Intelsat, Procom. Среди отечественных компаний, стенды которых привлекали внимание посетителей, можно отметить, в частности, «Газпром Космические системы», «Микран», «Натекс», «Трансвок», «Саранскабельоптика», «Супертел», «Технологии радиосвязи». ■

[www.connect-wit.ru](http://www.connect-wit.ru)

## Компания Artezio назвала лучшие мессенджеры для бизнеса

Мессенджер Cisco Jabber возглавил список самых технологичных мессенджеров в корпоративном сегменте. Таковы результаты специального исследования, проведенного аналитическим отделом софтверной компании Artezio (входит в Группу «ЛАНИТ»). По данным аналитиков, Cisco Jabber значительно опережает разработки других вендоров по технической функциональности и удобству использования в корпоративной среде. В технологическом рейтинге Cisco Jabber набрал максимальное количество баллов, при этом незначительно опередив Atlassian HipChat. По мнению экспертов-аналитиков, оба мессенджера поддерживают полный набор функций, востребованных в бизнес-коммуникациях. Среди главных достоинств специалисты выделили возможность общения сотрудников через локальный (корпоративный) сервер, обмен файлами, наличие опции «телефонная конференция» и мобильной версии. Специалисты также проанализировали качество работы мессенджеров, их надежность и безопасность передачи данных. Рейтинг наиболее функциональных и надежных корпоративных мессенджеров выглядит следующим образом: Cisco Jabber; Atlassian HipChat; IBM Lotus Sametime; Skype for Business; Brosix; Slack; Viber; Google Hangouts; Adium. В исследовании

Artezio отмечает, что включенные в рейтинг программы ориентированы на запросы различных компаний. Небольшие стартапы (до десяти человек) могут использовать бесплатные версии мессенджеров Cisco, стандартный Skype или начальную версию Slack. Для крупных компаний (от 100 до 500 человек) предусмотрены платные бизнес-версии. При этом все решения, вошедшие в список лучших, обеспечивают достаточную функциональность и качество для делового общения. Однако часто компании несвободны в выборе средств коммуникации. Аналитический отдел компании Artezio исследует существующие технологические и программные платформы, выявляет тренды: как бизнес использует современные технологические решения. Исследование проводится на основе технологического и функционального анализа приложений, учитываются такие критерии, как поддержка наиболее востребованных функций, масштабируемость и безопасность. Цель исследования – выявить на рынке продукты, которые максимально удовлетворяют требованиям бизнеса. На рынке Америки и Европы Artezio работает более 16 лет и специализируется на проектах в области IoT, машинного обучения, Big Data и убер-решениях.

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

## Huawei отметила 20-летие деятельности в России открытием центра, лаборатории и академий

Компания Huawei представила результаты работы в России в течение 20 лет, а также планы на будущее в рамках Петербургского международного экономического форума. Huawei продолжит активную работу на операторском, корпоративном и мобильном рынках, а также предпримет новые инициативы – открывает Центр исследований и разработок в Санкт-Петербурге и Открытую лабораторию в Москве. Кроме того, в честь 20-летия деятельности на российском рынке компания намерена подарить двадцати вузам России оборудование для открытия Сетевых авторизованных инфокоммуникационных академий. В 1997 г. Huawei открыла в России свой первый офис за пределами Китая. Сегодня 11 офисов компании расположены по всей стране – от Санкт-Петербурга до Владивостока. Функционируют научно-исследовательский и учебный центры в Москве, а также центр технической поддержки в Новосибирске и центр управления сетями в Уфе. Московский Центр исследований и разработок работает с 2002 г. Центр специализируется на исследованиях алгоритмов и математических моделей в области беспроводной связи, передачи и хранения данных, облачных вычислений, обработки информации. В рамках мероприятия

вице-президент Huawei Эми Линь (Amy Lin) объявила об открытии второго в России Центра исследований и разработок в Санкт-Петербурге. Центр будет специализироваться на прикладных исследованиях, в частности в области математических моделей для технологий связи. Также Huawei откроет Открытую лабораторию – специализированную площадку, на которой компании операторского и корпоративного рынка смогут тестировать и создавать локализованные решения в таких областях, как сетевые технологии, Интернет вещей, умный и безопасный город, умная энергетика, транспортные решения и др. Лаборатория будет открыта до конца 2017 г. в главном офисе компании в Москве. Третьей инициативой компании в честь двадцатилетия станет открытие двадцати новых авторизованных инфокоммуникационных академий Huawei в течение пяти лет. До конца 2017 г. новые академии откроются в нескольких ведущих вузах России. В их учебную программу войдут курсы «Системы хранения данных» и «Коммутиация и маршрутизация», разработанные при участии специалистов Huawei. Практические занятия будут проводиться на оборудовании Huawei.

Huawei Russia

# Доступность финансовых услуг

Финансовые услуги – базовая потребность человека, поскольку деньги нужны всем. Однако есть категория граждан, для которых получение любых услуг является проблемой, – это инвалиды. Для них обычное посещение отделения банка уже проблема, поэтому для них важно дистанционное предоставление услуг, причем как можно большего их набора. Проблемы доступа различных категорий пользователей к финансовым услугам обсуждались на 21-м форуме «Информационные технологии в финансовом секторе», организованном ANConferences.

К счастью, именно в направлении дистанционного предоставления услуг в основном и развивается финансовый рынок, чему способствуют информационные технологии «во главе» с Интернетом. Наиболее современные банки активно переводят свои услуги в электронный формат, не требуя для наиболее массовых операций физического присутствия пользователей в собственных филиалах. В частности, по словам Ивана Паткина, директора по электронному бизнесу среднего и малого бизнеса «Промсвязьбанка»,

до 60% продуктов банка уже переведено в электронный вид. Причем 35% общего набора услуг вообще не требует участия человека со стороны банка. «Нам удалось даже полностью автоматизировать такой массовый сегмент, как выдача кредитов, – похвалился Иван Паткин. – Правда, полностью автоматизировать этот процесс удалось только для выбранной группы наших клиентов».

Следует отметить, что для стимулирования улучшения доступности финансовых услуг в России Центробанк даже создал отдел отдела анализа рисков и перспективных технологий финансовой доступности, руководитель которого Юрий Божор рассказал на конференции о рекомендациях Центробанка по обеспечению доступности финансовых услуг для инвалидов. Чтобы максимально полно удовлетворить их потребности, недостаточно просто разработать веб- или мобильное приложение. Нужно учесть и такие особенности, как слабое или полностью отсутствующее зрение. При разработке приложений для слабовидящих следует придерживаться определенных правил. В частности, необходимо разрабатывать интерфейс таким образом, чтобы в нем могли хорошо масштабироваться шрифты и картинки. Кроме того, надо правильно подписывать элементы интерфейса. Дело в том, что слепые люди используют так называемые экранные сканеры,

которые анализируют текст на странице и преобразуют его в звук. Причем пользуются они такими сканерами очень умело и эффективно. Но если в красивом дизайнерском приложении кнопки называются «Кнопка 1», «Кнопка 2» и «Кнопка 3», то ориентироваться в таком интерфейсе с помощью сканера будет проблематично. Поэтому Центробанк рекомендует, прежде чем выпускать банковское приложение, протестировать его с учетом физических ограничений пользователей и посетителей.

Проделанная работа по учету требований инвалидов может стать для банка конкурентным преимуществом. В России зарегистрировано более 12 млн инвалидов различных категорий, и учет их требований позволит банку расширить свою рыночную нишу. Кроме того, упрощение интерфейса и его оптимизация обеспечивают возможность не искушенным в информационных технологиях пользователям легко ориентироваться в интерфейсе приложений. «Мы не рекомендуем делать отдельный интерфейс для инвалидов, – пояснил Юрий Божор, – со временем про этот интерфейс забывают, и он перестает развиваться. Проще основной интерфейс адаптировать к потребностям инвалидов, а остальные пользователи также его оценят». ■



Юрий БОЖОР, начальник отдела анализа рисков и перспективных технологий финансовой доступности, Центральный банк РФ

Валерий КОРЖОВ

# Импортозамещение в сфере инфраструктурного ПО



# Больше, чем ОС

## Обзор рынка отечественных операционных систем



**Алексей СМИРНОВ,**  
советник генерального директора,  
«Базальт СПО»

С 1 января 2016 г., согласно постановлению Правительства № 1236, при закупке программного обеспечения госорганы обязаны отдавать предпочтение российским разработкам, включенным в Единый реестр российских программ для электронных вычислительных машин и баз данных. Госкорпорациям также рекомендовано соблюдать это правило при закупке софта – летом прошлого года первый вице-премьер Игорь Шувалов направил соответствующую директиву представителям государства в советах директоров госкомпаний.

Федеральным органам исполнительной власти предписано уже к концу 2018 г. перейти на использование отечественного ПО на рабочих станциях. 27 июля 2016 г. принято распоряжение Правительства № 1588 «Об утверждении плана перехода органов исполнительной власти и государственных внебюджетных фондов на использование отечественного

ПО по мере обновления нормативной базы в сфере ИТ рынок отечественного офисного программного обеспечения постепенно оживляется. Заметную активность проявляют госструктуры, которым предстоит решать задачи, связанные с замещением импортных продуктов, и развивать ИТ-инфраструктуру на основе российских программных инструментов. Вряд ли стоит напоминать о важности выбора ПО, когда технологическая платформа закладывается на годы вперед. Операционная система – один из системообразующих элементов ИТ-инфраструктуры. Рассмотрим состояние и основные тенденции в сегменте отечественных ОС на базе ядра Linux сквозь призму ориентиров для выбора комплекса свободного программного обеспечения, включающего также ПО для управления ИТ-инфраструктурой и офисные приложения.

программного обеспечения». А недавно, в марте текущего года, были уточнены требования к отечественному офисному ПО, включенному в реестр российского программного обеспечения (постановление Правительства РФ № 325). К офисному ПО относятся операционная система, коммуникационное ПО, почтовые приложения, интернет-браузер, системы электронного документооборота, средства антивирусной защиты, файловые менеджеры, редакторы презентаций, табличный и текстовый редакторы, справочно-правовая система и др.

С принятием этих нормативных документов рынок отечественного офисного ПО заметно оживился. С одной стороны, мы на собственном опыте почувствовали, как активизировались государственные организации, которым предстоит реализовать программу импортозамещения и создать ИТ-инфраструктуру на базе российских программных продуктов. Новая технологическая платформа закладывается на годы вперед, поэтому организациям крайне важно выбрать ПО быстро и безошибочно. В противном случае

можно заложить «мину замедленного действия» в виде разнообразных рисков: технологических, экономических, репутационных, карьерных. В этом ряду выбор операционной системы как одного из основных системообразующих элементов ИТ-инфраструктуры относится к ключевым факторам.

В то же время рынок ОС стал активно прирастать разработками на базе ядра Linux, которые позиционируются как отечественные операционные системы. Среди них преобладают решения для рабочих станций и серверов, предлагаются также модификации для применения в облачной среде и весьма скромный набор мобильных платформ. На первый взгляд, ОС одного сегмента схожи по функционалу, а различия между ними незначительные. На самом деле разница существенная, что определяет соотношение полезных качеств и рисков для заказчиков.

При ответе на вопросы о состоянии и перспективах рынка отечественных операционных систем на базе ядра Linux через призму выбора и оптимального набора ориентиров будем учитывать,



что речь идет не столько об ОС как таковой, сколько о дистрибутиве – комплексе свободных программного обеспечения, включающего помимо ОС системное ПО для управления ИТ-инфраструктурой и офисные приложения для организации работы пользователей.

## Чистота «родословной»

При разработке программы импортозамещения организациям можно ориентироваться на перечень программных продуктов в Едином реестре российских программ для электронных вычислительных машин и баз данных (<https://reestr.minsvyaz.ru/>). Обязательным условием включения приложения в реестр служит тот факт, что исключительные права на ПО принадлежат российскому лицу. Если лицо юридическое, то более половины конечных бенефициаров являются российскими и за рубеж направляются не более 30% лицензионных отчислений. Соответствие программных продуктов этим условиям проверяет экспертный совет. Более половины его участников – представители известных российских разработчиков ПО, люди, чья профессиональная и человеческая репутация признана ИТ-сообществом.

Эксперты тщательно проверяют, не является ли представленное на рассмотрение ПО зарубежным продуктом в российской оболочке. Использование таких псевдоотечественных систем сродни опасной иллюзии технологической независимости. Поясню на примере. Будучи членом экспертного совета, я принимал участие в проверке операционных систем. Анализируем программный продукт, представленный на экспертизу. Возникает подозрение, что мы имеем дело с клоном CentOS – свободным вариантом платного дистрибутива американской фирмы Red Hat Enterprise Linux. Сравниваем бинарные пакеты программ, более полутора тысяч пакетов. Выясняется, что изменены... менее десяти из них – те, что связаны с брендингом

(обои рабочего стола, названия). А остальные фактически копия американского ПО. Для заказчика это означает, что российский «разработчик» сам находится в стопроцентной зависимости от создателя оригинала и не влияет на его развитие. Разумеется, такой продукт не был включен в реестр. Но история, к сожалению, не уникальна. Поэтому при выборе решения необходимо ориентироваться на перечень ПО, внесенного в реестр.

Однако присутствие в реестре не исключает иностранной «родословной» ПО. Из трех основных игроков рынка отечественных ОС – «Базальт СПО» (системы «Альт»), «НТЦ ИТ РОСА» и НПО «РусБИТех» (Astra Linux) – третий выпускает дистрибутивы для серверов и рабочих станций на базе зарубежных платформ Linux, второй – дистрибутивы для рабочих станций на базе собственного репозитория, унаследованного от международного проекта Mandriva, а серверные версии – тоже на базе зарубежной платформы. И только первый из перечисленных создает свои дистрибутивы на базе российского репозитория Sisyphus. Названный репозиторий, представляющий собой хранилище пакетов программ и инфраструктуру для разработки и тестирования операционных систем, создается совместными усилиями сообщества разработчиков из нескольких стран. Держатель репозитория определяет политику его развития с учетом потребностей российских заказчиков, совместимость с отечественными системами защиты информации, корпоративного документооборота, финансового учета и др., с аппаратными платформами, учитывает требования российского законодательства и регуляторов. В настоящее время Sisyphus – один из четырех крупнейших в мире репозиториях свободных программ. На его основе были созданы десятки дистрибутивов для органов власти и местного самоуправления, крупных промышленных предприятий, учебных и медицинских учреждений.

Благодаря независимости Sisyphus российский заказчик может быть уверен в том, что приобретенное им решение не прекратит существование по воле западных разработчиков, он не столкнется с проблемой санкционных мер в отношении ПО, программный продукт будет оперативно обновляться при обнаружении уязвимостей, а при необходимости его свойства будут дополняться.

Из отечественных мобильных операционных платформ на сегодняшний день в реестр занесена только Sailfish OS – российская версия ОС, созданная на базе разработки финской фирмы Jolla, которая, в свою очередь, взяла за основу платформы MeeGo и Maemo, которые проектировались Nokia и Intel. Параллельно развивается проект операционной системы с открытым кодом «Тайзен», которая разрабатывается участниками международного консорциума «Тайзен.Ру», объединяющего в своих рядах лидеров поставщиков свободного ПО, крупных международных вендоров ПО и оборудования (Intel, Samsung и др.). ОС предназначена для всех типов устройств Интернета вещей. Однако оба этих проекта пока испытывают трудности с получением драйверов от ведущих разработчиков устройств мобильной связи.

## В масштабах организации

В ближайшие годы наиболее динамично будет развиваться сегмент операционных систем уровня предприятия. На подходе спрос на решения, которые позволят крупным организациям построить территориально распределенную ИТ-инфраструктуру – масштабную, защищенную, гетерогенную. Именно на таких инфраструктурных решениях работают многие организации и предприятия государственного сектора, насчитывающие десятки тысяч сотрудников, тысячи рабочих мест и серверов, десятки приложений. И все это размещено по всей территории страны. Поэтому важно, чтобы в дистрибутив наряду с ОС были включены

системообразующие решения, позволяющие полноценно заменить проприетарные системы.

К ним относятся прежде всего компоненты для управления гетерогенной ИТ-инфраструктурой (аналоги Microsoft Active Directory) и обеспечения совместной работы пользователей (аналоги Microsoft Exchange Server). Так, в дистрибутивы «Базальт СПО» «Альт сервер» и «Альт рабочая станция» включены соответствующие решения Samba DC, SOGo и FreeIPA на базе свободного программного обеспечения. Причем «Базальт СПО» участвует в разработке этих продуктов.

Для организации облачных сервисов не существует отдельного класса операционных систем, для решения этой задачи ОС интегрируется с соответствующей платформой, которая может быть включена в состав дистрибутива. Так, наличие в дистрибутиве платформы OpenStack позволяет организации или провайдеру облачных услуг создавать облачные ресурсы. Средства управления виртуальными окружениями, включенные в дистрибутив, дают возможность вывести ИТ-инфраструктуру организации на новый уровень надежности и безопасности. Например, вынести в ЦОД виртуальные места пользователей, создав инфраструктуру с терминальным доступом. Такое решение на базе ОС «Системы Альт» сейчас реализуется в рамках проекта создания Единого государственного реестра ЗАГС.

Вопрос обеспечения информационной безопасности решается путем применения встроенных сертифицированных средств защиты информации с дискреционным и мандатным контролем доступа. В этой части функционала решения российских вендоров достаточно конкурентоспособны.

Еще один компонент, на наличие которого стоит обращать внимание в составе дистрибутива, – средства для разработки собственных приложений. Этот инструмент позволит заказчику самостоятельно дорабатывать необходимый функционал, а российским вендорам

облегчит задачу создания Linux-версий приложений.

Импортозамещение предполагает замену не только операционных систем, но и офисных приложений, необходимых сотрудникам организаций в их повседневной деятельности (системы электронного документооборота, бухгалтерского учета, интернет-браузер, электронная почта, ПО для создания и редактирования текстов, электронных таблиц, презентаций, для работы с видео- и звуковыми файлами, сложной графикой и анимацией, антивирусные программы и т. п.). Крайне важно, чтобы эти приложения были совместимы с операционной системой. Для удобства заказчиков разработчики ОС либо включают офисное ПО в состав дистрибутива, либо обеспечивают совместимость с разработками, включенными в реестр отечественного ПО.

## Жизнь после внедрения

До недавнего времени техподдержка была слабым звеном решений на базе свободного ПО, что препятствовало его внедрению в крупных организациях и предприятиях. Ситуация быстро меняется к лучшему. Разработчики отечественных системообразующих решений формируют экосистему интеграторов, которые берут на себя задачу оказания услуг техподдержки. Одновременно вокруг крупных организаций, инфраструктура которых насчитывает десятки, а то и сотни приложений, формируется своя экосистема поставщиков услуг поддержки решений на базе свободного ПО.

На российском рынке наметился интересный тренд создания принципиально новой сервисной модели, объединяющей эти экосистемы. Сервисный центр в режиме одного окна осуществляет поддержку целого пула решений. Заказчик получает все услуги от сервисного центра, в рамках единого SLA (Service Level Agreement), где четко прописаны количественные и качественные показатели. Но самое главное – он избавлен от традиционной

«проблемы на стыках». В гетерогенной ИТ-инфраструктуре, где множество приложений взаимосвязано, бывает сложно выявить причину проблемы. В подобных ситуациях службы техподдержки программных продуктов могут бесконечно перенаправлять заказчика друг к другу, не пытаясь решить проблему в комплексе. Сервисный центр будет принимать от заказчика заявку, самостоятельно привлекать к ее решению специалистов вендоров, и заказчик получит результат. «Базальт СПО» совместно с компанией ALP Group создала и реализует подобную модель «единой сервисной шины», в рамках которой предоставляются услуги на всей территории страны. Таким образом, выстроена модель поддержки жизненного цикла программного продукта: создание, сопровождение эксплуатации и совершенствование на основе обратной связи.

Модель техподдержки с двумя линиями, на которых осуществляется взаимодействие с пользователями и техническими специалистами заказчика, отлажена на проприетарных решениях. Но российские разработчики свободного ПО включили в эту модель третью линию техподдержки: к решению проблем подключаются эксперты, которым эскалируется проблема заказчика, причем быстро, без бюрократических проволочек, свойственных крупным вендорам проприетарного ПО. В ответ на запрос заказчик получает развернутые рекомендации и помощь в сложной настройке приложения либо его обновленную версию с устраненной уязвимостью, причем в разы быстрее, нежели это происходит в случае с зарубежным проприетарным ПО.

В заключение остается отметить, что развитая система техподдержки поможет преодолеть проблему кадрового голода, которая уже актуальна на рынке свободного программного обеспечения. Неслучайно разработчики СПО реализуют программы обучения для технических специалистов и пользователей, но на выправление ситуации потребуется время. ■

## Финальный шаг к 5G

В дни работы Петербургского международного экономического форума (ПМЭФ) «МегаФон» и Huawei установили абсолютный рекорд скорости мобильного интернет-соединения в России, продемонстрировав работу сети пятого поколения на скорости 35 Гбит/с. «Ровно год назад мы показывали скорости, чуть превышающие 1 Гбит в секунду. Символично, что мы возвращаемся на то же место – в петербургский Музей связи, но уже с новыми разработками: сегодня мы покажем еще большую скорость на сети 5G. В 2018 г. в России пройдет Чемпионат мира по футболу, и я могу сказать, что этот турнир станет самым быстрым в истории. У всех, кто окажется в Москве и Санкт-Петербурге во время проведения чемпионата, будет возможность по-новому прочувствовать эмоции этих соревнований благодаря быстрому Интернету от «МегаФона», – отметил Сергей Солдатенков, генеральный директор «МегаФона». В Санкт-Петербурге «МегаФон» и Huawei на своем стенде представили базовую станцию пятого поколения в действии. Сети 5G помимо высокой скорости также обеспечивают беспрецедентно низкие задержки передачи данных (до 1 мс), что открывает новые возможности по применению технологии 5G в различных сферах жизни. Одно из таких направлений – беспилотное вождение,

где скорость реакции является критичным фактором. На демонстрационном стенде был представлен макет автомобиля и виртуальной реальности, и посетитель мог ощутить, как автомобиль и окружающая инфраструктура, оснащенные множеством датчиков, взаимодействуя друг с другом по беспроводной технологии 5G, позволяют автомобилю своевременно реагировать на изменяющиеся дорожные условия, пересекать бесветофорные перекрестки, совершать автоматический обгон и т. д. «5G как технология сетей будущего обеспечит подключение в любом месте, в любое время, в движении, практически с нулевыми задержками и безграничными возможностями применения. Для этого потребуются усилия всей экосистемы, включая операторов, производителей оборудования и промышленных партнеров. Huawei активно сотрудничает с игроками отрасли в области разработки и совершенствования технологии 5G, создания новых сценариев применения, бизнес-сценариев для ускорения промышленной и социальной трансформации», – говорит Эйден У, генеральный директор компании Huawei в России. Сети пятого поколения позволят реализовать сервисы, способные повысить конкурентоспособность всей экономики страны.

<http://www.megafon.ru>

## «Детский мир» инвестирует в развитие проектов SAP

SAP и Группа компаний «Детский мир», крупнейший оператор торговли детскими товарами в России, подписали меморандум о долгосрочном стратегическом партнерстве. В ближайшие несколько лет инвестиции ритейлера составят 260 млн руб. Соглашение предусматривает новый этап развития существующей ERP и аналитической системы, платформы для электронной коммерции, централизацию поставок через собственный распределительный центр (РЦ) в Московской области, а также перевод поставщиков РЦ на электронный документооборот. Совместный проект SAP и «Детского мира» начался четыре года назад. За это время компании проделали большую работу: по результатам предыдущего этапа в 2016 г. рост розничной сети и эффективность сотрудников увеличились вдвое, также более чем двукратно возросло количество строк, ежедневно обрабатываемых на складе компании. Число обслуживаемых магазинов с 2014 по 2016 г. увеличилось с 272 до 480. С 2013 г. доля коммерческих, общехозяйственных и административных расходов в проценте от выручки уменьшилась с 31 до 23,7% благодаря повышению операционной эффективности и сокращению расходов. «Мы сотрудничаем с SAP с 2013 г. и уже успели многого достичь: построили

единое информационное пространство, внедрили новые информационные системы для оптимизации коммерческих, административных и управленческих расходов. В марте 2017 г. мы успешно завершили проект по внедрению e-commerce платформы SAP Hybris, запустив на ней все регионы. С 2016 г. наши онлайн-продажи увеличились вдвое», – прокомментировал Владимир Чирахов, генеральный директор Группы компаний «Детский мир». Ранее в «Детском мире» были внедрены модули SAP ERP (управление ассортиментом, финансы и бухгалтерия, операции в магазинах, ценообразование, автозаказ товара), SAP Business Warehouse on HANA (бизнес-аналитика), SAP Extended Warehouse Management (логистика). «Детский мир» – компания, которая находится в постоянном поиске новых форматов общения со своими, – отметил Павел Гонгарев, генеральный директор SAP СНГ. – Электронная коммерция сегодня – один из самых быстрорастущих сегментов мировой экономики. С помощью SAP Hybris «Детский мир» ведет качественное персонализированное взаимодействие с клиентами по всем доступным каналам, собирает данные о покупателях из разных источников, анализирует их активность».

[www.sap.com](http://www.sap.com) [www.sap.ru](http://www.sap.ru)

# Российская отрасль СУБД продвигается на «слонах»

Отечественные разработки в сфере программного обеспечения привлекли к себе особое внимание три года назад, когда страна взяла курс на импортозамещение. В поддержку отечественного ПО вышел целый ряд законодательных инициатив. Что происходит на рынке российских СУБД? Достижимы ли цели программы развития отечественного программного обеспечения? С какими трудностями сталкиваются российские разработчики? Каким требованиям должна отвечать СУБД для обеспечения технологической независимости России?

## Реестр и другие законодательные инициативы

Среди законодательных инициатив прежде всего следует отметить Федеральный закон № 188-ФЗ от 29 июня 2015 г. «О предоставлении преференций российским разработчикам ПО при госзакупках». Во исполнение закона подписано постановление Правительства № 1236 от 16 ноября 2015 г. «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

С января 2016 г. при Минкомсвязи ведется Единый реестр отечественного ПО, куда в настоящее время входит свыше 3300 программных продуктов. Все это позволяет надеяться на позитивные изменения, по крайней мере на увеличение доли отечественного ПО в государственных информационных системах.

Между тем необходимость обеспечения технологической независимости страны в сфере информационно-коммуникационных технологий возникла гораздо раньше, чем обстоятельства подтолкнули к стратегии импортозамещения. В первую очередь это касается таких ключевых сегментов, как системы управления базами данных, операционные

системы, системы автоматизированного проектирования. В период становления в нашей стране рыночной экономики зарубежные продукты без труда обосновались на российском рынке ПО. Сильные позиции удалось сохранить в области информационной безопасности, информационно-поисковых систем, социальных сетей и систем машинного обучения. Однако другие важные направления просели, несмотря на хороший задел, оставленный советской инженерной школой. Так, в 1991 г. состоялась последняя научная конференция по технологиям баз данных, при СССР проходившая ежегодно. На ней было сделано более 200 докладов. Спустя несколько лет почти никого из специалистов не удалось собрать снова.

В апреле 2011 г. Правительственная комиссия по высоким технологиям и инновациям утвердила перечень технологических платформ, в который вошла и национальная программная платформа. Предполагалось, что результатом программы станет разработка стека отечественных технологий по десяти категориям, включая операционные системы, СУБД, САПР и пр. Объем финансирования должен был составить 490 млн руб. до конца 2012 г. Применение разработки должны были найти в первую очередь в государственных системах для обеспечения независимости государства от западных поставщиков

проприетарных решений и безопасности критически важных систем.

Почти сразу началось обсуждение технологии баз данных, которая может быть положена в основу национальной СУБД. Если для операционной системы и офисных пакетов была поставлена задача использовать свободное ПО с открытым кодом, в частности на основе Linux, то в отношении СУБД однозначного решения не было, и проприетарные программные продукты рассматривались наравне с открытыми.

В то время лидирующие позиции на российском рынке СУБД занимали продукты западных корпораций – Oracle Database, MS SQL Server и IBM DB2. Из конкурентоспособных продуктов с открытым кодом, развиваемых международным сообществом, наибольшую популярность получили PostgreSQL, MySQL и Firebird. В следующие два года появились такие российские СУБД, как «Линтер 6.0 Бастион» (2011 г., РЕЛЭКС) и «Заря» (2012 г., ФГУП ЦНИИ ЭИСУ). В основу СУБД «Заря», а также СУБД, поставляемой в российских ОС Alt Linux СПТ 6.0 (2011 г., ALT Linux) и Astra Linux Special Edition (2012 г., НПО «РусБИТех»), положены различные версии системы с открытым кодом PostgreSQL. В 2015 г. компания Postgres Professional, российский вендор PostgreSQL, выпустила свободную, сертифицированную для коммерческой версии СУБД Postgres Pro. На основе открытой

СУБД Firebird компания «Ред Софт» создала СУБД «Ред База Данных», последний релиз которой состоялся в 2016 г. Популярная СУБД MySQL с открытым кодом, как и ее ответвление MariaDB, не представлены на рынке российскими производителями.

По данным на май 2017 г. в Единый реестр российских программ для электронных вычислительных машин и баз данных входят СУБД «Ред База Данных», «Линтер Бастион», Postgres Pro, а также несколько значительно уступающих по популярности систем (Odant, «Синтез», «Циркон», HyTech, ARL, M10) и платформ. Из недавних, но уже нашумевших российских разработок СУБД, пока не включенных в реестр, стоит упомянуть NoSQL Tarantool от группы компаний Mail.ru и ClickHouse от «Яндекса». Они рассчитаны на решение отдельных вопросов, но заменить СУБД общего назначения пока не могут.

## Требования к СУБД в контексте технологической независимости

Рассмотрим требования, которым должна отвечать СУБД для обеспечения технологической независимости России, и оценим, насколько имеющиеся на рынке технологии им соответствуют.

### Высокая функциональность и расширяемость СУБД

Этот критерий выявляет преимущества открытых систем перед проприетарными разработками СУБД с нуля. История показывает, что создание полнофункциональной системы управления базами данных может занять десятки лет и требует привлечения большой команды квалифицированных разработчиков. Попытка равняться на возможности таких ИТ-гигантов, как Oracle, Microsoft и IBM, занимающихся разработкой СУБД более 30 лет и имеющих бюджеты, сравнимые с ВВП некоторых государств, означает не только неизбежные огромные

финансовые и трудовые инвестиции, но и заранее ставит российскую отрасль СУБД в догоняющую позицию.

Если оценивать наличие в России достаточного количества квалифицированных кадров для разработки функциональной СУБД, то ситуация выглядит неутешительно. Многие компетенции для страны были потеряны в 1990-е гг. вместе с разработчиками старой школы. А анализ образовательных программ ведущих вузов

международного сообщества разработчиков. В России оно составляет примерно полторы тысячи человек. Это напрямую коррелирует с частотой выхода обновлений и расширений системы. Сообщество разработчиков открытой СУБД Firebird на порядок меньше. Впрочем, вернемся к сравнению основных функциональных возможностей российских СУБД.

Расширяемость СУБД зависит от того, насколько сама архитектура

---

## В плане изначально заложенной гибкости PostgreSQL может дать фору коммерческим решениям.

---

показывает, что сейчас они ориентированы на подготовку администраторов СУБД, но не разработчиков. В первую очередь администраторов для Oracle Database, MS SQL Server и IBM DB2, которые вкладывают немалые ресурсы в поддержку профильных специальностей. Но без глубокого понимания языка SQL и технологий баз данных невозможно научиться самостоятельной разработке алгоритмов, расширяющих возможности СУБД и создающих ее функциональность.

По этой причине системы с открытым кодом и свободной лицензией, поддерживаемые международным сообществом, открывают шанс сделать ход конем: взять за основу готовую СУБД, добавить национальные компетенции и адаптировать продукт для российских условий. По такому пути идут и многие другие страны. В частности, с 2009 г. Франция решила использовать открытый PostgreSQL в государственных информационных системах, таких как Национальный фонд семейных пособий и Национальная метеослужба. Из открытых систем СУБД PostgreSQL обладает преимуществом самого развитого

СУБД позволяет добавлять новые возможности, не переписывая огромных объемов кода. В плане изначально заложенной гибкости PostgreSQL может дать фору коммерческим решениям: СУБД позволяет дописывать свои расширения и функции, даже проводить доработку ядра, которая, в случае принятия сообществом, сможет войти в стандартную версию. Последнее относится и к СУБД Firebird. С другой стороны, для закрытой сертифицированной системы расширяемость не столь полезна: при внесении любых изменений необходима дополнительная сертификация. Поэтому для СУБД «Линтер Бастион», «Заря», Astra Linux Special Edition, которые ориентированы на нишу специальных и закрытых применений, расширяемость и следование последним достижениям технологий баз данных не столь приоритетны. В дистрибутив СУБД «Заря» и «Астра Линукс» входят версии СУБД PostgreSQL, доработанные с точки зрения безопасности, но практически не влияющие на расширение функционала по сравнению с открытой версией, за исключением проверки контрольных сумм для контроля целостности.

СУБД Postgres Pro основана на последней версии PostgreSQL 9.6.3. Доработки функциональности в Postgres Pro значительны. В Postgres Pro Standard доступны физическая и логическая синхронная и асинхронные репликации. В коммерческой версии Postgres Pro Enterprise присутствуют логическая синхронная репликация с изоляцией транзакции на уровне кластера серверов, адаптивное планирование запросов, компрессия данных на уровне блоков, 64-битный счетчик транзакций и эффективное секционирование таблиц.

В текущей версии «Линтер Бастион 6.0» реализована только асинхронная репликация. По сравнению с PostgreSQL он уступает в максимальном размере записи

пространственного типа данных и пр.

СУБД ClickHouse предназначена прежде всего для эффективной аналитики больших данных (OLAP). Архитектура изначально ориентирована на распределенные вычисления и обеспечивает быстроту обработки больших объемов информации (петабайты данных). Однако при этом ClickHouse не гарантирует таких важных для транзакционных СУБД свойств, как ACID (atomicity, consistency, isolation, durability – атомарность, согласованность, изоляция, долговечность хранения). В ClickHouse поддерживается подмножество языка SQL, которое далеко от полноты универсальных реляционных СУБД. Таким образом, ClickHouse хороша и может рассчитывать на успех

к полнофункциональной реляционной системе с ее механизмами контроля целостности неминусом скажется на основном преимуществе Tarantool – высочайшей производительности.

#### **Наличие пула отечественных разработчиков, владеющих исходным кодом СУБД, способных развивать и сопровождать систему**

Системы с открытым кодом формально нельзя отнести к продукту российских разработчиков, так как участие в их развитии принимает международное сообщество, т. е. люди из разных стран. Однако при определенных условиях, когда вклад и влияние именно российских разработчиков достаточно велики, можно не только говорить о контроле кода с российской стороны, но и отметить фактор большей устойчивости продукта: в отличие от проприетарных разработок открытым системам не грозит быть выключенными из оборота по воле одного хозяйственного субъекта или в силу политической конъюнктуры. Таким образом, компетенции разработчиков открытых СУБД не ограничены рамками компании, владеющей исходным кодом, и специалисты могут активно использовать наработки международного сообщества, а также продвигать собственные улучшения кода, что в достаточной мере гарантирует воспроизводимость национальных компетенций.

Российские системы на основе открытой СУБД PostgreSQL являются собой яркий пример. Вклад отечественных разработчиков в развитие PostgreSQL с самого начала был значимым и сейчас оценивается до одной трети кода проекта. Вадим Михеев из Красноярска – один из первых разработчиков PostgreSQL, автор таких ключевых частей СУБД, как многоверсионное управление одновременным доступом, на которой базируются управление транзакциями и поддержка целостности данных, система очистки, журнал транзакций, вложенные запросы и триггеры. Среди основателей

## Tarantool быстро развивается, приобретая черты универсальной СУБД.

(64 кБ против 1,6 ТБ), размере поля (4 кБ против 1Гб) и количестве ключей в таблице (250 против 1600). Поддерживается меньшее разнообразие типов индексов, что влияет на скорость поиска данных. Как и в PostgreSQL, в «Линтер Бастион 6.0» доступен пространственный тип данных, реализован полнотекстовый поиск, поддерживается формат данных JSON.

В «Ред База Данных» есть логическая синхронная и асинхронная репликация на уровне ядра. От Firebird унаследовано, пожалуй, главное преимущество – консистентное состояние базы данных на диске в любой момент времени. Благодаря этому система получила распространение как СУБД для встраиваемых систем, кассовых аппаратов и пр. По базовому функционалу «Ред База Данных» уступает PostgreSQL и его производным: ниже уровень поддержки стандартов SQL, нет

только в той области применения, для которой она создана.

Нереляционная СУБД Tarantool ориентирована на обработку в памяти больших объемов таблиц ключ-значение, без транзакций и ACID. Однако поверх Tarantool работает сервер приложений, с помощью которого можно эмулировать реляционность, поддержку SQL и обеспечить ACID. В Tarantool появились дисковое хранение, журнал упреждающей записи, асинхронная репликация в режимах master-slave и master-master. Таким образом, Tarantool быстро развивается, приобретая черты универсальной СУБД. В то же время широкому распространению будут препятствовать экзотичность процедурного языка Lua и отсутствие значимой истории эксплуатации на реальных проектах в качестве универсальной СУБД. А главное, переход от нишевой NoSQL СУБД

компании Postgres Professional, российского вендора PostgreSQL, три ведущих разработчика проекта в международном статусе major contributor – Олег Бартунов, Федор Сигаев и Александр Коротков. В списке их заслуг: локализация PostgreSQL, создание системы полнотекстового поиска и работы со слабоструктурированными данными (hstore, json, jsonb), а также новые методы индексации (GiST, GIN, SP-GiST). О масштабе российского сообщества можно судить и по размаху технической конференции PgConf Russia, ежегодно собирающей в Москве более 500 участников и ставшей одной из крупнейших в мире по тематике PostgreSQL. Ни одна другая российская СУБД пока не может сравниться по степени вовлеченности в разработку.

#### **Реализация в России полного цикла поддержки СУБД, включая разработку, техническую поддержку и обучение пользователей**

Одним из условий признания программного продукта российским должна быть организация на территории России полного цикла поддержки и разработки. И это правильно, поскольку для серьезных задач недостаточно грамотно установить ПО: российским компаниям необходимо иметь возможность оперативно решить проблемы, если они возникнут, и получить профессиональную техническую поддержку.

Вопрос вендорской поддержки часто становится камнем преткновения при выборе свободного ПО, в частности, для разработчиков прикладных систем на основе open source, которые в таком случае вынуждены брать на себя функцию поддержки ПО, которое они не создавали. Для PostgreSQL эта проблема решена в 2015 г. созданием компании Postgres Professional, взявшей на себя миссию российского вендора СУБД PostgreSQL. Теперь пользователям доступны техническая поддержка в режиме 24×7, документация на русском языке, обучающие

курсы, профессиональные консультации по вопросам миграции на PostgreSQL, разработка расширений и дополнений.

Подробная документация на русском языке имеется также у «Линтер Бастион», «Астра Линукс», Alt Linux и «Ред База Данных». СУБД ClickHouse и Tarantool документацией на русском языке пока не обзавелись. Перечисленные СУБД лишь частично решили вопрос с организацией обучения пользователей и технической поддержкой в формате 24×7.

и ФСТЭК России на соответствие третьему классу защищенности от несанкционированного доступа (НСД) и второму уровню контроля отсутствия недеklarированных возможностей (НДВ). В состав сертифицированного дистрибутива входит СУБД PostgreSQL 9.3.3 с дополнительными средствами защиты информации, обеспечивающими мандатное разграничение доступа и регистрацию событий безопасности.

СУБД «Линтер Бастион 6.0» прошла сертификацию в Мини-

---

## Министерство обороны РФ является и основным пользователем СУБД «Заря».

---

#### **Возможность сертификации по требованиям ФСТЭК России**

Для государственных информационных систем, информационных систем персональных данных, АСУТП и критически важных систем необходимы защищенные системы управления базами данных, сертифицированные по требованиям ФСТЭК России. СУБД, претендующая на роль гаранта технологической независимости, должна обладать сертификатом соответствия и входить в Единый реестр российских программ для электронных вычислительных машин и баз данных. На практике треугольник «функциональность – безопасность – производительность» не позволяет без сверхзатрат создать систему, отвечающую всем трем критериям, и разработчикам приходится идти на компромиссы. Для специальных систем этот компромисс обычно выглядит как «функциональность + безопасность».

Операционная система специального назначения Astra Linux Special Edition изначально была разработана с прицелом на защищенность. Она получила сертификаты Министерства обороны, ФСБ

стерстве обороны (по третьему классу защищенности от НСД и второму уровню контроля отсутствия НДВ) и ФСТЭК России (по второму классу защищенности от НСД и второму уровню контроля отсутствия НДВ). Многоуровневая защита позволяет строить информационные системы, в частности, предназначенные для обработки и хранения секретной информации. Отсюда и основные заказчики системы – подразделения Министерства обороны РФ, Министерства внутренних дел РФ, силовые структуры.

СУБД «Заря» обладает сертификатом Министерства обороны и предназначена для обработки и хранения информации, составляющей государственную тайну не выше уровня «совершенно секретно». Министерство обороны РФ является и основным пользователем данной СУБД. Дистрибутив «Альт Линукс» СПТ 7.0 сертифицирован ФСТЭК России (по четвертому классу защищенности от НСД и третьему уровню контроля отсутствия НДВ).

СУБД Postgres Pro Certified сертифицирована по требованиям ФСТЭК России (по пятому классу

защищенности от НСД и четвертому уровню контроля отсутствия НДВ) и может применяться для защиты информации, не составляющей государственную тайну, в государственных информационных системах и автоматизированных системах управления до первого класса защищенности, а также для обеспечения до первого уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 1-го, 2-го или 3-го типа. В дополнение к штатному механизму поддержки

Вопросы безопасности систем с открытым кодом можно трактовать по-разному. С одной стороны, разработки с закрытым кодом менее уязвимы с точки зрения изучения злоумышленниками их слабых мест. С другой стороны, СУБД на основе открытого кода регулярно исправляют все найденные ошибки и уязвимости и выпускают необходимые обновления гораздо более оперативно – в PostgreSQL это происходит практически ежеквартально. Возможность внести «закладку» в открытую систему с развитым сообществом также

операционных систем ОС «Заря» и ОС «Заря-ЦОД» на аппаратных платформах x86-64, POWER7, IBM System z. «Ред База Данных» работает на основных версиях Windows, семействе Linux, BSD Unix, IBM AIX, HP-UX, Sun Solaris, 32-битных и 64-битных аппаратных платформах. PostgreSQL Pro имеет сборки под различные платформы, в том числе Windows, Linux, CentOS, ROSA, Alt Linux, MCBC, Alt Linux, Debian, Ubuntu, SUSE Linux Enterprise Server. Поддерживается ARM.

Таким образом, по совокупности критериев можно сделать следующие выводы о российской отрасли СУБД. Наибольшим потенциалом среди СУБД общего назначения обладает PostgreSQL, которая способна обеспечить высокую функциональность и расширяемость системы, профессиональную поддержку пользователей и безопасность. Остальные разработки занимают хорошие позиции в собственных нишах – защищенных СУБД специального назначения, системах реального времени, встроенных приложениях. В 2015 г. консорциум во главе с PostgreSQL Professional победил на конкурсе проектов по импортозамещению инфраструктурного программного обеспечения Минкомсвязи России в номинации «Системы управления базами данных». И хотя по результатам финансирования не было выделено и реальная поддержка данного направления пока невелика, все больше государственных структур (правительство Москвы и Московской области, ФНС, «Росакредитация») и крупных российских компаний (Сбербанк, «Яндекс», «Ростех») выбирают именно эту СУБД, мигрируя с зарубежных решений. Это лучшее свидетельство того, что у отечественной отрасли СУБД есть будущее, и «слоны»\* в его приближении играют заметную роль своей поступью. ■

*Благодарим за помощь в подготовке материала компанию PostgreSQL Professional*

## Наибольшим потенциалом среди СУБД общего назначения обладает PostgreSQL.

безопасности на уровне строк, имеющемуся в СУБД PostgreSQL Pro, в сертифицированной версии реализованы встроенные средства защиты от несанкционированного доступа к информации, включая очистку оперативной и дисковой памяти, встроенный контроль целостности исполняемых файлов, конфигурационных файлов и таблиц системного каталога.

СУБД «Ред База Данных» также дорабатывалась с учетом требований безопасности: реализован мандатный доступ, который на уровне операционной системы поддерживается доработками в подсистемах безопасности SELinux и SELinux Reference Policy. «Ред База Данных» сертифицирована ФСТЭК России и может использоваться при создании информационных систем до класса защищенности 1Г включительно и при создании информационных систем персональных данных до 1-го класса включительно. Исходный код этой системы открыт в отличие от других сертифицированных СУБД.

маловероятна – все дополнения проходят независимую многоступенчатую проверку, перед тем как будут приняты в основную ветку. Поэтому безопасность открытых СУБД на уровне универсального применения не является камнем преткновения, а для специальных применений решается выпуском сертифицированных версий.

### Поддержка спектра аппаратных платформ и операционных систем

СУБД «Линтер Бастион» обладает широкой базой операционных систем, на которые она может быть установлена: семейство Unix/Linux (в том числе «Эльбрус», защищенные Astra Linux, «РОСА» и «MCBC»); 32-битные Windows и 64-битные WindowsNT, WinCE; Android; z/OS для мэйнфреймов; ряд ОС реального времени (QNX, VxWorks) и др. «Астра Линукс» функционирует на платформе x86-64 и предназначена для одноименной ОС Astra Linux Special Edition. СУБД «Заря» работает под управлением

\* Логотипом СУБД PostgreSQL является слон. Считается, что слоны обладают хорошей памятью и на протяжении жизни помнят все.



## Систему «Безопасный регион» построят в Астрахани

«Ростелеком» совместно с компанией «ЭйТи Сервис», входящей в группу AT Consulting, внедряет в Астрахани элементы системы безопасности «Безопасный регион». До конца 2017 г. на территории Астраханской области появится новая система безопасности дорожного движения.

Внедрение подобных решений позволяет сократить на 25% общее число ДТП и на 44% количество аварий с летальным исходом. В рамках проекта планируется развернуть новые комплексы фото- и видеофиксации нарушений ПДД, провести модернизацию существующих, смонтировать пункты весогабаритного контроля, а также объединить комплексы в систему контроля и наблюдения. Для этого

в Астрахани будет создан новый центр мониторинга, куда будут поступать данные с комплексов фиксации нарушений ПДД и весогабаритного контроля. Специалисты компании AT Consulting, выступающей на проекте генеральным подрядчиком, провели анализ наиболее опасных участков автомобильных дорог в целях размещения новых комплексов. Что касается существующих, то некоторые объекты устарели или пришли в негодность. В результате было



определено 75 комплексов, которые планируется модернизировать. Подготовительные работы завершены. Сдана проектная документация 16 комплексов фото- и видеофиксации нарушений скоростного режима и выезда на встреч-

ную полосу, 23 комплексов, ведущих наблюдение за соблюдением правил дорожного движения на перекрестках, пяти комплексов контроля нарушений парковки и четырех комплексов, которые планируется установить на железнодорожных переездах. Места размещения камер выбраны на основе анализа аварийности и с учетом повышения безопасности дорожной сети региона, согласованы с УМВД России по Астраханской области. В список работ также

включено развертывание пяти автоматических пунктов весогабаритного контроля транспортных средств на дорогах регионального значения. Установка таких систем позволит повысить безопасность, сократить издержки на ремонт дорожного полотна, наладить систему эффективного контроля и выявления нарушений перевозок крупногабаритных и тяжеловесных грузов.

[www.at-consulting.ru](http://www.at-consulting.ru)

## NetApp улучшает масштабирование StorageGRID Webscale

Компания NetApp представила новую версию своего программного обеспечения StorageGRID Webscale следующего поколения для объектного хранения данных. Она дает возможность предприятиям контролировать данные с богатым информационным наполнением и ускорить переход на цифровые технологии.

«Стремительный рост объемов и разнообразия цифровой информации усложняет управление данными для предприятий с большой географической распределенностью, а также для сервис-провайдеров, — отметил Амига Потнис (Amita Potnis), менеджер IDC по исследованиям. — NetApp StorageGRID Webscale — простое в развертывании масштабируемое решение, которое поможет пользователям создать необходимую инфраструктуру для поддержки массивного роста объемов как структурированных, так и неструктурированных данных».

Теперь StorageGRID Webscale предлагает: дополнительные варианты развертывания ПО, включая поддержку контейнера Docker и возможность установки

непосредственно на выделенных серверах; упрощенное развертывание систем хранения данных для OpenStack; управление многопользовательской системой с возможностью мониторинга и контроля за распределением мощностей между пользователями; сертификацию Veritas Enterprise Vault для централизации управления данными в электронной почте, файловой системе, социальных сетях и многое другое.

«Уникальные возможности, которыми обладает NetApp, позволяют нам помочь трансформировать бизнес наших заказчиков, сделав данные движущей силой его развития, — говорит Клеменс Зиблер (Clemens Siebler), директор NetApp по архитектуре программных решений в регионе EMEA. — StorageGRID Webscale предлагает архитектуру хранения нового поколения, помогающую заказчикам легко создавать огромные масштабируемые озера данных для организации архивов, аналитики и хранения мультимедийных данных как в географически распределенных ЦОД, так и в публичном облаке».

# О замещении иностранного ПО в инженерных проектах



**Сергей АВТОМАНОВ,**  
ведущий инженер, ФГУП «ГосНИИАС»

## Особенности иностранного ПО для инженерной разработки в России

Во времена СССР разработка авиационной техники шла от развития прототипов и выполнения экспериментов на стендах и в испытательных полетах. Не было каких-либо серьезных отставаний от иностранных разработок технических комплексов и систем автоматизированного проектирования. Гармоничное развитие технологии разработки сложной техники нарушилось с распадом СССР и крахом плановой экономики.

Применяемое в настоящее время ПО инженерной разработки можно сегментировать по позиции в процессе разработки:

- ПО обработки требований;
- ПО в составе САПР или среды кодирования ПО;



**Александр ПОПОВ,**  
ведущий инженер, ФГУП «ГосНИИАС»

- ПО моделирования и инженерного анализа;
- ПО коллективной работы и делопроизводства.

ПО обработки требований вошло в практику российских предприятий в 1990-е и нулевые годы в проектах с иностранными компаниями. Тогда же начался перевод на русский язык иностранных стандартов и терминологии, используемых в иностранной технологии инженерного проектирования. В настоящее время может использоваться только автономно в качестве редактора файлов с коллекциями требований, представляющих собой строки авторского текста с присоединенными к ним таблицами атрибутов. Для обмена этими файлами применяется протокол ReqIF, а для контроля изменений в требованиях (т. е. в файлах) применяют специальное ПО.

Для разработки печатных плат, электронных схем и конструкций

Статья знакомит со свежим примером подготовки к замещению иностранного ПО, много лет применяемого в России для проектирования воздушных судов и бортовой электроники, критичных в смысле безопасности. В статье обсуждаются особенности иностранного ПО, необходимость и принципы его замещения, требования к российскому ПО, заменяющему импорт.

блоков аппаратуры вычислителей и коммуникаций (силовых и цифровых; жгутов и проводов), как правило, применяют иностранные САПР (CATIA, NX, Solid Edge, AutoCAD, etc). Отечественные САПР (T-Flex, FlowVision, Нанософт и др.) следуют концепции иностранных с отставанием на годы.

Для моделирования и инженерного анализа (расчеты динамики конструкций и систем, прочности, тепловых потоков и электромагнитных полей, технической и системной надежности и т. п.) используется как иностранное (ANSYS, Femap, etc), так и российское ПО (компании АССОНИКА, SimInTech, Тесис, Тор, Ангстрем).

В сегменте «ПО коллективной работы и делопроизводства» присутствуют не только ПО управления проектами (работами и ресурсами), но и ПО инженерного делопроизводства, включая архив документации (в концепции PLM), сопровождающее жизненный цикл изделий. Здесь господствует

иностранное ПО от компаний IBM, Siemens, Dasso Systems.

В свободном доступе отсутствуют сведения о том, какую в действительности сквозную технологию разработки самолетов и бортовых систем применяют компании Dasso Aviation, Boeing, Airbus, Snecma, Sagem, Thales, Collins. Нам доступны для изучения лишь отдельные компоненты ПО предполагаемой иностранной сквозной технологии разработки.

Представленное в России иностранное ПО инженерной разработки не может дать примера сквозной технологии разработки бортового оборудования – систем, блоков, микроэлектроники, ПО, устройств коммуникаций – даже на уровне отдельного предприятия. Потребуется многолетняя кропотливая разработка недостающего ПО и его интеграция в инфраструктуру. Так и происходит на развивающемся российском предприятии. Каждое российское предприятие приборостроения вынуждено создавать свою сквозную технологию разработки.

## Перспективы иностранного ПО инженерной разработки

В перспективе ПО для инженерной разработки продолжит развиваться в рамках концепции параллельного существования реального и виртуального мира, т. е. в центре внимания останется моделирование реальных предметов и процессов на протяжении всего срока жизни разрабатываемого изделия электроники и электротехники.

В период 2004–2016 гг. в Евросоюзе по программе F7 выполнены ряд НИР для решения проблем на пути создания общей платформы (среды) сквозной технологии разработки высоконадежных и безопасных электронных систем автомобильного, авиационного и железнодорожного транспорта. Например, это НИР:

- Artemis, Crystal-Artemis, 163 млн евро, 2004–2017;
- OPENCROSS (open platform for evolutionary certification

of safety-critical systems), 12 млн евро, 2011–2015, www.opencross-project.eu;

- Verisoft XT, 2007–2010, verisoftxt.de/;
- COMPASS (comprehensive modelling for advanced SoS, UK), 2012–2020;
- DANSE (designing for adaptation and evolution in SoS engineering, DE), 2012;
- T-AREA-SoS (trans-atlantic research and education agenda on SoS, UK), 2012;
- Age-Sys (systems engineering workshop), 2012.

Общий недостаток этих НИР – неявный отказ от построения инструментальной среды разработки с общим для всех систем хранилищем в пользу варианта интеграции ПО информационных систем и баз данных, созданных автономно (см. рис. 1).

Поэтому для интеграции ПО пары информационных систем и баз данных нужны два конвертора формата передаваемых данных, которые при каждом случае изменений нуждаются в модернизации (проектирование, изготовление и тестирование). На это требуются время и деньги.

Можно предполагать, что в проектах программы F7 и других программ Евросоюза будут созданы единые стандарты форматов представления данных для цифровой разработки бортовой электроники автомобильного, авиационного и железнодорожного транспорта. Это кратно снизило бы затраты на интеграцию такого ПО в среду разработки электроники на каждом предприятии. Но единой среды

разработки электроники в Евросоюзе не будет.

## Необходимость замещения иностранного ПО

Проблемы низкой эффективности применения иностранного ПО в российской радиоэлектронной промышленности:

- на предприятия поставляются отдельные программные продукты, но никогда не поставляются комплексные решения масштаба предприятия, ни ПО среды разработки электроники;
- отсутствует единая государственная политика создания и распространения на предприятиях радиоэлектронной промышленности ПО типовой среды разработки электроники (российские САПР и среда поддержки САПР).

Российские ИКТ-компании страдают от недостатка заказов внутри экономики России и вынуждены заниматься обслуживанием развития чужих экономик, в том числе явных врагов России. Доля импорта ПО категорий PLM, CAD, CAM, CAE в 2014 г. превысила 88% [1]. Это можно оценить как подавляющую зависимость российских предприятий от политики иностранных разработчиков.

Российский рынок ПО открыт для российских же компаний, что вызвано следующими обстоятельствами:

- иностранное ПО, закупленное российскими предприятиями, часто поддерживает только

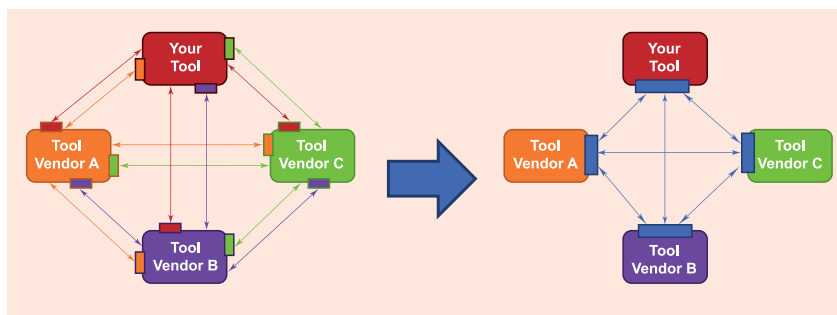


Рисунок 1. Цель проекта Crystal - создание типовой технологической платформы (Reference Technology Platform, RTP) в качестве европейского стандарта технического решения для совместимости информационных систем в процессах проектирования и других фаз жизненного цикла критически важных систем авионики.

собственные протоколы обмена моделями, а всем в мире открытые кросс-платформенные протоколы (например, DWF, JT, 3DPDF, STEP) недоступны для российских разработчиков ПО;

- лобби иностранного ПО в учреждениях российского государства, корпорациях и крупных предприятиях содействуют перераспределению заказов на ПО в пользу иностранных разработчиков и поставщиков ПО.

Эксплуатация иностранного ПО обходится российским предприятиям очень дорого (цена годовой лицензий порядка 10 тыс. долларов за место).

Функциональность иностранного ПО, продаваемого в России, искусственно ограничена некоторыми изготовителями ПО. Информационная интеграция и системная поддержка жизненного цикла продукции включены в качестве перспективного направления науки и техники в перечень критических технологий Российской Федерации [2].

Иностранное ПО категорий PLM, CAD, CAM, CAE распространяется в России как проприетарное. У пользователей ПО нет уверенности, что его программный код не имеет недекларированных возможностей и ограничений на применение.

Электроника, созданная с применением иностранного ПО в категориях PLM, CAD, CAM, CAE, может быть источником опасности при установке в блоках управления автомобильным, авиационным и железнодорожным транспортным средством.

В стратегии экономической безопасности Российской Федерации [3] определены основные угрозы и вызовы:

- «стремление развитых государств использовать свое преимущество в уровне развития экономики, высоких технологий (в том числе информационных) в качестве инструмента глобальной конкуренции» (п. 12.1 [3]);
- «использование дискриминационных мер в отношении ключевых секторов экономики Российской Федерации, ограничение доступа к... современным технологиям» (п. 12.3 [3]);

и поставлены задачи:

- «обеспечение безопасности экономической деятельности» (п. 15.7 [3]);
- «преодоление критической зависимости от импортных поставок программных средств...» (п. 18 [3]).

В рамках санкций, объявленных нам США и странами Евросоюза, прекращены продажи некоторого чувствительного для российских предприятий ПО и обслуживание ранее проданного такого ПО [4].

## Принципы замещения иностранного ПО

1. Замещение импорта должно быть не заменой один в один, оно должно быть выходом на качественно новый уровень развития технологий инженерной разработки [5].
2. Импортное ПО категории PLM должно быть замещено общей для российского приборостроения информационной инфраструктурой, объединяющей российское и иностранное ПО категорий PLM, CAD, CAM, CAE.
3. Замещение иностранного ПО категорий PLM, CAD, CAM, CAE должно сопровождаться преобразованием российской и иностранной нормативной базы для компьютерной обработки и применения для сертификации результатов разработки, в том числе в иностранных специализированных органах.
4. Замещение иностранного ПО категорий PLM, CAD, CAM, CAE должно быть «мягким», т. е. допускать совместное применение российского и аналогичного по функционалу иностранного ПО, не требуя от предприятия делать выбор между иностранным и отечественным ПО.
5. Иностранное проприетарное ПО должно замещаться российским ПО, созданным на принципах открытого свободного ПО без встроенных частей проприетарного кода или ссылок на него.
6. ПО на замену импорта должно гарантировать независимым

разработчикам участие в развитии его функций, интерфейса и области применения.

## Принципы устройства российского ПО на замену импорта

Для выхода предприятий российского приборостроения на качественно новый уровень развития нужна общая для всех сквозная технология разработки бортовых систем (ПО, блоков электроники, цифровых и силовых коммуникаций), построенная как «живая» система (т. е. можно изменять в момент применения без ограничения срока).

ПО на замену импорта должно использовать только открытые стандарты протоколов обмена данными и моделями (например, AADL, etc.) с внешними системами категорий PLM, CAD, CAM, CAE.

ПО на замену импорта должно иметь внутренний язык описания современных и будущих метамodelей изделий бортовой электроники и процессов их разработки и управления. ■

### Литература

1. 1. Приложение к приказу Министерства связи и массовых коммуникаций Российской Федерации от 01.04.2015 № 96.
2. Перечень критических технологий Российской Федерации утвержден Президентом Российской Федерации 21 мая 2006 года № 842.
3. Указ Президента Российской Федерации 13 мая 2017 года № 208 «Стратегия экономической безопасности Российской Федерации на период до 2030 года».
4. «Ангстрем» и «Микрон» попали под американские санкции – [d-russia.ru/angstrom-i-mikron-popali-pod-amerikanskie-sankcii.html](http://d-russia.ru/angstrom-i-mikron-popali-pod-amerikanskie-sankcii.html)
5. Мысль Г.И. Джангава (президент ПАО «Раменское ПКБ», д. т. н.) – [vpk.name/news/151136\\_givi\\_dzhandzhgava\\_importozameshenie\\_dolzno\\_stat\\_vnedreniem\\_novyih\\_tehnologii.html](http://vpk.name/news/151136_givi_dzhandzhgava_importozameshenie_dolzno_stat_vnedreniem_novyih_tehnologii.html)

## Cisco выпустила решение для защиты IoT

По прогнозам компании Cisco, к 2020 г. будут функционировать до 50 млрд подключенных устройств, что означает достижение критической массы в процессе реализации потенциала IoT. Решение Cisco IoT Threat Defense помогает сохранить этот потенциал и минимизировать риски. IoT Threat Defense – обширное архитектурно-сервисное решение, которое обеспечивает адаптируемую, наращиваемую защиту организаций в масштабе Интернета вещей с помощью сегментирования устройств в сети. Первое направление применения IoT Threat Defense – защита жизненно-важных сервисов в таких отраслях, как здравоохранение (оказание высокотехнологичной медицинской помощи), выработка и распределение электроэнергии, автоматизированное производство.

Обеспечивая безопасность Интернета вещей, организации сталкиваются с двумя основными препятствиями. Во-первых, большинство IoT-устройств не обладают функциями самозащиты. Поэтому их уязвимости могут быть использованы атакующими для перехвата управления устройствами и получения доступа к сети. Во-вторых, ситуацию осложняет масштаб:



в ближайшие несколько лет предприятия могут подключать к сети миллиарды устройств.

Cisco IoT Threat Defense – позволяет безопасно масштабировать IoT-решения. Это архитектура, объединившая продукты Cisco для обеспечения информационной безопасности: Cisco TrustSec (сегментация сети); Cisco Stealthwatch (анализ сетевых процессов); Cisco ISE (визуализация устройств); Cisco AnyConnect (удаленный доступ); Cisco Umbrella (облачная безопасность); Cisco AMP (защита от вредоносного ПО); Cisco Firepower NGFW (межсетевой экран).

Для обнаружения угроз и скомпрометированных узлов в этой архитектуре выполняется визуализация и анализ входящего и исходящего трафика IoT-устройств, а также входящего и исходящего трафика всего предприятия. Решение способно обнаруживать аномалии, блокировать угрозы, идентифицировать пораженные узлы, содействовать в устранении последствий пользовательских ошибок. Кроме того, эта архитектура обеспечивает безопасность удаленного доступа между сайтами и между организациями.

## Сбербанк внедряет в Красноярске микроЦОД

Компания «ЛАНИТ-СИБИРЬ» (входит в ГК «ЛАНИТ») запустила в эксплуатацию микроцентр обработки данных DataStone на базе отечественной разработки в красноярском отделении Сбербанка. Уникальность спроектированного ЦОД состоит в функционально-техническом запатентованном решении, спроектированном специально под нужды заказчика.

Специалисты «ЛАНИТ-СИБИРЬ» провели технико-экономический анализ внедрения решения, произвели монтаж необходимых трасс коммуникаций и поставку оборудования микроЦОД Utilex, после чего совместно с инженерами компании «Утилекс» провели пусконаладку и запуск решения.

МикроЦОД (мЦОД) DataStone – это комплекс инженерной инфраструктуры для размещения и обеспечения отказоустойчивой работы информационно-вычислительных и/или телекоммуникационных систем. Внешне мЦОД представляет собой защищенный шкаф с расположенными внутри него прецизионными кондиционерами и возможностью комплектации дополнительными инженерными системами: системой гарантированного

питания, системой распределения питания, автоматической установкой газового пожаротушения. Конструкция мЦОД мобильна и приспособлена для перевозки всеми видами транспорта.

Модульный мЦОД DataStone обладает защитой IP65, полностью замкнутым циклом прецизионного охлаждения и контроля влажности, системой шумопонижения, системой дистанционного мониторинга и управления. Универсальность решения позволяет сократить дальнейшие финансовые и временные затраты на подготовку серверных помещений и их проектирование с учетом особенностей каждого отделения банка по сравнению с классическими вариантами серверных.

Александр Абрамкин, заместитель председателя – управляющий Красноярским отделением Сбербанка: «Решение, предложенное компанией «ЛАНИТ-СИБИРЬ», отвечает нашим задачам и позволяет сократить площадь технических помещений. Теперь мы можем увеличить количество рабочих мест для сотрудников и сократить административно-хозяйственные расходы».

# К импортозамещению ERP крупные предприятия подходят особенно аккуратно



**Алексей КАЗАРЕЗОВ,**  
директор ЦИТК «Парус»

## Приоритеты флагманов: учет, планирование, масштабируемость

С точки зрения развития ИТ предприятия оборонно-промышленного комплекса и гражданского машиностроения подошли к той черте, когда управление финансами, активами и кадровыми ресурсами автоматизировано. Но для дальнейшего повышения эффективности нужна информатизация процессов управления НИОКР и производством. В промышленности основные издержки формируются в процессе производственной деятельности. Неудивительно, что здесь же скрываются и незадействованные резервы их снижения. Очевидна потребность в классической ERP, которая будет взаимоувязывать производственные операции со всеми

Решение общей для разных сегментов задачи по замещению импорта в сфере ИТ различается в зависимости от масштабов деятельности и целей автоматизации. И это не единственные критерии, с учетом которых предприятия, учреждения и организации вынуждены подходить к выбору ИТ-инструментов на определенном этапе своего развития. Рассмотрим возможные подходы к решению задач, связанных с импортозамещением, тенденции и трудности, с которыми сталкиваются флагманы отечественного ОПК, на примере миграции решений компании «Парус» на непроприетарное инфраструктурное программное обеспечение.

ресурсами предприятия в целях их оптимизации.

Если основная деятельность не автоматизирована, невозможно спланировать и выполнить производственную программу в срок с максимальной финансовой эффективностью и обеспечить подтверждение фактических затрат.

Однако по сравнению с финансово-хозяйственной деятельностью автоматизировать управление производством не так просто. Это более сложная и требовательная к информатизации предметная область, так как нормативно-справочная информация (НСИ) производственно-технического характера существенно объемнее, чем, например, НСИ для бухгалтерского или складского учета.

В производстве колоссальные объемы информации, подлежащей обработке. Как показывает опыт компании «Парус», отечественного разработчика программного обеспечения, количество записей, формируемых в базе данных в процессе оперативного производственного учета, у некоторых заказчиков измеряется миллиардами в месяц. И это связанные записи, описывающие плановое и фактическое движение детали-сборочных единиц

от формирования планового производственного состава до подготовки электронного паспорта изделия с пооперационным учетом всех стадий производственного процесса.

На основании этого можно сделать вывод, что для крупных предприятий критичными являются обеспечение максимально подробного производственного учета, быстрое действие системы при решении задач планирования производства и высокая масштабируемость информационной системы.

Приведу конкретные примеры. Один из российских промышленных концернов – «Тракторные заводы» – использует для автоматизации продукты «Парус 8» на своих производственных предприятиях. Сейчас управление производством автоматизирует завод «Промтрактор» – самое крупное предприятие концерна и один из мировых лидеров в сегменте тяжелых бульдозеров-рыхлителей и трубоукладчиков. «Промтрактор» выпускает примерно полсотни единиц техники, а количество модификаций доходит до 500. Производственная программа предприятия включает миллионы позиций. И вследствие высокой волатильности спроса заводу требуется еженедельно пересчитывать

месячную программу выпуска. Первый этап этого большого проекта завершен: автоматизированы производственное планирование, учет изготовленных деталей и цеховая логистика. В результате система рассчитывает производственную программу бригад на месяц, потребность в покупных материалах, себестоимость изделий и выдает всю информацию о выполнении плана в одном окне.

В настоящее время решаются задачи автоматизации позаказного учета затрат, планирования закупок, оперативно-календарного планирования на цеховом уровне, а также подготовки электронных паспортов изделия, что поможет снизить уровень незавершенного производства как минимум до двухмесячной потребности.

Другой пример – обеспечение производственного учета на Воткинском заводе. По оценкам специалистов предприятия, в системе, созданной на базе продуктов «Паруса», работает примерно 5 тыс. пользователей. В 30 цехах основного производства этого большого многоименного предприятия организован партионный учет движения детали-сборочных единиц. Каждая партия деталей запускается в производство в строгом соответствии с подетальным планом, рассчитанным на основе плана выпуска изделий и заключенных договоров. Движение детали-сборочных единиц в процессе изготовления изделий сопровождается электронными сдачными накладными. Благодаря внедрению этих инструментов у специалистов завода появилась возможность контролировать место размещения каждой детали-сборочной единицы в любой момент времени.

Реализовать такие процессы можно только в очень мощном ПО. Компания наращивала возможность системы «Парус 8» на СУБД Oracle годами, что позволило обеспечить высокий уровень производительности, необходимый крупным машиностроительным компаниям и таким холдингам, как «СУЭК» и «Евроцемент групп». Сегодня в числе клиентов «Паруса» стратегически важные отечественные предприятия. Помимо «Тракторных заводов»,

Воткинского завода к ним относятся Московский машиностроительный завод «Авангард», НПО «Сплав», «Туламашзавод» и другие предприятия.

## Экскурс в историю

«Парус» разработал импортно-независимое программное обеспечение задолго до объявления курса на замещение импорта. Еще в начале 2010-х компания запустила линейку стандартных учетных продуктов «Парус 10» для небольших государственных учреждений – музеев, лицеев, централизованных бухгалтерий. Идея была в том, чтобы предложить более дешевое в эксплуатации решение за счет применения бесплатной PostgreSQL вместо проприетарных СУБД. Так что к началу волны импортозамещения у «Паруса» уже был продукт на непроприетарной платформе, а партнеры компании перевели на свободное программное обеспечение сотни различных учреждений по всей стране. В рамках совместной работы десятков пользователей для выполнения учетных финансово-хозяйственных задач система на PostgreSQL поддерживает высокую отказоустойчивость и хорошую скорость обработки данных.

Но у крупных клиентов «Паруса» – федеральных ведомств, региональных министерств и тем более у производственных компаний – другие масштабы и иные задачи автоматизации. Поэтому с началом кампании по замещению импортных решений перед «Парусом» встала задача перехода к поддержке СУБД PostgreSQL для системы «Парус 8», которую используют большие организации. Фактически это означает выжать максимум производительности из этой платформы. С учетом масштаба автоматизируемых операций наших клиентов производительность на PostgreSQL должна быть сопоставима с Oracle. Над этой задачей мы работаем на протяжении последних нескольких лет. При этом особое внимание уделяется разработке инструментов для максимально простого перехода клиентов на непроприетарную СУБД. Например, разработан полнофункциональный универсальный конвертер базы данных Oracle

в PostgreSQL. Путем нажатия одной кнопки можно преобразовать все объекты клиентской базы данных, в том числе все пользовательские наработки, в среду PostgreSQL.

## Необходимость и целесообразность

Но конвертация базы данных – не самая большая проблема, с которой сталкиваются наши заказчики при смене платформ. Для крупных предприятий импортозамещение означает необходимость замены существующей развитой инфраструктуры (по сути, покупки новых дорогостоящих серверов), переобучения пользователей и администраторов систем, а также переинтеграции связанных программных продуктов. Тем самым от каждого предприятия ИТ-импортозамещение требует огромных вложений и организационных усилий, не говоря уже о рисках потери производительности при ИТ-перестройке.

Безусловно, применение российского или свободного ПО целесообразно при запуске новых проектов, когда можно заранее рассчитать мощность оборудования и корректно спроектировать ИТ-ресурсы для функционирования софта с требуемыми показателями производительности.

На сегодняшний день проекты импортозамещения в ИТ-сфере ограничиваются переходом на российские системы электронного документооборота, видеоконференцсвязи и антивирусное ПО. А вот примеров успешного импортозамещения информационных систем ERP-класса на больших производственных предприятиях пока не наблюдается. Неудивительно, что крупные компании, в том числе наши клиенты, аккуратно подходят к вопросу импортозамещения мощных прикладных систем, тщательно взвешивая все «за» и «против». В таких условиях свою задачу мы видим в том, чтобы обеспечить развитие функциональности и поддержку высоких показателей производительности системы «Парус» как в классическом варианте – с СУБД Oracle, так и с использованием непроприетарной платформы. ■

*Круглый стол*

# Замещение импорта в сфере инфраструктурного ПО: риски, проблемы и алгоритмы решений

## В круглом столе принимают участие

**Илья БЕЛОВ**,  
ведущий менеджер по развитию департамента инфраструктурных решений, ГК Softline

**Валерий БОРДЮЖЕ**,  
председатель Координационного совета по информационным технологиям предприятий оборонно-промышленного комплекса

**Александр ЗАЦАРИННЫЙ**,  
заместитель директора ФИЦ ИУ РАН, д. т. н., профессор, член КС ИТ ОПК

**Александр ГОЛИКОВ**,  
председатель совета директоров ГК «АСКОН»

**Алексей КАЗАРЕЗОВ**,  
директор ЦИТК «Парус»

**Юрий КУЗЬМЕНКО**,  
руководитель отдела исследований и разработки, «Энвижн Групп»

**Виталий МАКСИМОВ**,  
заместитель генерального директора по маркетингу, Группа компаний РЕЛЭКС

**Ольга ТЫРНОВСКАЯ**,  
вице-президент по работе с вендорами, группа «Астерос»

Трудности, с которыми столкнулись российские специалисты в рамках импортозамещения в сегменте инфраструктурного программного обеспечения, не являются уникальными. Опыт решения подобных задач есть в других странах. Участники заочного круглого стола обращают внимание на основные тенденции в этой сфере и анализируют риски, преимущества и недостатки возможных моделей, стимулирующих инструментов и вариантов поддержки отечественных разработчиков. При всем разнообразии точек зрения эксперты единодушны в том, что при выборе подходов к замещению импорта необходимо учитывать уровень технологического развития государства, общества и бизнеса.

**Некоторые эксперты сегодня критикуют Реестр отечественного ПО, указывая, в частности, на тот факт, что большинство продуктов, внесенных в список, можно использовать только на Windows и с базами данных SQL и Oracle. Насколько обоснована такая критика?**



**Илья БЕЛОВ**

Небезосновательна. Существуют разработки под Windows, но это более старые продукты. Новые системы дорабатываются так, чтобы уйти от этого. Также в Реестр попадают

решения, производительность которых не рассчитана на enterprise-сегмент.



**Валерий БОРДЮЖЕ**

Критика обоснована. Из более чем трех тысяч единиц



зарегистрированного отечественного ПО большая часть функционирует на иностранном системном обеспечении. Вместе с тем факт существования реестра позитивен, так как может служить хорошей базой для отбора программных продуктов с повышенными требованиями к информационной безопасности. Например, потребители, представляющие интересы предприятий ОПК, критически важных объектов и другие специализированные структуры, вполне могут повысить ведомственные требования к ПО по безопасности и закупать только те продукты, которые полностью их устраивают.



**Александр ЗАЦАРИННЫЙ**

Действительно, по нашим данным, не просто большинство, а подавляющее большинство программных продуктов, зарегистрированных в Реестре отечественного ПО, разработано на платформе Windows с СУБД SQL и Oracle. И такое положение объективно отражает реальное состояние дел, поскольку указанное базовое ПО предоставляет разработчикам прикладного ПО наилучшие условия для выполнения необходимых этапов разработки, тестирования, документирования, проверки и сертификации. Нельзя не учитывать и накопленный опыт работы информационных систем в программной среде Windows во многих ФОИВ и коммерческих структурах. Поэтому вопрос по поводу обоснованности критики Реестра не совсем корректен; более актуальным является вопрос о степени доверенности программных продуктов, зарегистрированных в Реестре, которая должна

подтверждаться документами от соответствующих экспертных организаций. Регистрация должна проводиться только при наличии таких документов в соответствии с требованиями к конкретному программному продукту, включая требования по информационной безопасности.



**Александр ГОЛИКОВ**

Что тогда, по мнению указанных экспертов, использовать? Отечественных ОС и СУБД такого класса сегодня нет. Для построения коммерческих высокотиражных продуктов важны не просто наличие отечественных ОС и СУБД, а их надежность, быстрдействие, способность работать под большой нагрузкой, удобные инструменты разработчиков ПО и многое другое. Никто не мешает вкладываться в развитие того же Postgre, формируя мощный центр компетенции, постепенно переводя на него критичные с точки зрения инфобезопасности задачи.



**Алексей КАЗАРЕЗОВ**

Наверное, разные эксперты по-разному представляют цели создания Реестра отечественного ПО. Вероятно, есть эксперты, считающие, что в Реестр должно быть включено ПО, использующее

только непроприетарные компоненты либо компоненты отечественной разработки и желательно поддерживающее отечественные аппаратные платформы. Да, такие эксперты могут быть не удовлетворены. Мы же придерживаемся более прагматичной позиции: Реестр должен способствовать приоритетному применению отечественного ПО в госкомпаниях и предотвращать немотивированное использование зарубежных аналогов. Этой цели Реестр отечественного ПО соответствует. Вероятно, со временем требования по включению ПО в Реестр могут пересматриваться.



**Юрий КУЗЬМЕНКО**

И да, и нет. С одной стороны, в России широко распространена система Windows. Именно эта система используется как основная на большинстве государственных и коммерческих предприятий. По этой причине большая часть ПО разрабатывалась под эту систему. С другой стороны, в Реестре также представлено и кроссплатформенное ПО, что в последнее время является трендом.

По поводу баз данных можно сказать, что часть ПО использует ORM и, как следствие, может работать с базами данных, отличными от Oracle и MS SQL. В Реестре, кстати, представлена Postgres Pro, российская ветка популярной базы данных PostgreSQL, которая составляет достойную конкуренцию реляционным СУБД от Oracle и Microsoft. Также необходимо отметить, что в последнее время все большую популярность приобретают базы данных NoSQL, которые преимущественно являются проектами open source.

**Виталий МАКСИМОВ**

Прежде чем отвечать на этот вопрос, нужно задать другой: с какой целью создавался этот Реестр? Если целью было зафиксировать все написанные российскими разработчиками программы – это одно. Если же целью было обеспечить технологическую независимость от иностранного ПО – совсем другое. Можно ли говорить о кибербезопасности страны, когда государственные информационные системы

работают на иностранных СУБД, которые официально спонсируются Минобороны США? Может ли считаться отечественной операционная система, исходный код которой заимствован у того же Linux? Чтобы система была признана по-настоящему отечественной, она не только должна быть написана с нуля нашими разработчиками, но и вся инфраструктура (аппаратно-программная среда) должна быть отечественной и безопасной. Только так крупнейшие государственные компании могут спокойно работать, не боясь иностранных программных закладок и уязвимостей. Мы в «Релаксе» считаем, что только проприетарное ПО может быть безопасным, потому что мы как налоговый резидент РФ несем ответственность перед заказчиками и государством за каждую строчку кода в нашей СУБД.

**Ольга ТЫРНОВСКАЯ**

Реестр формируется по определенным правилам, его цель – поддержка отечественных программных продуктов. Если есть нарушения, то необходимо их устранять, если нет, то вопросы надо задавать разработчикам, почему они выбирают те или иные платформы. Реестр будет полезен при наличии конкурентоспособных продуктов. Если российские разработки не будут отвечать требованиям заказчиков, сам факт существования Реестра никого не спасет.

### Какие сложности возникают при портировании наиболее популярных в России бизнес-приложений на отечественные/открытые ОС и СУБД?

#### **Илья БЕЛОВ**

Основная сложность – совместимость с бизнес-критичными приложениями заказчика и техническая поддержка. SAP ERP Business Suite, Siemens PLM и другие решения, аналогов которых нет в России, требуют Oracle или IBM DB2 как СУБД. Соответственно, если мигрировать их на отечественные СУБД, то даже при сохранности функциональности приложения не будет поддержки от вендора. А чтобы обеспечивать бесперебойное функционирование таких сложных высоконагруженных систем, важно своевременно получать консультации разработчиков.

Отмечу, что если перед заказчиком стоит реальная, а не формальная задача по импортозамещению, то нельзя хаотично подходить к вопросу, менять отдельные решения и компоненты. Нужно подготовить подробный план, а перед этим провести аудит.

Прописать архитектуру решений (серверы, СХД, ПО), а потом спроектировать ее на отечественном программном обеспечении. При этом критичные системы, например Siemens SAP, не затрагиваются. В итоге заказчик получает отчет, в котором отражены сведения об имеющемся оборудовании, план перехода на другие решения, возможные риски. При наличии четкого плана развития инфраструктуры можно сделать процесс более эффективным.

#### **Александр ЗАЦАРИННЫЙ**

Принципиальных технических сложностей нет. Но! Часто портирование трактуется как некий перенос уже разработанного в среде Windows программного продукта в среду открытого ПО (варианты Linux). При этом понимания того, что такой перенос – по существу, трудоемкий процесс создания нового программного продукта со всеми

вытекающими последствиями (трудозатраты, сроки и финансирование), как правило, не проявляется. Если называть вещи своими именами, портирование – это разработка программного комплекса, которая должна определяться тремя классическими параметрами: заданием, сроками и деньгами. Новое задание потому, что со временем у заказчика, естественно, появляются потребности в новых приложениях, а в некоторых прежних необходимость отпадает. Очевидно, что разработчик исходного программного продукта выполнит такую работу более качественно, быстрее и, может быть, дешевле, чем новый исполнитель. А технических трудностей, действительно нет. Не хватает истинного понимания существа портирования ПО.

#### **Александр ГОЛИКОВ**

Риск потери быстродействия. Хотя все зависит от задачи. Но самое главное: зачастую архитектура построения системы может не позволить просто портировать приложения – может потребоваться серьезная переработка программного

продукта. Также надо понимать, что во время работы над портированием бизнес-приложений на отечественные/открытые ОС и СУБД разработчик не занимается наращиванием их пользовательской функциональности.

#### **Юрий КУЗЬМЕНКО**

При портировании на открытые ОС бизнес-приложений, написанных на Java, таких сложностей не возникает. Это касается и приложений, написанных на скриптовых языках (JavaScript, Python и т. д.). Причем большинство приложений, написанных на этих языках, уже портированы на Linux-системы.

Что касается приложений, написанных на C#, то в последнее время одной из приоритетных задач разработчиков платформы .Net компании Microsoft является именно кроссплатформенность. К сожалению, не все так быстро, как хотелось бы. На данный момент .Net Core является кроссплатформенной системой с открытым исходным кодом. Существуют соответствующие рекомендации от вендора по миграции на .Net Core, пользуясь которыми наши Net-разработчики уже перевели часть приложений на .Net Core, и теперь эти приложения могут работать на Linux-системах. Правда, нельзя сказать, что это был простой и гладкий процесс.

Основной проблемой при портировании приложений, написанных на C++, является использование библиотек, которые работают исключительно под Windows. В некоторых случаях возникает необходимость писать отдельное приложение для другой платформы, переходить на другую среду разработки, например Qt, или

смотреть в сторону Java, если быстрое действие не является настолько критичным.

Что касается портирования на открытые СУБД, то часть приложений взаимодействует с базой данных посредством ORM. В таких случаях портирование на открытые СУБД не вызывает особых проблем, а скорее является легкой настройкой. Другая же часть приложений не использует ORM, так как применение ORM в некоторых случаях – дополнительная нагрузка на приложение и причина потери быстрого действия. Кроме того, ORM не позволяют использовать специфические возможности, которые существуют в определенной СУБД и являются причиной ее выбора при разработке. В подобных случаях при портировании приходится отказываться от этих возможностей, искать новые пути решения, возможно, менять логику, переписывать хранимые процедуры, функции, триггеры и т. д. Этот вопрос особенно актуален, когда большая часть логики приложения находится в СУБД.

Помимо технических существуют вопросы, связанные с формированием новой экспертизы, переподготовкой специалистов. Процесс обучения и адаптации занимает месяцы.

#### **Виталий МАКСИМОВ**

Понятные технические проблемы связаны с переносом больших объемов данных, переписыванием исходного кода приложений, неизбежностью остановки бизнес-процессов клиента в период внедрения и т. д. Немаловажен и фактор времени: далеко не все заказчики понимают, что миграция приложений – сложная техническая задача, решение которой может длиться

несколько лет. Все эти проблемы вполне решаемы, другое дело – убедить заказчика в том, что весь функционал и производительность импортных продуктов нужны далеко не всегда. Например, пользователи привыкли к моментальному отклику приложений на их действия и не готовы к снижению производительности, даже если оно будет временным и не отразится на бизнесе. Следует признать, что отечественных продуктов, которые могут обеспечить аналогичные иностранным ПО скорость и функциональность, сегодня нет. Для их появления необходимо партнерство другого порядка: когда заказчик готов обеспечивать разработчика задачами, которые дают развитие продукту. У нас есть многолетний опыт сотрудничества с ОАО «Сургутнефтегаз». Начинали с относительно небольших задач, в процессе работы получали обратную связь и дорабатывали нашу СУБД под требования заказчика. В итоге выиграла все стороны.

Стоит отметить также, что много времени отнимает перенос значительного объема данных, больших затрат требуют ручное переписывание кода, необходимость внесения изменений в бизнес-приложения для работы с другой СУБД. Нельзя не учитывать возможные высокие издержки простоя, устаревание системы в процессе разработки.

#### **Ольга ТЫРНОВСКАЯ**

На данный момент мы не наблюдаем у наших заказчиков массовых смен платформ и решений, на основании которых можно было бы сделать выводы. Каждый случай является уникальным – со своими задачами и проблемами.

**Может ли Россия использовать опыт отдельных европейских стран? Например, во Франции существует система жестких запретов на использование государственными органами зарубежных ОС и СУБД. В Германии и Италии государство субсидирует миграцию муниципальных органов власти на открытое ПО (OS Linux).**

#### **Илья БЕЛОВ**

Помощь государства была бы своего рода толчком для развития технологий: процесс создания решений может стать более эффективным, это будет одним из способов стимулирования спроса на них. Например, разработок

на Linux очень много, но мало инсталляций, а система эволюционирует только тогда, когда она активно используется.

#### **Валерий БОРДЮЖЕ**

Должна использовать. И не только европейских стран. В Китае еще в 2014 г. создали национальную ОС, базирующуюся на Linux, и заменили ею Windows на всех компьютерах в правительстве Китая. Для внутреннего рынка в рамках сотрудничества с оборонным научно-техническим университетом Китая также создана операционная система Ubuntu Kylin.

Поскольку ИТ уже давно стали продукцией двойного назначения и приобрели все признаки оружия массового поражения сознания граждан, инфраструктуры государств и технологических объектов, а кибервойны становятся все масштабнее, России, безусловно, следует иметь собственное национальное системное программное обеспечение.

#### **Александр ЗАЦАРИННЫЙ**

В России вполне может быть внедрен подобный подход. Дело за малым: ограничить функционал и для него спланировать целевое субсидирование.

#### **Александр ГОЛИКОВ**

Разумное решение. У нас серьезным препятствием является то, что основным инвестором создания отечественных ОС и СУБД пока является государство. Это приводит к доминированию подхода: раз государство что-либо финансирует, то права на продукт

также должны принадлежать государству. А как, на какие средства дальше будут развиваться созданные ОС, СУБД или программный продукт? Кто будет оплачивать развитие? С нашей точки зрения, это одно из главных препятствий для импортозамещения.

#### **Юрий КУЗЬМЕНКО**

В России можно было бы запретить использование государственными органами зарубежных ОС, если бы имелись собственные разработки уровня ведущих мировых аналогов (у нас уже есть неудачный опыт попытки пересадить государственных служащих на отечественные автомобили).

Системы с открытым исходным кодом, на мой взгляд, выглядят предпочтительнее, но уровень экспертизы на сегодняшний день оставляет желать лучшего. Большинство российских средних и высших учебных заведений продолжает использовать и продвигать систему Windows. Крупные российские компании не торопятся спонсировать open source-проекты или как-либо в них участвовать и, что еще хуже, не поощряют, а порой запрещают своим сотрудникам участвовать в таких проектах. Ведущие зарубежные компании, напротив, приветствуют участие своих сотрудников в open source-проектах и сами пытаются поддерживать эти проекты, чтобы повысить контроль и уменьшить собственные риски.

В любом случае процесс перехода на open source-системы должен быть плавным, постепенным.

Нельзя всех в приказном порядке перевести на open source с завтрашнего дня. Сначала нужно нарастить экспертизу и вовлечь российский бизнес в open source-проекты.

Если говорить о создании государственного ПО в целом, то разработку новых проектов нужно начинать на open source, если его уровень соответствует уровню коммерческих систем. Нужно понимать, что open source-проект сам по себе не является панацеей, важна собственная экспертиза. Как показывает опыт, любой open source-проект так или иначе может быть поглощен крупной компанией или просто перестать существовать, например, open source-проект Titan (графовая база данных) перестал развиваться, а дальнейшее продолжение получил в коммерческой версии DataStax.

#### **Ольга ТЫРНОВСКАЯ**

Конечно, может. Именно этим Россия занималась много лет в области ИТ: в результате здесь у нас не самая плохая ситуация. Тем не менее опираться на мировой опыт следует осторожно и избирательно: далеко не всегда нужно следовать зарубежным моделям, тратя ресурсы взамен их развития и не учитывая рисков, заложенных в правила игры зарубежных партнеров. Санкционная политика в отношении России показала, что необходимо искать собственные решения, учитывающие текущий уровень технологического развития государства, общества и бизнеса.

### **В какой форме осуществляется или будет осуществляться поддержка работы открытых ОС и СУБД? Кто несет или будет нести ответственность за проблемы совместимости? Кто отвечает или будет отвечать за безопасность ОС и СУБД?**

#### **Илья БЕЛОВ**

Существуют разработки, основанные на открытых дистрибутивах. Специалисты дорабатывают

решения, добавляют новые функции, коммерциализируют продукт и продают лицензии. В этом случае ответственность несет

вендор. Если заказчик выбирает вариант работы на открытом ПО, то есть два пути развития событий. Первый – внедрять может партнер или заказчик своими силами. А поддерживают систему, если это крупный проект, интеграторы в рамках консалтинга. Заказчик подписывает с подрядчиком многолетний контракт. Здесь важно выбрать надежную компанию с богатой

экспертизой. Второй вариант – заказчик сам занимается внедрением и поддержкой. В этом случае он берет на себя ответственность за корректную работу системы и несет все сопутствующие риски.

#### **Александр ЗАЦАРИННЫЙ**

Вопрос очень правильный и актуальный. Действительно, проблема не в том, чтобы разработать открытое ПО, которое приобрело бы статус отечественного и стало бы основой для импортозамещения; такую задачу способны выполнить десятки фирм. Проблема в том, как внедрить и, главное, в дальнейшем поддерживать это ПО, и не только поддерживать, но и постоянно развивать с учетом растущих требований самых разных пользователей. Так, как эти процессы организованы в Microsoft, в IBM, в Oracle и ведущих мировых фирмах-лидерах.

У нас подобных коммерческих структур нет. Но поскольку проблема импортозамещения действительно актуальна и поставлена на государственном уровне, то и решаться она должна на соответствующем уровне – организационно и финансово. Тогда и вопросы безопасности будут решены адекватно. Вместе с тем вопрос настолько многогранен, что требует весьма подробного обсуждения с привлечением всех

заинтересованных сторон: ФОИВ (прежде всего Минпромторга, Минкомсвязи), корпораций («Росатома», «Ростеха», «Роскосмоса», ОАК и др.), ведущих научных организаций.

#### **Александр ГОЛИКОВ**

Необходимо не просто использовать наработки зарубежного репозитория, важно, как минимум, участвовать на равных в развитии продукта, накапливать самостоятельные компетенции для его развития. Еще лучше – создавать отечественные репозитории, что невозможно без решения первого вопроса. Создание отечественного репозитория открытого ПО, а также появление мощного отечественного центра компетенций, занимающегося разработкой, сборкой, тестированием и поддержкой, позволят решить все вопросы, связанные с развитием продукта по подобной модели.

#### **Юрий КУЗЬМЕНКО**

Вне зависимости от того, открытая система или коммерческая, разрабатывается и поддерживается она специалистами-разработчиками. Вопрос скорее в наличии таких специалистов. Если смотреть на проблему глобально, то государству необходимо поддержать подготовку/переподготовку кадров. Вопрос на самом деле шире. Он касается

не только ОС и СУБД, но и среды разработки, фреймворков, библиотек и т. д.

Что касается проблемы совместимости, то это технический вопрос, который полностью находится в компетенции разработчиков независимо от того, открытая система или коммерческая. Некоторые open source-проекты имеют платную коммерческую поддержку, некоторые – серьезное комьюнити с большим количеством высококвалифицированных специалистов, готовых помочь своим коллегам.

Если говорить про безопасность, то у государства есть службы, отвечающие за безопасность, они и будут отвечать за безопасность ОС и СУБД. Соответствующие кадры у них имеются, а при необходимости они будут привлекать подрядчиков, занимающих ведущие позиции в отрасли.

#### **Ольга ТЫРНОВСКАЯ**

Вся полнота ответственности всегда лежит на заказчике системы, и только в рамках договоров она может перекладываться на плечи вендоров и поставщиков. Конкретный производитель и заказчик есть и у ПО с открытым кодом. Вопрос только в том, как производитель будет поддерживать свой программный продукт и хватит ли ему для этого ресурсов.

**Существуют две противоположные точки зрения на финансирование разработок ПО. Сторонники одной считают, что лучший вариант процесса импортозамещения следующий: промышленные корпорации получают средства из бюджета, объединяются в пулы и заказывают разработчикам ПО с жестким контролем за выполнением. Сторонники другой предлагают целенаправленно (на уровне государственных проектов) финансировать проекты разработки отечественного ПО, выбранные в силу их важности для решения проблемы импортозамещения. Какая позиция вам ближе и почему? Какая позиция (не обязательно из указанных выше) представляется наиболее реалистичной?**

#### **Илья БЕЛОВ**

Первая позиция логична, если речь идет о крупном заказчике со специфическими процессами. Например, оборонная промышленность. Но дело в том, что для этой отрасли уже разрабатывается специализированное ПО, которое продается только таким предприятиям и не имеет коммерческой лицензии. Это подход для решения внутренних критических задач. Во всех остальных случаях мне ближе вторая точка зрения: нужно поддерживать разработчиков, привлекая их к участию в государственных

проектах создания отечественного ПО. При наличии таких решений на российском рынке будет формироваться спрос на них, в том числе и у госструктур. Думаю, при целенаправленном финансировании этот процесс будет запущен.

#### **Валерий БОРДЮЖЕ**

Оба варианта хороши и реалистичны, но применять их нужно под разные программные продукты. На уровне федеральных целевых программ следует обеспечить финансирование и организовать разработку системного ПО и стратегического прикладного, например, инженерного ПО. Для разработки остального отечественного прикладного ПО вполне приемлем вариант создания пулов заказчиков и формирования государственно-частных партнерств с разработчиками.

#### **Александр ЗАЦАРИННЫЙ**

На основании изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» в апреле 2015 г. Минкомсвязи России утвердило приказ об отраслевом плане замещения импортного программного обеспечения. Документ определяет, каковы к 2025 г. должны быть максимальные доли импорта в различных сегментах программных продуктов. Для импортозамещения программного обеспечения в изделиях специального назначения необходимо открыть ряд работ по развитию программного обеспечения, входящего в состав базовых защищенных информационно-компьютерных технологий (БЗИКТ). На сегодняшний день ряд программных продуктов, входящих в состав БЗИКТ, не соответствует современным требованиям, а в некоторых областях отсутствуют аналоги ПО.

#### **Александр ГОЛИКОВ**

Первая стратегия наиболее близка рыночным компаниям, разработчикам тиражного программного обеспечения. Этот подход разделяет и Консорциум

компаний-разработчиков инженерного ПО, куда входят компании «АСКОН», АДЕМ, НТЦ АПМ, «Тесис», «Эремекс». Подобная стратегия позволяет развивать продукты, оставляя их в рынке. Вторую стратегию считаем неработоспособной – она будет генерировать нерыночные продукты со всеми вытекающими последствиями (низкое качество, дороговизна, слабая конкурентоспособность, невозможность жизни в рынке и т. д.). Они будут существовать только в условиях потребителю, а монополизм и конкурентоспособность не живут вместе. Инженерный софт – это не инфраструктурное ПО, «Платон» с ЕГАИС, когда у потребителей нет выбора.

Государство опасается финансировать коммерческие компании, разработчиков тиражного ПО, обладающих как раз максимальным опытом создания рыночных, коммерчески успешных продуктов. Попытки создания госсистем в высококонкурентных сегментах обречены на вечное бюджетное финансирование с принуждением потребителей использовать продукт, который они не выбирали.

#### **Алексей КАЗАРЕЗОВ**

Для успеха продвижения любой продукции прежде всего должен быть сформирован целевой рынок, готовый эту продукцию потреблять. Бессмысленно финансировать проекты разработки отечественного ПО без должной мотивации промышленных корпораций к его потреблению. Таким образом, подход, когда промышленные корпорации получают средства из бюджета, объединяются в пулы и заказывают разработчикам ПО, кажется более рациональным.

#### **Юрий КУЗЬМЕНКО**

На мой взгляд, на государственном уровне необходимо целенаправленно финансировать разработку отечественного ПО. Промышленные корпорации должны формировать задания на проекты и в конечном счете получать качественное отечественное ПО,

полностью удовлетворяющее их нужды.

Заказы необходимо объединять в пулы, чтобы 100 компаний-разработчиков не разрабатывали одно и то же для 100 заказчиков. Должно быть создано одно или несколько типовых решений с самым высоким качеством, а не по самой низкой цене и ратифицировано на всю сотню компаний-заказчиков.

#### **Ольга ТЫРНОВСКАЯ**

Действительно, эти два подхода наиболее очевидны. Первый («под заказ») основывается на целенаправленном финансировании конкретных разработок. Второй предполагает ориентацию на производителя ПО, который видит потребности рынка, и на привлеченные инвестиционные средства разрабатывает программный продукт.

Но есть и третий вариант, представляющий собой комбинацию первых двух: так или иначе по этому пути пошли все мировые софтверные лидеры. В его основе лежит технологическое лидерство, ведь лидеры – это не только те, кто имеет большую долю рынка, а еще и те, кто наиболее полно может удовлетворить требования заказчиков. Догнать и перегнать лидеров – весьма затратная задача, как по ресурсам, так и по времени. Объединение корпораций в пулы будет малоэффективным, так как неясно, кто именно заказчик и сможет ли разрабатываемое решение удовлетворить потребности каждого из участников. Вызывает сомнение и то, насколько эффективно такой коллективный заказчик сможет ставить задачи и контролировать их выполнение.

По моему мнению, победят энтузиасты из числа разработчиков, и не в разрезе продуктов-аналогов, а в разрезе совершенно новых решений, подходов и инструментов. При этом в краткосрочной и среднесрочной перспективах основные заказчики останутся на продуктах лидеров рынка, если это будет возможно и выгодно для них. ■

## Программно-конфигурируемая СХД сэкономила бюджет и время

Управляющая компания ТКБ Инвестмент Партнерс (АО) и «Инфосистемы Джет» запустили в эксплуатацию отказо- и катастрофоустойчивый файловый кластер на базе программно-конфигурируемой СХД (Software-Defined Storage, SDS) HPE StoreVirtual VSA. Применение SDS позволило выполнить внедрение менее чем за месяц и существенно сэкономить бюджет проекта. Благодаря модернизации время восстановления файлового сервиса в случае сбоя сократилось с 15 минут до 30 секунд.

Файловый кластер охватывает две площадки ТКБ Инвестмент Партнерс (АО), расположенные в нескольких десятках километров друг от друга. Система развернута на базе уже имеющихся у заказчика оборудования и среды виртуализации, что существенно снизило стоимость проекта. Решение обеспечивает автоматическое резервное копирование данных и быстрое восстановление файлового сервиса в случае сбоя.

Программно-конфигурируемая кластерная система заменила собой устаревшее решение, которое уже не справлялось с существующим объемом задач. Для

ее построения использовались виртуальная СХД HPE StoreVirtual VSA, ОС Microsoft Windows Server и система резервного копирования Veritas Backup Exec. Данные и права доступа к каталогам и файлам перенесены со старого файлового кластера на новый автоматически. При этом соблюдено требование непрерывной доступности файлового сервиса. Проверка по итогам проекта доказала, что внедренное решение полностью соответствует всем требованиям заказчика.

«Катастрофоустойчивость – наше принципиальное требование ко всем системам обработки и хранения данных. Для конкретного сервиса важнейшую роль также играли доступность в режиме 24×7 и обязательное автоматическое переключение без потери данных в случае сбоя одного или нескольких компонентов системы. Эксперты компании «Инфосистемы Джет» предложили решение, которое полностью удовлетворяло всем нашим требованиям», – отмечает руководитель проекта со стороны заказчика, начальник отдела развития и сопровождения инфраструктуры ТКБ Инвестмент Партнерс (АО) Илья Смирнов.

## «МегаФон» продемонстрировал работу своих M2M- сервисов

Столичный филиал «МегаФона» провел для СМИ и блогеров пресс-тур, посвященный современным цифровым технологиям M2M (Machine-to-Machine – межмашинное взаимодействие). Мероприятие прошло на базе мясокомбината ТМ «Окраина» – корпоративного клиента компании и самого молодого мясоперерабатывающего предприятия в столичном регионе.

M2M-решения «МегаФона» увеличили на 25% количество клиентов ТМ «Окраина», заказывающих продукцию у предприятия и пользующихся услугой трекинга. К концу мая 2017 г. их общее количество достигло 10 тыс. человек.

За счет использования сервисов «Контроль кадров» и «Интернет вещей» удалось сделать бизнес эффективным, оптимизировать ресурсы и время.

«Для нас решением этих задач стало подключение услуги «Контроль кадров» от «МегаФона». За год работы сервиса нам удалось сократить расходы на топливо на 300 тыс. руб., а также сэкономить рабочее время на 8%. Это позволило увеличить количество заказов. За 6 месяцев с момента подключения сервиса их количество выросло

на 15%», – комментирует генеральный директор ТМ «Окраина» Виталий Деледидка.

«Уже сейчас нашим клиентам доступно 22 решения для бизнес-среды на основе M2M. Это помогает макси-

мально использовать ресурсы мобильной связи и возможности современных цифровых технологий. Только за 2017 г. количество M2M и IoT-устройств в России должно вырасти на 40%. В ближайшие три года «МегаФон» планирует перейти от традиционного телеком-оператора к технологическому игроку, предоставляющему современные цифровые услуги для бизнеса всех уров-

ней», – рассказывает Владимир Волков, руководитель по развитию корпоративных клиентов Столичного филиала «МегаФона».

По итогам 2016 г. компания «МегаФон» установила 4 млн телематических SIM-карт в России, из которых 50% используются в сфере мониторинга транспорта. Сервисы на платформе M2M также востребованы в сфере ЖКХ, промышленном производстве, в логистических и транспортных услугах, в банковской сфере, в здравоохранении.



# PLM с прицелом на замещение импорта



**Игорь КОЧАН,**  
директор по маркетингу, ЗАО «Топ Системы»

Поскольку у нас в стране тема применения PLM и его эффективности обсуждается довольно редко, для начала стоит разобрататься в терминах и понять актуальность данной задачи. Что же такое PLM? Ответ на этот вопрос легко найти в энциклопедии. PLM (Product Lifecycle Management) – это прикладное программное обеспечение для управления жизненным циклом изделия. В общем, PLM можно определить как стратегию ведения бизнеса на основе системных бизнес-решений, поддерживающих коллективную разработку, управление, распространение и использование информации о спецификации изделия в рамках расширенного предприятия от концепции до конца жизненного цикла изделия. PLM обеспечивает интеграцию персонала, производственных процессов, бизнес-систем и информации.

Основные этапы жизненного цикла изделия – управление

На мировом рынке тема применения PLM обсуждается давно. Компании демонстрируют, насколько масштабными и эффективными являются соответствующие платформы, на которые переводятся специализированные решения разных производителей. Однако все предлагаемые крупными компаниями инструменты PLM, как правило, весьма дорогостоящие. Кроме того, их применение в оборонно-промышленного комплекса России ставит предприятия фактически в полную зависимость от иностранных производителей. Выход из ситуации один – обеспечить информационную и технологическую безопасность производства путем полного перехода на отечественные PLM-решения. Попробуем выяснить, есть ли такие системы.

требованиями, проектирование, производство, техническая эксплуатация, утилизация. PLM объединяет в комплексную систему передовые подходы и основные технологии: проектирование изделия (CAD), инженерные расчеты и анализ конструкций (CAE), управление данными об изделии и инструменты коллективной разработки (PDM), средства технологической подготовки производства и разработки программ для станков с ЧПУ (CAPP и CAM), а также комплекс мер по обеспечению послепродажного обслуживания изделия. Кроме того, сегодня много говорится о цифровом производстве и автоматизации не только жизненного цикла выпускаемого изделия, но и всех сопутствующих процессов: управления проектами и ресурсами (PM), планирования производства, организации взаимодействия с заказчиками и партнерами (CRM), обслуживания производственного оборудования (ТОиР), работы склада и др.

Таким образом, под PLM-системами понимаются программные комплексы, позволяющие решать большинство перечисленных задач, но в обязательном порядке имеющие минимальный

джентльменский набор: CAD/CAM/CAE/CAPP/PDM. Из этого и будем исходить при рассмотрении имеющихся у пользователей возможностей.

## Подходы к разработке PLM-комплексов

Очевидно, что решение столь широкого круга вопросов под силу лишь наиболее крупным игрокам рынка. Компаниям, которые концентрируют свою деятельность в указанном направлении и работают на этом поприще, много лет. В результате в мировой практике сформировался определенный подход к созданию полномасштабных PLM-комплексов. Его суть – разработка единого вертикального платформенного решения, на базе которого в дальнейшем строятся все приложения предметной области. Методологические вопросы построения PLM-решений неоднократно поднимались на различных международных конференциях, в том числе на наиболее авторитетной из них – COFES 2016 (Scottsdale, Arizona). В ходе обсуждений участники конференции, представляющие всех крупнейших



мировых игроков рынка САПР, сошлись во мнении, что только полноценное платформенное решение позволит выполнить такую задачу в полном объеме. Именно предложенный подход даст возможность избежать многократной конвертации и дублирования данных, необходимости решения задач синхронизации приложений, согласования механизмов безопасности и многих других проблем, с которыми сталкиваются пользователи, когда пытаются строить PLM-решение не на основе единой платформы, а из набора отдельных приложений, закрывающих отдельные направления.

Наиболее известным и масштабным платформенным решением является платформа 3DEXPERIENCE, разработанная компанией Dassault Systèmes. Это системное решение в числе лидеров в области 3D-проектирования, создания цифровых 3D-макетов и управления жизненным циклом изделий. Еще один пример аналогичного по масштабу комплекса демонстрирует компания Siemens, которая построила собственную PLM-платформу и активно ее расширяет, в частности переводит на эту платформу специализированные решения сторонних производителей. Однако все эти мощные инструменты относятся к весьма дорогостоящим. К тому же применение их на российских предприятиях оборонно-промышленного комплекса ставит эти предприятия в полную зависимость от иностранного производителя. Выход из ситуации – обеспечить информационную и технологическую безопасность производства путем полного перехода на отечественные PLM-решения.

## Возможности и потенциал отечественных решений

Сегодня на отечественном рынке довольно много компаний, предлагающих «PLM-решения». Это словосочетание взято в кавычки не случайно. За правильными и практически одинаковыми

Компания	Специализация				
	CAD	CAM	CAE	CAPP	PDM
«АСКОН»	«Компас 3D»			«Вертикаль»	«Лоцман»
«Топ Системы»	T-FLEX CAD	T-FLEX ЧПУ	T-FLEX Анализ		
T-FLEX Динамика	T-FLEX Технология	T-FLEX DOCs			
Группа компаний ADEM	ADEM	ADEM			
ТЕСИС	ViewVidia, 3DTransVivdia, CompareVidia		FlowVision		
Компания «Фидесис»			CAE Fidesys		
ЗАО «Нанософт»	«Нанокэд»				
НТЦ «Гемма»		«Гемма-3D»			
«СПРУТ-Технология»		SprutCAM		«СПРУТ-ТП»	
CSoft				TechnologiCS	TDMS
Группа компаний «Лоция Софт»					Lotsia PDM PLUS
Примечание. Информация о производителях и продуктах получена из открытых источников.					

словами часто скрывается разная суть. Но чтобы оценить ситуацию, достаточно обратиться к приведенным выше понятиям о сути решаемых задач и компонентах, которые должен содержать программный комплекс, чтобы называться PLM, и все проясняется.

Как видим, решений, охватывающих всю базовую линейку, не много. Большинство производителей предлагают отдельные программные системы, направленные на решение определенного круга задач. Эти системы умеют взаимодействовать между собой, но при их внедрении пользователь гарантированно столкнется со всеми трудностями синхронизации, конвертации, дублирования данных и согласования механизмов безопасности. Если вы готовы к нелегкой борьбе, то у вас очень широкий выбор. Если вы намерены развернуть на своем предприятии настоящее современное платформенное решение уровня ведущих мировых производителей, но сделанное в России, то выбор на сегодняшний день сужается до одного-единственного варианта. Это программный комплекс T-FLEX PLM производства российской компании «Топ Системы». Рассмотрим его возможности более подробно.

В текущем году компании «Топ Системы» исполнилось 25 лет. За четверть века разработчики систем T-FLEX прошли большой путь: от системы проектирования T-FLEX CAD к созданию первой в России коммерческой PLM-платформы, на основе которой построен крупнейший отечественный специализированный программный комплекс – T-FLEX PLM.

Сегодня T-FLEX PLM – полномасштабное решение промышленного уровня, с помощью которого можно эффективно организовать работу на всех этапах жизненного цикла изделия. В основе комплекса лежит первая отечественная PLM-платформа, построенная с учетом специфики использования единой цифровой модели изделия. Комплекс программ T-FLEX PLM позволяет организовать единую информационную среду конструкторского и технологического проектирования, подготовки и управления производством, сбытом и послепродажным сопровождением изделия. Расширенные функции T-FLEX PLM+ обеспечивают возможности управления проектами и планирования ресурсов, ведения полноценного организационно-распорядительного документооборота, контроля взаимоотношений с клиентами и многое другое.



Базовые компоненты платформы обеспечивают решение наиболее общих системных задач начального уровня и включают в себя следующие опции:

- работа с файлами;
- построение информационно-справочной системы;
- механизмы авторизации и управления доступом;
- встроенная почтовая служба;
- средства поиска и генерации отчетов;
- средства автоматизации бизнес-процессов;
- инструменты разработки;
- инструменты администрирования.

Компоненты информационных систем представляют собой специализированные решения типовых задач построения единой информационной системы предприятия и обеспечения взаимодействия сотрудников в процессе выполнения работ:

- инструменты управления проектами;
- средства работы с документами и ведения архива предприятия;
- средства автоматизации канцелярского документооборота;

- организация единой информационной среды предприятия (MDM);
- инструменты двусторонней интеграции с внешними ERP-системами;
- веб-компоненты для защищенного доступа к PLM-данным.

Компоненты инженерных систем спроектированы специально для решения задач, возникающих в процессе разработки, производства и послепродажного обслуживания изделия:

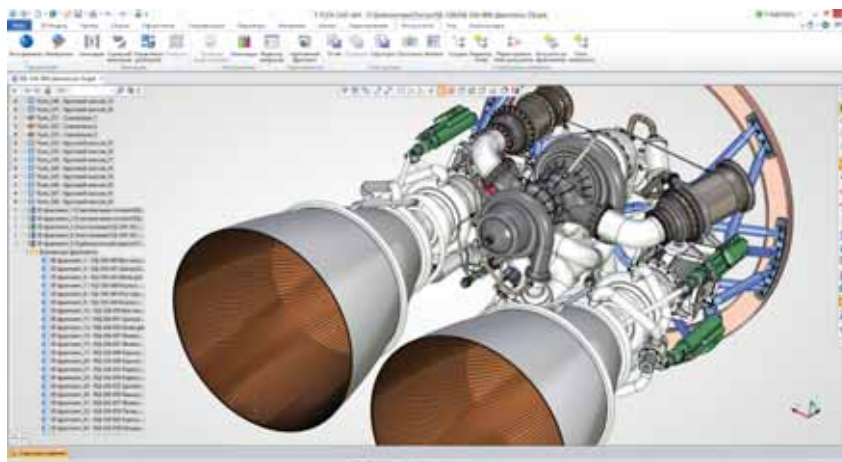
- инструменты работы с параметрической 2D- и 3D-моделью. Готовые механизмы интеграции с различными CAD-системами;
- средства формирования структуры изделий и управления изменениями. Формирование выходных конструкторских документов;
- поддержка параллельного ведения конструкторской, технологической и других вариантов структуры изделия;
- механизмы автоматизации технологической подготовки производства и генерации выходных технологических документов;
- инструменты планирования производства.

Решение T-FLEX PLM – это не только тщательно проработанная теория, но и многолетняя практика применения на российских и зарубежных предприятиях. В списке пользователей систем T-FLEX более 3500 предприятий, в том числе входящих во все ведущие концерны, такие как «Алмаз-Антей», Объединенная двигателестроительная корпорация, «Роскосмос», корпорация «Тактическое ракетное вооружение», Объединенная судостроительная корпорация и др.

При помощи инструментов комплекса T-FLEX разрабатываются изделия самого различного назначения и любой сложности.

Альтернативный вариант единого программного комплекса – решение компании «АСКОН».

Пользователям предлагается набор программных продуктов для решения задач автоматизации конструкторско-технологического



проектирования. В частности, система трехмерного моделирования и черчения «Компас-3D», система автоматизации технологической подготовки производства «Вертикаль», система управления инженерными данными и технического документооборота «Лоцман:PLM» и др. Компоненты комплекса популярны благодаря простоте и легкости освоения. Уровень их интеграции позволяет обмениваться проектными данными, однако отсутствие единой платформы существенно затрудняет применение комплекса в качестве единой информационной системы предприятия. Кроме того, в его составе пока нет некоторых компонентов, необходимых для полного покрытия задач управления жизненным циклом изделия. Но комплекс постоянно расширяется и в будущем может пополнить перечень отечественных PLM-решений.

Несколько иной подход избрали разработчики инженеринговой компании «ТЕСИС», которые сосредоточили усилия на развитии специализированных решений, предназначенных для расчетов трехмерных течений жидкости и газа; решении сложных многодисциплинарных задач по взаимодействию жидкости и конструкции: интеллектуальной трансляции моделей CAD-систем между прикладными системами, включая верификацию и валидацию этих моделей; автоматизированные средства работы с PMI (Product Manufacturing Information). Названная линейка продуктов не является универсальным PLM-решением, но безусловно

претендует на автоматизацию жизненного цикла расчетных задач в области течения жидкостей и газов. Благодаря многолетней специализированной направленности своих разработок инженеры компании «ТЕСИС» достигли больших успехов в своей области, предлагаемые продукты являются лидерами в этом сегменте.

## Проект «Гербарий»

В контексте темы импортозамещения в области PLM следует отметить еще одну отечественную разработку, не включенную в приведенную таблицу. Это проект «Гербарий», который выполнялся по заказу Фонда перспективных исследований (ФПИ). Стратегическая цель проекта «Гербарий» – обеспечение активного развития рынка отечественного инженерного ПО. В рамках проекта велась разработка интегрированной инженерной программной платформы (ИИПП), которая предназначена для решения широкого спектра задач по организации работы с цифровой моделью изделий и нацелена на то, чтобы стать основой нового российского рынка программных продуктов инженерного назначения.

Ключевым компонентом ИИПП является результат другого инновационного проекта – разработки отечественного геометрического 3D ядра RGK. Ядро построено на основе самых современных технологий, что обеспечивает высокий уровень производительности и точности моделирования. В перспективе

ядро RGK может быть положено в основу создания российской системы 3D-моделирования, которая сможет составить конкуренцию ведущим западным системам.

Все эти масштабные разработки могли бы стать надежной основой будущей российской PLM-платформы. На ее базе любые независимые разработчики специализированных приложений из самых разных предметных областей могли бы создавать компоненты, которые стекались бы в единую среду, образуя самое развитое PLM-решение в мире. В настоящий момент работы по этим проектам приостановлены, но мы надеемся на их скорое продолжение. Потребности промышленности в отечественном решении такого уровня очень высоки. На карту поставлены не только деньги, которые многие российские предприятия платят за иностранное ПО, но и вопросы информационной и технологической безопасности. Так что нет сомнений в том, что эта тема получит развитие, и со временем мы сможем подняться на новый уровень автоматизации предприятий.

Отметим, что отечественные PLM-решения развиваются в духе мировых трендов в этой области. На примере четырех крупнейших игроков мирового рынка PLM очевидна тенденция к консолидации локальных решений в определенных предметных областях в состав крупных программных PLM-комплексов. Общая стратегия состоит в поглощении малых компаний крупными, включении их разработок в состав большого PLM-решения и постепенном переводе программ на единую PLM-платформу, принадлежащую головной компании. Особенно решительно в этом направлении действует компания Siemens PLM Software.

В заключение можно сказать, что в области PLM в России есть как современные промышленные отечественные решения, так и перспективные разработки. Это позволяет с оптимизмом смотреть в будущее и надеяться, что отечественное инженерное ПО будет развиваться и активно применяться не только на российских предприятиях, но и за рубежом. ■



# АСУПП: что первично?



**Игорь РЕШЕТНИКОВ,**  
основатель и руководитель российского  
MES-центра, к. т. н.

Ведущие мировые производители строят свою систему управления производством по принципу «компьютер сказал – человек сделал». И это работает. У «них». И не потому, что у нас не хватает ума или денег – по уровню затрат на ИТ многие наши предприятия давно обогнали конкурентов. К такой системе нужно прийти – постепенно, вдумчиво, методично. И только тогда это заработает. Основой успеха является не волшебная суперпрограмма от известного разработчика, а понимание того, что делаешь, зачем и как. Вот этого нашим производственникам и не хватает.

## Простые вещи вместо «волшебной таблетки»

В процессе продолжительного общения с руководителями заводов выявляются общие черты и тенденции. Когда десять лет назад начиналась наша просветительская деятельность в сфере систем цехового управления, то казалось: достаточно

О том, что информационные технологии плотно вошли во все сферы деятельности, можно не напоминать. Но правильно ли мы их используем? Нужно ли нам уметь писать от руки или достаточно научиться работать с клавиатурой? Вопрос на самом деле далеко не простой. А уж когда речь заходит об управлении сложными процессами, производством, то правильный ответ найти еще труднее, если вообще удастся. Вот об этом и поговорим.

разъяснить людям очевидные вещи и все начнет развиваться. Но, увы. Сколько ни рассказывай про «грабли», про честный учет, про разницу между «есть в наличии» и «есть в документах» и т. д. – не помогает.

При этом все признают наличие проблемы, но тут же уверенно говорят, что для ее решения нужно выбрать «правильную программу». И тут же просят посоветовать такую программу. Хотелось бы, конечно, но... Проходит год, два, а люди все надеются и ищут ту самую «волшебную таблетку». И... не находят, что закономерно. А на самом деле нужно лишь понять и принять несколько простых вещей.

Первое. Зачем это надо, какой показатель эффективности? Хочется вывести себестоимость на уровень конкурентов и победить на рынке или освоить выделенный бюджет и отчитаться перед головной структурой? Оставим в стороне философские рассуждения на тему «порядка хочется», давайте научимся формулировать проблемы и задачи.

Второе. Хватит пытаться переложить бумажно-личностную систему управления в компьютер. Вы что хотите: показать, что внедрили компьютерную систему управления, а лучше не стало, значит, и до этого работали с полной отдачей? Или начать собирать через терминалы то, что раньше собирали записками от руки?

Третье. Ответьте на такой вопрос: про цикл Деминга P-D-C-A

слышали все, на каждой презентации про это говорится, но ни на одном заводе еще ни разу не видел, чтобы это было внятно реализовано. Даже на заводах, где считается куча показателей, более или менее честно рассчитываются ОЕЕ и т. п., все это идет мимо лиц, принимающих решения. По-прежнему во главе угла «интуиция».

Четвертое. О лозунге «Учиться, учиться и еще раз учиться», похоже, забыли. На семинарах я всегда спрашиваю, кто и что читал по вопросу организации управления производством. Стандартный ответ: «Нам читать некогда, мы заняты, вы нам расскажете, и мы пойдем дальше работать». Ставить линейным руководителем производства человека без специальных знаний и стремления их получать в надежде, что «покрутится – разберется», – это путь к успеху?

Пятое. Современное производство – царство информационных систем разных уровней: от CAD до ERP. Так почему на наших заводах ИТ-, с позволения сказать, «директор» часто даже не знает сути деятельности предприятия? Его роль на современном заводе – входить в совет директоров и продумывать стратегии развития. А они, как ни грустно это наблюдать, только бухгалтерию сопровождают, остальное, мол, подрядчики сделают. И при такой организационной структуре руководство верит, что скоро выйдет на мировые показатели эффективности...

Можно добавить и шестое, и седьмое, и десятое, и сотое. Но стоит ли? Отмеченного вполне достаточно, чтобы понять принципиальную разницу между подходом к процессу построения системы управления там, где этого требуют рынок и законы выживания, и у нас.

## На пути к вершине

Теперь немного пофантазируем и представим себе, что директор завода решил, что логотип его предприятия должен возглавлять мировой рейтинг по отрасли. И он берется за реорганизацию. Попробуем пройти этот путь вместе с ним.

Сначала надо понять, где находимся сейчас. Развивать всё и вся нереально, фокус и ресурсы должны быть направлены на наиболее важные направления. Тут и появляется первая проблема. Вооружаемся правильными методиками, например теорией ограничений по общим процессам, показателями эффективности по производственным участкам, и начинаем работать. Сразу выясняется, что построить дерево текущей реальности невероятно сложно, хотя на уровне подсознания все кажется простым и понятным, все проблемы налицо. Но попытка вскрыть истинную проблему упирается, как правило, в морально-этические аспекты. Нельзя же писать, что «директор принимает необоснованные решения», – неполиткорректно. Значит, все свалим на «проблемы с планированием».

Показатели эффективности производственных участков попросим посчитать мастеров цехов, даже методику им дадим, для ОЕЕ формула-то по сути несложная. В результате, вместо того чтобы выявить проблемы с неправильной загрузкой оборудования, структурой управления производством и т. п., начинаем искать «эффективную систему планирования». Даже не выделив ключевые проблемы.

А как надо? Надо поставить в цехах системы мониторинга,

MES на уровне привязки заказов (пока просто по факту) к состоянию оборудования, пригласить консультанта и вместе с ним выявить ключевые проблемы, истинные причины, выбрать цель. Но так никто не делает, увы.

К слову, основные тенденции в сегменте внедрения MES в промышленном производст-

во ограничение по размеру идентификатора, или путают производственный и бухгалтерский учеты и т. д. Так что это искусственно создаваемые проблемы.

Теперь представим, что дерево текущей реальности мы прорисовали корректно и сняли фактические показатели эффективности по производственным участкам. Путь даже пока

---

Надо поставить в цехах системы мониторинга, MES на уровне привязки заказов (пока просто по факту) к состоянию оборудования, пригласить консультанта и вместе с ним выявить ключевые проблемы, истинные причины, выбрать цель.

---

ве на российском рынке пока не сформировались. Можно отметить, что на зарубежных рынках появляются интеллектуальные контроллеры и облачные MES, правда, пока это разовые внедрения. Но работы в данном направлении активно ведутся.

Если говорить о факторах, которые с учетом специфики предприятия или отрасли нужно учитывать при выборе решений для MES, то при правильном подходе и корректном выстраивании процессов решение возникнет «само». Как известно, все «хорошие» решения созданы под «хороший» бизнес-процесс. Поэтому, как только процессы станут разумными и хорошими, тут же станет понятно, что из решений можно использовать, а что нет.

На практике часто отмечают сложности интеграции MES с вышестоящими системами. На мой взгляд, сложностей нет. Просто никто не любит думать об этом заранее. Вот и складывается ситуация, когда информация из MES некуда передать, или возникает «непреодолимое»

условные, так как нормирование еще не настроено, зарплатные нормы в расчет не берем. На этом этапе важно сдержаться и не бросаться наказывать нерадивых. Попытаться начать что-то «оперативно» исправлять – нажать врагов и ничего изменить не получится.

Аналогично и с анализом дерева текущей реальности. Надо выявить ключевые конфликты и, опираясь на мировые практики и стратегические инициативы, сформировать прорывные идеи, которые дадут толчок к развитию. При этом не следует путать инструменты стратегические и тактические. В нормальной организационно управляющей среде такие вещи, как поток создания ценности и оперативные показатели исполнения заказов, должны работать как тактические инструменты. А у нас их строят как стратегические, тратят на это много сил, средств и времени, в результате часто получают теоретическую модель, не реализуемую на практике. Тактические схемы на то и тактические,

что строятся от «как есть» и постепенно улучшаются, без глобальных изменений. Стратегические подразумевают план мероприятий по переходу из точки А в точку Б.

Вот и следующий вопрос: а куда же хотим прийти? На уровне идеи все понятно – к светлому будущему и лидерству на рын-

Если вы хотите стать номером один, необходимо стратегическое преимущество, а подглядеть его чаще всего получается в смежных отраслях. Вот почему стоит выбирать бизнес-туры многопрофильные, а не стараться найти референс только на точно такое, как у вас предприятие: так вы не станете лучше их.

результаты, которые обеспечат достижения будущей реальности. Ну и не забывать про сроки: конкуренты не спят.

Сделать «всё» нереально, поэтому важно не ошибиться на первом этапе с ключевыми проблемами, которые мешают стать лучше, не биться с ветряными мельницами, а решать проблемы.

Обратите внимание, что нигде мы не строили модель управления, танцуя от возможностей конкретной информационной системы. Информационная система появляется потом, когда в процессе анализа становится ясно, например, что надо сражаться за клиента через борьбу за качество и обеспечить автоматизированное формирование паспортов продукции, сделать его прозрачным для покупателя. Тогда понятно, что и когда должно регистрироваться, какие алгоритмы управления должны работать.

И только так. Теоретически, если все честно работают с нормативной скоростью и качеством, не воруют, не занимаются приписками, не... (здесь список из 174 пунктов), то никакая система контроля и управления не нужна. А если еще и поставщики не обманывают, привозят все вовремя...

---

## Надо выявить ключевые конфликты и, опираясь на мировые практики и стратегические инициативы, сформировать прорывные идеи, которые дадут толчок к развитию.

---

ке. Конкретные цели мало кто формулирует. Куда ни помотришь, кого ни послушаешь – сплошные «инновации». Порадуешься и снова окунаешься в ширпотреб из Европы, Америки и Азии.

Чтобы формализовать наши стремления, строим модель будущей реальности. Именно в ней задаются ключевые цели, показатели, составляющие успеха. Не забывая при этом о выбранной концептуальной стратегической инициативе. Построить такую модель, или «дерево будущей реальности» в терминах теории ограничений, – задача нетривиальная. Для ее решения нужно обладать широким кругозором: поехать по мировым выставкам, посмотреть другие предприятия, изучить показатели эффективности конкурентов.

Причем искать нужно не только в своей отрасли, но и в смежных. Вы же планируете стать номером один на рынке или в сегменте? Других целей быть не может, именно так учит теория менеджмента. Хотя у нас можно встретить цели типа «войти в двадцатку ведущих регионов страны по инновационности»...

И еще: помните о нежелательных явлениях, которые стремятся разрушить нашу идеалистическую модель. Для примера возьмите любую стратегию крупной корпорации. Одни плюсы. И ни слова про то, что завтра цена на нефть может упасть до 20 долларов и планам не суждено будет сбыться. Это риски, к которым надо быть готовым, а не делать вид, что их нет.

---

## Система производственного контроля и управления должна обеспечивать выполнение текущих задач по будущей реальности.

---

Будем считать, что дерево будущей реальности сформировано. Но нас ждет еще один сюрприз: знать, куда нужно идти, и правильно выстроить процесс перехода – разные вещи. На этом этапе важно продумать модель делегирования прав на проведение преобразований и обозначить промежуточные

Помечтали и возвращаемся к реальности. Система производственного контроля и управления должна обеспечивать выполнение текущих задач по будущей реальности, но не только. Помните про Деминга? А еще замечательную фразу Алисы в Зазеркалье: «Нужно бежать со всех ног, чтобы только оставаться

на месте, а чтобы куда-то по-пасть, надо бежать как минимум вдвое быстрее!» Это значит, что без мониторинга ситуации, анализа, корректировки целей и планов, назначения новых целевых показателей достигнутый успех будет очень недолгим.

Для того чтобы процесс управления был реальным, показатели процессов должны быть честными и беспристрастными, реальной должна стать информация в системе управления. И тут дело обычно не в том, что кто-то пытается обмануть, а в том, что «установленная система супер-КИС так не умеет, но мы придумали, как выкрутиться, мы вводим все хитрым способом, но в среднем все сходится».

К сожалению, это бывает чаще, чем хотелось бы. А ведь мы говорили про риски. И если было заранее известно о такой проблеме, почему ее сразу не отметить и не выбрать средства нейтрализации? Любая попытка заставить людей вводить нереальные данные приводит к негативным последствиям: теряется вера в КИС, появляются параллельные бумажки, отражающие «реальную реальность», а не виртуальную. Понятно, чем все закончится...

Ну и еще ложка дегтя про показатели. На различного рода КПЭ или КРІ в последнее время все помешались. Но в 99% случаев руководство не понимает, какие показатели ему нужны, все КПЭ выдуманы исполнителями под себя. И далее борьба с недостатками (тут и модное слово «муда», и «нежелательные явления», да и просто разгильдяйство) проходит под лозунгом «пчелы против меда», и число передовиков производства неуклонно растёт.

Надеюсь, все коллеги узнали. Теперь можно раскрыть тайну, о чем все. А о том, что один поэт высказал словами «все ищут смысла тайного извне». Поясню: когда надо посмотреть реальный опыт хорошей системы управления производством, все просят: «Нам нужно увидеть, как это

работает в России». Увы, российская производственная система еще не затмила TPS и, кроме показателей ОЕЕ 120% и более в «оперативной цеховой отчетности», нам гордиться пока нечем. Поэтому надо изучать опыт тех, кто смог найти силы и средства и пройти нелегкий путь развития на деле, а не в бумаж-

С расширением кругозора у нас совсем плохо, так как внимание к этому нулевое. Если что, в Яндекске можно посмотреть. В результате на предприятиях никто не видел ничего, кроме собственного обустройства, на выставки их не пускают, не учат (кроме необходимого минимума), литературы и жур-

---

Для того чтобы процесс управления был реальным, показатели процессов должны быть честными и беспристрастными, реальной должна стать информация в системе управления.

---

ных отчетах, построил модель производства, которая умеет работать по мировым критериям эффективности: ОЕЕ 85%, качество 99%, процент использования входных материалов 97%. Тут импортозамещению – бой!

## Вектор замещения импорта

Вместо того чтобы уповать на то, что приедет иностранный консультант с мировым именем, настроит весь процесс, ибо наши, доморощенные, не годятся, давайте будем учиться и развиваться сами. Да, это сложно. Да, найдется миллион (и не один) неотложных дел и сверхважных причин, по которым мы не можем прочитать полезную книжку. Но вот тут и надо биться за импортозамещение. Формировать группы компетенции, расширять кругозор, поощрять идеи и инициативы, устраивать обмен знаниями внутри организации, создавать атмосферу творчества и развития, «импортозамещать» привлеченные мозги своими, привлеченными за деловые качества, а не по родственной линии.

налов в доступе нет. Даже те, кто хочет развиваться, становятся однобокими специалистами в условиях постоянных попыток пробить стену непонимания. Зачем ехать в Пекин на выставку, если для таких поездок председатель профкома или отдел по внешним связям есть? А однобокость – это что значит? Правильно, ходят по кругу. А люди, которые не видели ничего лучше того, что у них есть, смогут построить новый лучший мир? Вопрос риторический.

Так что, коллеги, давайте делать все с умом: «импортозамещать» наши представления о том, что такое хорошо и что такое плохо на производстве, импортными, но при этом развивать собственный потенциал ИТР, управленцев и ИТ-специалистов, которые делают все по высшему разряду, знают мир и любят читать, для чего выучили английский язык. Их мотивация – бонус от того, что предприятие стало номером один на рынке, а не откаты и левая продукция. И больше ничего не нужно, остальное – просто рутина. Главное – не перепутать. ■

# Доверенные ПАПы



**Валерий АНДРЕЕВ,**  
заместитель директора по науке и развитию,  
ЗАО ИВК, к. ф.-м. н.

## Определение ПАП

Уж с чем с чем, а с понятием программно-аппаратная (реже аппаратно-программная) платформа (ПАП) наш ИТ-рынок определился и понимает его практически однозначно. Программно-аппаратная платформа состоит из взаимосвязанной совокупности следующих основных элементов:

- аппаратной составляющей платформы, представляющей собой комплекс технических средств, объединенных в одно отдельное средство вычислительной техники (СВТ);
- базового программного обеспечения, обеспечивающего заявленное функционирование комплекса технических средств, конфигурирование системы и реализующего другие системные функции;
- общесистемного ПО, реализующего описанный функционал платформы;
- программных средств разработчика;
- комплекта документации, регламентирующего процесс внедрения указанной платформы в состав

информационных систем заказчика, включая разрешительные документы по специальному применению платформы и сертификаты, устанавливающие соответствие требованиям регуляторов.

Аппаратная составляющая платформы определяется в основном архитектурой ее центрального процессора, а также аппаратными реализациями дополнительного оборудования в едином конструктиве СВТ, например сетевыми интерфейсами, адаптерами ввода-вывода, видеоадаптерами и интерфейсами и т. д.

Основным компонентом базового программного обеспечения (программной составляющей платформы) является операционная система (ОС), обеспечивающая работоспособность прикладного программного обеспечения на выбранном типе процессора, а также комплекс специальных программных средств (драйверов и специализированных библиотек), обеспечивающих функционирование аппаратного окружения процессора на платформе (контроллеры шины, сетевые адаптеры, интерфейсы ввода-вывода, мультимедиа и пр.).

К общесистемному ПО можно отнести прикладные программные средства мониторинга и контроля функционирования платформы, средства удаленной настройки, интерфейсы взаимодействия с пользователем, встроенные средства информационной безопасности и т. п.

В качестве средств разработчика обычно рассматриваются всевозможные SDK, режиссеры различных языков программирования (Си, Си++), отладчики, профилировщики и иные системные инструменты и библиотеки.

В связи с тем, что рассматриваемые платформы часто имеют узкую функциональную направленность, в состав документации обычно входит стандартный набор эксплуатационных документов,

формуляр изделия, описывающий и аппаратную, и программную составляющие платформы, прошедшие необходимые проверки, подтвержденные соответствующими сертификатами соответствия и предписаниями на эксплуатацию в информационных системах заказчика.

## Российские ПАП

Как видим, общие определения позволяют отнести к разряду ПАП практически любые СВТ, начиная от стандартных серверов, рабочих станций или терминалов вплоть до активного сетевого оборудования. И это совершенно справедливо. История развития ИТ-отрасли РФ знает десятки различных платформ, поставляемых ранее и живущих поныне. Многие из этих платформ изначально разрабатывались на принципах импортозамещения, например ПАП «Багет», «Эльбрус», «Комдив». Они ориентировались на различные типы центральных процессоров, имеющих различную архитектуру (например, x86, MIPS, ARM). При этом необходимо учитывать тот факт, что любой процессор характеризуется не только его архитектурой, т. е. набором команд, но и микроархитектурой – конкретной реализацией заявленного производителем набора команд. Прежние ПАП часто отличались оригинальными сочетаниями архитектуры и микроархитектуры, что, конечно же, не способствовало ни достаточной производительности изделий, ни широкому охвату прикладного ПО.

В итоге это привело к их повсеместному вытеснению более открытыми решениями, но далеко не во всех областях. Традиционные ПАП до сих пор работают в специализированных информационных системах, и кажется, что так будет всегда. Почему? Потому что здесь имеется неубиваемый довод, идущий со стороны информационной безопасности



и справедливый для любых закрытых платформ: чем более закрытой (менее популярной и распространенной) является платформа (или приложение), тем меньше экспертизы для ее взлома. Значительная часть несанкционированной экспертизы как раз привязана именно к архитектуре процессора атакуемой системы. Поэтому взлом закрытых систем весьма дорог с точки зрения трудозатрат, поскольку известно о них не много, а риск разоблачения нарушителя, чаще всего внутреннего, весьма велик. В подобном случае проблемы информационной безопасности ставятся выше проблем с производительностью, удобством работы и вообще целесообразностью применения такой платформы. Но если речь идет о закрытой информационной системе, то применение такой платформы можно считать вполне разумным.

Имеется и еще один важный аспект в относительной стабильности закрытых платформ на рынке – отработанная годами функциональность, отсутствие избыточных вычислительных мощностей и периферийного оборудования, минимум окружения среды исполнения. Эта тенденция полностью противоречит известному закону Мура, вернее, она его полностью игнорирует, утверждая, что первичность требований рынка очевидно вступает в противоречие с требованиями обеспечения информационной безопасности платформы. Почему? Потому что навязываемая потребителям парадигма постоянного наращивания функциональности аппаратного и программного обеспечения не позволяет сколько-нибудь долго оставаться в рамках надежных, апробированных решений с доказанной безопасностью. Конкуренция среди производителей элементной базы, аппаратного и программного обеспечения заставляет сокращать сроки разработки новых продуктов, что ведет к снижению качества тестирования и выпуску продуктов с различными известными дефектами, в том числе с дефектами защиты. Таким образом, нарочитая сложность многих ПАП является

основным препятствием на пути обеспечения их же безопасности. Этот разумный вывод и сегодня позволяет существовать многим специализированным ПАП, в особенности решающим задачи в режиме реального времени. Такие платформы обеспечивают минимум функциональности аппаратуры и ОС, достаточную для реализации основного функционала и сервисов безопасности.

## Безопасность ПАП

Когда-то считалось, что именно требования безопасности для платформ являются главными, определяющими. Однако со временем функциональность платформы все же победила. ПАП должна прежде всего работать, а уж после этого быть защищенной. Тогда платформы стали несколько более открытыми, потому что появились сначала UNIX-, а потом и вовсе Linux-подобные ОС в качестве практически стандартной основы для программной составляющей платформы (взамен, например, ОС2000 в ПАП «Багет»). Для систем реального времени в качестве базового ПО стали выступать QNX или специальный Linux реального времени. Вот тогда-то и вспомнили об архитектуре и микроархитектуре процессоров, тогда и появились несколько основных направлений развития отечественной аппаратной составляющей платформ – на основе MIPS- и ARM-архитектур в силу их коммерческой доступности. По понятным причинам основная на сегодня архитектура Intel x86 здесь не рассматривается. Сегодня этот очевидный тренд становится определяющим даже не столько в силу декларируемого импортозамещения, а просто в силу естественного прогресса отрасли.

Соответственно все проблемы ИБ тут же спроецировались на возможности ОС по разграничению доступа, работе с пользователями, контролю целостности и поддержке криптосредств. От аппаратной части ПАП сегодня требуется наличие штатных слотов расширения (PCI и пр.). Требования к базовому ПО ПАП уперлись в основном

в вопрос портирования тех или иных дистрибутивов Linux под известные архитектуры, поэтому, например, ПАП «Эльбрус» сегодня поддерживает не только свою собственную архитектуру, но и известную архитектуру SPARC. В то время как ПАП «Байкал» поддерживает и ARM, и MIPS. Для конечного пользователя, впрочем, разницы почти никакой, ведь базовым ПО на всех этих изделиях является одна из разновидностей ОС Linux, а вот для разработчиков разница в применяемом варианте ОС чрезвычайно существенна.

Широкие возможности ОС Linux привели к появлению довольно мощных ПАП типа «Холст», в состав общесистемного ПО которого входили уже и офисный пакет, и СУБД, а базовой ОС являлась ОС MC BC. Еще дальше продвинулась ПАП «Каркас», оснащаемая ОС Astra Linux, включающая в состав платформы к тому же дополнительное средство защиты информации АПМДЗ «Максим», осуществляющее контроль доступа к собственно СВТ и соответствующее СЗИ из состава ОС.

Что касается средств разработки ПО, то они стали достаточно стандартными и представляют собой 32- и 64-битные SDK, поставляемые в составе ПАП или запрашиваемые отдельно у разработчика. Прочие средства разработки отдаются на откуп третьим производителям из состава распространенных средств Open Source.

Вспомним еще, что указанные ПАП чаще всего применяются в защищенных информационных системах. Поэтому для их применения необходимо пройти сертификационные мероприятия на соответствие требованиям регуляторов, например ФСТЭК РФ или МО РФ. Все дистрибутивы базовой ОС проходят обязательную сертификацию по определенному (2-му или 3-му) уровню контроля недеklarированных возможностей (НДВ), а также по определенному (2-му или 4-му) классу защиты от несанкционированного доступа (НСД) в соответствии с руководящими документами ФСТЭК РФ. Межсетевые экраны (МЭ), которые также являются ПАП

по сегодняшним требованиям регуляторов, проходят проверки в соответствии с Руководящими документами для МЭ. Инструменты разработчика, различные офисные приложения, СУБД, серверы и другие программные пакеты также проходят сертификационные проверки и включаются в дистрибутив базовой ОС программной составляющей ПАП. Аппаратная составляющая чаще всего проходит специальные проверки на аппаратные закладки с выдачей предписания на эксплуатацию на объекте заказчика.

Конечно же, сертификация программного продукта сама по себе не гарантирует его полной безопасности. Дело в том, что значительная часть атак пользуется уязвимостями в ПО, которые не были своевременно выявлены разработчиками. Сертификация также не в состоянии выявить их в полном объеме. Особенно это касается закрытых платформ, использующих для своих программных компонентов закрытые репозитории собственных сборок Linux, оторванных от открытого сообщества и развиваемых по собственному усмотрению самими разработчиками ПАП. В связи с этим сегодня в качестве проверок таких программных средств в системе сертификации применяется проверка на защищенность ПО в соответствии с актуальными угрозами, совершенными атаками и опытом по их отражению из открытого сообщества. Вряд ли закрытое решение сможет выдержать такую проверку... И здесь требуется определенная степень открытости и доверенный репозиторий программных пакетов, на основе которого и можно собирать базовую ОС ПАП.

## Сетевые ПАП

Заметим, что буквально все активное сетевое оборудование также можно смело считать ПАП, поскольку оно полностью подходит под определение последней. Все изделия этой области развивались на проприетарных ОС, которые и сегодня закрыты (Cisco, Huawei и пр.). Раньше такие ОС были

действительно разными, но сегодня практически все являются клонами того же Linux. Разумеется, никаких проверок на соответствие требованиям регуляторов они не проходили, хотя известно несколько десятков недеklarированных возможностей изделий той же Cisco. Однако смысл применения ОС Linux в качестве базовой ОС, контролирующей активное сетевое оборудование и интегрирующей его в ИТ-ландшафт корпоративной ИС, ЦОД или иного объекта, еще более значим, причем не только с точки зрения информационной безопасности.

Сегодняшний долгосрочный тренд в этой области ПАПостроения – реализация сетевой инфраструктуры как единой программно-аппаратной платформы и предоставления функционала сквозных (end-to-end) сетевых услуг. В таком случае система управления инфраструктурой должна централизовать все высокоуровневые функции управления, а также иметь полную модель управляющих данных и параметров состояния всей сети в целом. Реализация такого подхода приводит к созданию ПАП на базе сетевой ОС (Network Operating System, NOS) Linux, что открывает широкие возможности для гибридного управления, когда высокоуровневые функции делегируются выше и координируются из общего центра, а на местах есть полный набор управляющих данных для полноценного выполнения всех функций, присущих сетевой ПАП. То есть каждое сетевое устройство имеет собственное управление, что позволяет сохранить классический децентрализованный подход к построению сетей и сохраняет отказоустойчивость и надежность сети на столь же высоком уровне. При этом обеспечивается существенная возможность централизованного управления всеми устройствами сразу посредством специализированных безагентских систем управления конфигурациями (например, Ansible). Заметим, что таким образом можно управлять любыми СБТ, функционирующими под управлением различных ОС, включая ОС Linux и ОС MS Windows.

Такое решение по управлению (конфигурированию, развертыванию, обновлению) сетевой инфраструктурой базируется на одном новом и существенном факте из жизни современных открытых платформ: они должны иметь внутреннюю способность к быстрому изменению под влиянием внешних быстро меняющихся условий функционирования, частому изменению настроек не только конкретного коммутатора, маршрутизатора или другого активного элемента сетевой инфраструктуры, но и целых групп сетевого и серверного оборудования и установленного на нем ПО. Более того, имеет место также резкое сокращение интервалов между внедрениями новых версий ПО. К этому приводят различные причины, например, распространение обновлений безопасности, ускоренное добавление новых функций, интеграция различных элементов ИС, автоматизация и роботизация операций по администрированию.

## Заключение

Сейчас необходимым условием новой парадигмы управления является по меньшей мере функционирование аппаратного компонента ПАП под управлением операционной системы Linux. Тогда вполне достижимым становится согласованное администрирование и даже оркестрация всей инфраструктуры ИС, начиная с прикладного уровня. Выгоды такого подхода чрезвычайно велики. Однако же здесь возникает определенная особенность реализации функций ИБ: складывается впечатление, что появляется своего рода новый глобальный администратор, имеющий широкие полномочия и технические возможности по настройке СБТ (в том числе и СЗИ) с помощью систем управления конфигурациями и других высокоуровневых инструментов. Это не здорово с точки зрения ИБ, но сколько еще вопросов предстоит решить на пути внедрения всего того потенциала, который называется сегодня загадочным, еще не до конца понимаемым термином – DevOps... ■

## АШАН планирует управлять персоналом с помощью SAP HCM

Компания SAP и АШАН Россия, одна из крупнейших в России торговых сетей, подписали меморандум о партнерстве в рамках Петербургского международного экономического форума (ПМЭФ-2017). Сотрудничество будет направлено на продолжение инновационного развития проекта SAP в сфере управления персоналом.

Меморандум включает в себя новый этап развития существующей системы по управлению персоналом SAP HCM, совместный проект по внедрению которого начался в октябре 2016 г. Основная цель – построение единой централизованной ИТ-системы, унификация HR-процессов, сокращение сроков формирования и предоставления отчетности, а также оптимизация затрат. Система охватит 41 тыс. сотрудников всех форматов магазинов российской сети: гипермаркетов, суперсторов, супермаркетов и магазинов «у дома».

В продолжение сотрудничества между компаниями будут определены дальнейшие этапы развития решения. Компании рассматривают возможности проведения совместного анализа функций HR и их цифровой трансформации: сервисов самообслуживания, процессов

повышения качества постановки целей и оценки сотрудников, пересмотра зарплат, формирования кадрового резерва, рекрутинга, а также перспективы создания корпоративного портала. Используя решение SAP, АШАН Россия планирует повысить вовлеченность сотрудников и производительность труда.

«Мы довольны первыми результатами нашего сотрудничества с компанией SAP. Как инновационная компания, мы понимаем важность применения облачных технологий, которые позволяют находить нам таланты, развивать их и последовательно вести по карьерному пути», – прокомментировал Жан-Пьер Жермен, президент АШАН Россия.

«Проект внедрения SAP HCM уже заложил основу для модернизации HR-процессов АШАН Россия. Продолжение нашего сотрудничества в этой области позволит компании не только построить единую централизованную HR-систему, но и создать главное конкурентное преимущество на современном рынке – счастливого сотрудника, который любит свою работу и компанию, в которой он имеет возможность развиваться», – отметил Павел Гонтарев, генеральный директор SAP СНГ.

## Виртуальная реальность внедряется в реальном секторе экономики

Итоги первого в России масштабного исследования востребованности технологий виртуальной реальности (VR) в российской экономике представлены на панельной сессии «Реальные продажи в дополненной реальности» в рамках Петербургского международного экономического форума.

Проект реализован участниками VR-Консорциума: компанией КРОК и Институтом современных медиа (MOMRI) совместно с порталом «Вести Экономики» в период с марта по май 2017 г. В ходе исследования было опрошено 247 руководителей и специалистов различного профиля, представляющих более 200 крупнейших компаний России из всех ключевых отраслей экономики.

Главный итог исследования – уровень осведомленности представителей крупнейших российских компаний и отраслей о возможностях применения технологий виртуальной реальности в бизнесе высок, причем как в реальном секторе, так и в сфере услуг. Почти две трети – 65% опрошенных знают о возможности применения технологий VR и AR на предприятиях. Наибольшую осведомленность о реальных кейсах внедрения VR

в технологические и бизнес-процессы продемонстрировали представители таких отраслей, как металлургия, машиностроение, строительная отрасль, энергетика,

транспортные компании, а также финансовый сектор и ИТ/Телеком.

Почти четверть – 24% представителей российского бизнеса сказали, что в их компаниях уже внедрены или планируются к внедрению технологии виртуальной реальности (15% принявших участие в опросе сообщили, что в их компаниях подобные технологии уже внедряются или внедрены, а 9% опрошенных сказали, что такое внедрение планируется в обозримой перспективе).

41% опрошенных ответили, что, хотя технологии виртуальной реальности не внедряются в их бизнесе, они знакомы с примерами такого внедрения в других компаниях. Об использовании VR в бизнесе не слышали 35% респондентов. Большая часть предприятий, уже работающих с VR- и AR-технологиями, представляет реальный сектор экономики (машиностроение, добыча и переработка, энергетика). В число основных сфер внедрения технологий вошли обучение персонала, проектирование и маркетинг.



# Актуальные вопросы защиты государственных информационных систем в период перехода на импортозамещающие технологии



**Сергей ОВЧИННИКОВ,**  
директор по маркетингу Центра защиты  
информации, ГК «Конфидент»

## Защита государственных информационных систем. Теория и практика

Существует несколько подходов к отнесению ИС к ГИС и их классификации. Они изложены в № 149-ФЗ, постановлениях Правительства, приказах и руководящих документах ФСТЭК России и других документах. Основными (но не единственными) документами, наиболее полно описывающими требования по защите ГИС, являются: приказ ФСТЭК России от 11.02.2016 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в редакции приказа ФСТЭК России от 15.02.2017 № 27)

С момента установления запрета на закупки импортного ПО прошло уже полтора года. ИТ-инфраструктура заказчиков постепенно меняется. В статье представлен довольно широкий взгляд на проблемы, с которыми могут столкнуться операторы государственных информационных систем (ГИС), планирующие перейти на импортозамещающие технологии.

Компания «Конфидент» занимается вопросами защиты информации в госсекторе 25 лет. За прошедшие годы накоплен большой опыт реализации многих тысяч проектов в качестве разработчика и производителя сертифицированных средств защиты информации (СЗИ). Этот опыт позволяет говорить о тенденциях в указанной сфере, вскрывать проблемы, которые не видны с первого взгляда, давать рекомендации заказчикам.

и методический документ «Меры защиты информации в ГИС», утвержденный ФСТЭК России 11 февраля 2014 г. Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении. Для защиты информации в ГИС используются средства защиты информации (СЗИ), которые сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России. Одним из мероприятий для обеспечения защиты информации, содержащейся в ГИС, является аттестация информационной системы по требованиям защиты информации.

Для защиты ГИС применяются сертифицированные СЗИ следующих видов: средства защиты

информации от несанкционированного доступа (СЗИ НСД), средства антивирусной защиты (САВЗ), средства доверенной загрузки (СДЗ), межсетевые экраны (МЭ) и системы обнаружения и предотвращения вторжений (СОВ), средства контроля съемных машинных носителей информации (СКН), ОС со встроенными механизмами защиты, а также средства анализа защищенности.

На рис. 1 представлена динамика появления на рынке отдельных видов сертифицированных решений по защите информации. По горизонтальной шкале отмечены даты утверждения требований. По вертикальной шкале – количество решений, доступных для приобретения. Пунктирной линией показан период, в течение которого осуществляются разработка и сертификация решения вендором. Эти периоды в целом имеют тенденцию к уменьшению. На текущий момент пока нет ни одной ОС, сертифицированной по новым требованиям, вступающим в силу с 1 июня 2017 г.

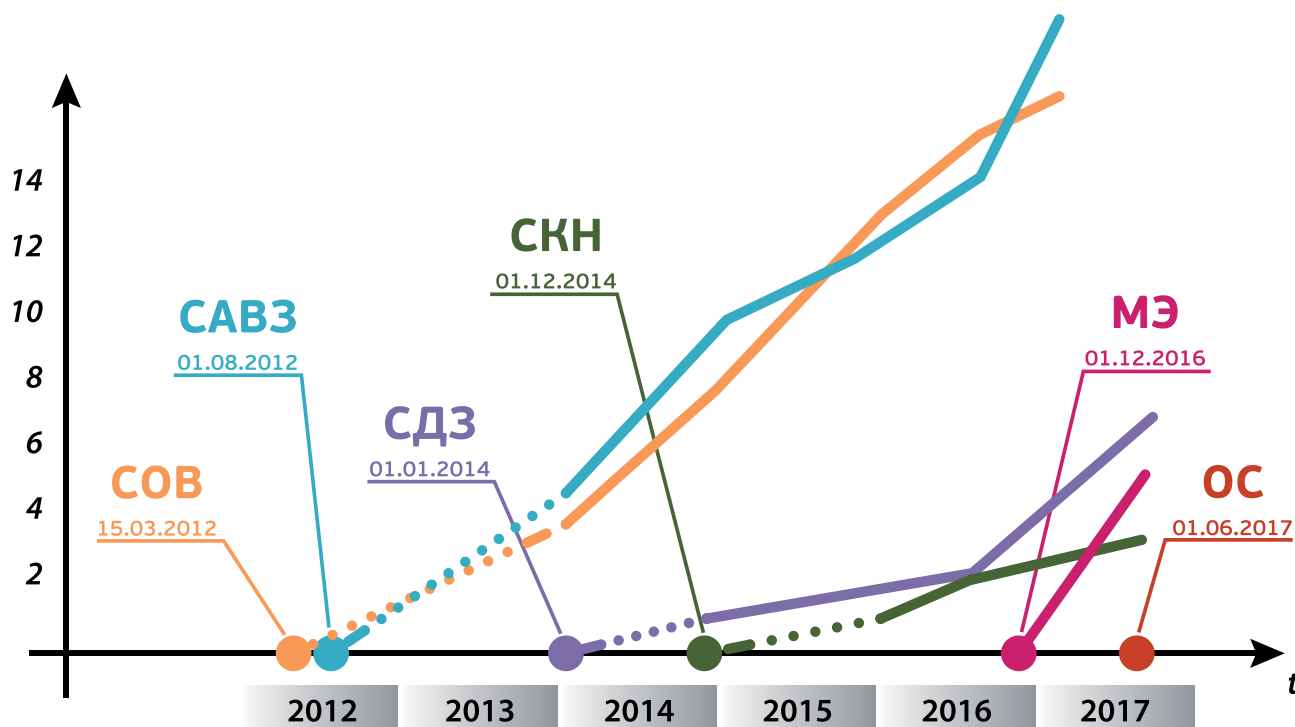


Рис. 1. Динамика появления на рынке отдельных видов сертифицированных решений по защите информации

Для каждой ГИС определяется уникальный набор защитных мер, в том числе с учетом класса ГИС. Таким образом, в каждой конкретной ситуации необходим некий набор сертифицированных решений для защиты информации. Можно с уверенностью сказать, что в подавляющем большинстве случаев для защиты ГИС 1-го и 2-го классов в соответствии с приказом № 17 ФСТЭК России требуются сертифицированные СЗИ от НСД, САВЗ, СКН, СДЗ, МЭ и СОВ.

## Переход на импортозамещающие технологии

В ноябре 2015 г. был установлен запрет на закупки иностранного программного обеспечения для государственных и муниципальных нужд, а с 2016 г. заработал Реестр российских программ для ЭВМ и БД (далее – Реестр). Отдельного рассмотрения заслуживает вопрос критериев отнесения ПО к российскому. Федеральный закон от 29 июня 2015 г. № 188-ФЗ однозначно определяет такие критерии, которые используются при рассмотрении

заявок на включение ПО в Реестр российского ПО. Среди них используются: принадлежность исключительных прав российским лицам, возможность свободной реализации на территории РФ, ограничения по суммам выплат иностранным лицам, а также отсутствие в программе сведений, составляющих государственную тайну. В списке критериев нет ни слова про «написание программного кода российскими разработчиками», зато есть указание на то, что Правительством Российской Федерации могут быть установлены дополнительные требования. Таким образом, не ясно, какая часть исходного кода российских программ написана российскими разработчиками. Этот вопрос особенно актуален для программ, основанных на свободном ПО (СПО).

Стремление государства перейти на отечественное ПО и поддержать отечественного разработчика понятно, и его можно только приветствовать. Вместе с тем, реалии таковы, что на текущий момент подавляющее большинство программ в инфраструктуре заказчиков, в том числе ПО, включенное в Реестр, работает под управлением ОС

Microsoft Windows. Отказываясь от использования ОС Microsoft Windows, заказчики вынуждены отказываться и от ПО российского производства из-за проблем с технической совместимостью. Чтобы действительно перейти на отечественное ПО, необходимо развивать и отечественные ОС, и прикладное ПО под управлением отечественных ОС (включая офисное), и средства разработки, и системное ПО, в том числе системы защиты информации. Процесс этот достаточно долгий, тем более если его реализовывать в масштабах всей страны.

На текущий момент в Реестре содержится 30 отечественных ОС различного назначения. Среди них как серверные ОС, так и ОС для офисного использования на рабочих местах пользователей, а также ОС для решения специализированных задач. Является ли российское происхождение ОС если не гарантией, то хотя бы фактором, указывающим на более высокий уровень защиты информации, обрабатываемой на защищаемых рабочих местах? Ответ на этот вопрос содержится в письме Минкомсвязи России «О необходимости соблюдения государственными заказчиками требований по защите

Таблица 1

Операционная система	Техническая совместимость со сторонними решениями для защиты информации				
	САВЗ	СКН	СДЗ	МЭ	СОВ
Альт Линукс СПТ 7.0	+	-	+	+	*
Astra Linux Special Edition	+	-	+	*	*
РОСА SX «КОБАЛЬТ» 1.0	+	-	+	*	*
ОС «Синергия»	+	-	+	*	*

\* поддерживаются только периметровые решения уровня сети (логических границ сети).

информации» от 15 марта 2016 г. № НН-П11-4736. В документе, в частности, говорится о необходимости самостоятельного принятия решений государственными и муниципальными заказчиками в части необходимых требований по защите информации, содержащейся в ГИС, в том числе в части выбора из Реестра общесистемного, прикладного, специального программного обеспечения, информационных технологий, а также средств защиты информации в соответствии с требованиями приказа № 17 ФСТЭК России, а также № 149-ФЗ от 27 июля 2006 г. и ПП-1119 от 1 ноября 2012 г. Другими словами, выбор ПО из Реестра никак не связан с защитой информации, которая в соответствии с приказом № 17 ФСТЭК России является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации.

С другой стороны, в Реестре есть ОС с действующими сертификатами ФСТЭК России. Приведем список этих ОС с указанием уровней сертификации и срока действия сертификата соответствия ФСТЭК России (по данным Государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00):

- операционная система Альт Линукс СПТ 7.0 – сертифицирована по 4-му классу РД СВТ, по третьему уровню отсутствия НДВ и ТУ. Сертификат действителен

до 14 марта 2023 г. (на сайте разработчика указан срок 22 марта 2020 г. – Прим. авт.);

- операционная система специального назначения Astra Linux Special Edition – сертифицирована на соответствие РД СВТ по 3-му классу и РД НДВ по второму уровню. Сертификат действителен до 27 января 2018 г.;
- операционная система РОСА SX «Кобальт» 1.0 со встроенными средствами защиты от несанкционированного доступа к информации – сертифицирована на соответствие РД СВТ по 5-му классу и РД НДВ по четвертому уровню контроля. Сертификат действителен до 7 июля 2017 г.;
- программное изделие «Операционная система с открытым программным кодом

«Синергия» – сертифицировано на соответствие РД СВТ по 3-му классу и РД НДВ по второму уровню. Сертификат действителен до 13 декабря 2019 г.

Как видим, на текущий момент указанные ОС имеют сертификаты по РД СВТ и РД НДВ. Это означает, что для построения системы защиты информации в ГИС 1-го и 2-го классов необходимо применять другие сертифицированные СЗИ, включая САВЗ, СКН, СДЗ, МЭ и СОВ, поскольку в составе российских ОС нет соответствующих сертифицированных защитных механизмов. С какими сторонними СЗИ имеется техническая совместимость у отечественных ОС? Во многих случаях совместимость достигается с СДЗ уровня платы расширения и антивирусами. С межсетевыми экранами ситуация чуть хуже, поскольку в части персональных межсетевых экранов не у всех российских ОС есть совместимость с такими решениями. Системы обнаружения и предотвращения вторжений уровня узла не поддерживаются. Средства контроля съемных машинных носителей информации также не поддерживаются. Техническая совместимость на основе данных, приведенных на официальных сайтах производителей российских ОС, содержится в табл. 1.

Таблица 2

Top 50 Products By Total Number Of «Distinct» Vulnerabilities in 2016

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	523
2	Debian Linux	Debian	OS	319
3	Ubuntu Linux	Canonical	OS	278
4	Flash Player	Adobe	Application	266
5	Leap	Novell	OS	259
6	Opensuse	Novell	OS	228
7	Acrobat Reader Dc	Adobe	Application	227
8	Acrobat Dc	Adobe	Application	227
9	Acrobat	Adobe	Application	224
10	Linux Kernel	Linux	OS	217
11	Mac Os X	Apple	OS	215
12	Reader	Adobe	Application	204
13	Chrome	Google	Application	172
14	Windows 10	Microsoft	OS	172

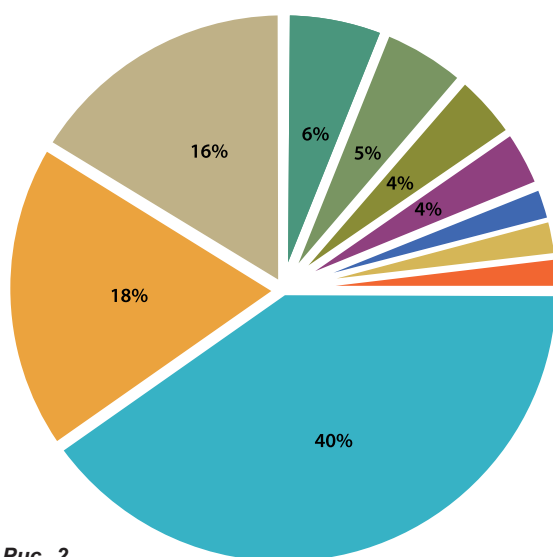


Рис. 2.

Таким образом, для обеспечения защиты информации, содержащейся в ГИС, во многих случаях аттестация информационной системы по требованиям защиты информации ФСТЭК России не представляется возможной.

Даже если не принимать в расчет вопросы, связанные с аттестацией рабочих мест, обычно считают, что российские ОС, основанные на СПО, являются наиболее безопасными, так как в них не может быть программных закладок по причине наличия доступа к их исходному коду, в них меньше уязвимостей. В табл. 2 приведена статистика уязвимостей CVE Details за 2016 г.

Если обратиться к Банку данных угроз безопасности информации ФСТЭК России (<http://bdu.fstec.ru/charts>) в части количества критических уязвимостей в ПО различных производителей, то ситуация со свободным ПО в отношении ОС схожая. См. рис. 2.

Посмотрим, как устраняются уязвимости. Производители выпускают бюллетени по безопасности. У Astra Linux за 2016 г. выпущен один бюллетень по безопасности ([http://www.astra-linux.com/wiki/index.php/Security\\_Updates\\_for\\_1.5](http://www.astra-linux.com/wiki/index.php/Security_Updates_for_1.5)), в котором содержится обновление по безопасности с исправлением 11 уязвимостей из БДУ ФСТЭК России. За 2017 г. выпущен пока только один бюллетень – он является кумулятивным

обновлением, в котором исправлено чуть более 300 уязвимостей. Для Альт Линукс СПТ 7.0 за 2016 г. выпущен один бюллетень по безопасности, как и за 2017 г. (<https://cve.basealt.ru/>). На сайтах разработчиков РОСА SX «Кобальт» 1.0 и ОС «Синергия» найти информацию об обновлениях по безопасности не удалось. Для сравнения: у компании Майкрософт за 2016 г. около 140 обновлений различного ПО (<http://www.cvedetails.com/microsoft-bulletins/2016/>), сгруппированных в бюллетени, которые выпускаются ежемесячно на постоянной основе.

В соответствии с требованиями, изложенными в приказе № 17 ФСТЭК России, необходимо выявлять и устранять уязвимости в информационных системах. Такие проверки должны проводиться на различных этапах жизненного цикла ИС. Любая такая проверка – это затраты. Чем больше уязвимостей в ИС, тем выше совокупная стоимость владения ИС. Более того, процесс устранения уязвимостей в сертифицированных СЗИ организационно зачастую более затратный, чем устранение уязвимостей в любом другом ПО. Если в качестве сертифицированного СЗИ мы рассматриваем ОС, а не накладное СЗИ, то ситуация усугубляется многократно ввиду сложности реализации самого продукта и количества уязвимостей

в нем. Дело в том, что уязвимости в накладных решениях – это единичные случаи, которые встречаются крайне редко.

## Выводы

Переход на импортозамещающие технологии действительно оказывает влияние на ИТ-инфраструктуру заказчиков. Доля организаций, где используются ОС на базе свободного ПО, увеличивается. Вместе с тем, статистика по уязвимостям говорит не в пользу свободного ПО. Возможно, поэтому регуляторы (в частности, ФСТЭК России) уделяют большое внимание вопросам поиска и устранения уязвимостей в информационных системах.

С точки зрения реализации мер по защите информации в соответствии с требованиями регуляторов пока рано говорить о том, что переход на импортозамещающие технологии близок к завершению. До сих пор нет необходимого количества сертифицированных СЗИ, которые способны обеспечить полноценную защиту ГИС, построенных на базе российских ОС. Встроенных в ОС сертифицированных защитных механизмов еще недостаточно для обеспечения защиты информации. Должно пройти некоторое время, чтобы на рынке сертифицированных СЗИ появились соответствующие решения. ■

# Импортозамещение ИТ- и ИБ-решений в ОПК



**Андрей ПРОЗОРОВ,**  
руководитель экспертного направления,  
компания Solar Security

## Доктрина импортозамещения

Речь идет в первую очередь о необходимости обеспечивать информационную безопасность ИТ-инфраструктуры объектов ОПК и потребности в разработке и реализации программы импортозамещения. Эти задачи отражены в актуализированных верхнеуровневых документах, определяющих развитие отраслей ИТ и информационной безопасности в России: Доктрине информационной безопасности Российской Федерации (утверждена указом Президента Российской Федерации от 5 декабря 2016 г. № 646) (далее – Доктрина) и указе Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» (далее – Стратегия).

Несколько лет назад я принимал участие в разработке проекта документа «Концепция создания, развития и использования информационных технологий в оборонно-промышленном комплексе Российской Федерации на период до 2020 года». Документ содержал описание состояния, проблем и тенденций использования информационных технологий в ОПК, а также направления развития, цели и первоочередные задачи. К сожалению, итоговая версия документа не была принята и утверждена, но важные идеи, заявленные в нем, не потеряли актуальности.

В частности, в Доктрине заявлена проблема «высокого уровня зависимости отечественной промышленности от зарубежных информационных технологий». Документ предлагает ориентироваться на «совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности». Это должно стать одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности.

В Стратегии развития информационного общества в качестве национального приоритета названо обеспечение безопасности граждан и государства. Один из методов достижения поставленной цели – создание и применение российских информационных и коммуникационных технологий. А для устойчивого функционирования информационной инфраструктуры РФ определена необходимость в «замене импортного оборудования, программно-обеспечения и электронной компонентной базы российскими аналогами, обеспечение технологической и производственной

независимости и информационной безопасности». Отмечена также необходимость в том, чтобы «обеспечить использование российских информационных и коммуникационных технологий в органах государственной власти РФ, компаниях с государственным участием, органах местного самоуправления».

Эти верхнеуровневые положения говорят о том, что компаниям оборонно-промышленного комплекса РФ уже сейчас стоит задуматься о разработке собственных программ импортозамещения.

## Импортозамещение реестром

В России приняты Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения,



происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»). Помимо прочего они устанавливают правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных (<https://reestr.minsvyaz.ru>, далее – Реестр). Именно на него и стоит ориентироваться организациям при выборе программного обеспечения. 16 сентября 2016 г. Председатель Правительства РФ Дмитрий Медведев подписал постановление о приоритете товаров российского происхождения.

Реестр функционирует с 1 января 2016 г., и на начало мая 2017 г. в нем уже зарегистрировано более 3500 наименований программного обеспечения по следующим классам:

- BIOS и иное встроенное программное обеспечение (33 зарегистрированных решения);
- встроенное программное обеспечение телекоммуникационного оборудования (14 зарегистрированных решений);
- геоинформационные и навигационные системы (86 зарегистрированных решений);
- операционные системы (30 зарегистрированных решений);
- утилиты и драйверы (63 зарегистрированных решения);
- средства обеспечения облачных и распределенных вычислений, средства виртуализации и системы хранения данных (47 зарегистрированных решений);
- серверное и связующее программное обеспечение (215 зарегистрированных решений);

Таблица. Разбиение средств защиты по классам	
Тип средства обеспечения ИБ	Примеры ПО в Реестре
Средства антивирусной защиты	Dr.Web, Kaspersky, NANO «Антивирус Pro», Positive Technologies MultiScanner
DLP-системы	Solar Dozor, InfoWatch Traffic Monitor, LanAgent, Kaspersky DLP, Zecurion DLP, КИБ «Серчинформ», «Гарда Предприятие»
SIEM-системы	MaxPatrol Security Information and Event Management, KOMRAD Enterprise SIEM («Эшелон»), Security Capsule SIEM
Средства анализа кода приложений	Solar inCode, InfoWatch ApperCut, Positive Technologies Application Inspector, АК-BC 2, IRIDA Sources
IDM-системы	Solar inRights, IDM-система «Куб», Avanpost IDM
Средства защиты от несанкционированного доступа / Средства доверенной загрузки	Secret Net, Dallas Lock, ПАК «Соболь», «Блокхост-МДЗ», «МДЗ-Эшелон»,
Средства анализа защищенности (сканеры)	«Сканер-ВС», MaxPatrol, xSpider, RedCheck
Межсетевые экраны и средства защиты каналов связи (VPN)	«Рубикон», TrustAccess, МЭ ИКК, ИБК «Кольчуга», «Интернет Контроль Сервер», Positive Technologies Application Firewall, «Континент», VIPNet Coordinator, Dozor Web-proxy

- системы управления базами данных (31 зарегистрированное решение);
- системы мониторинга и управления (351 зарегистрированное решение);
- средства обеспечения информационной безопасности (323 зарегистрированных решения);
- средства подготовки исполнимого кода (19 зарегистрированных решений);
- средства версионного контроля исходного кода (10 зарегистрированных решений);
- библиотеки подпрограмм (SDK) (30 зарегистрированных решений);
- среды разработки, тестирования и отладки (62 зарегистрированных решения);
- системы анализа исходного кода на закладки и уязвимости (13 зарегистрированных решений);
- прикладное программное обеспечение общего назначения (489 зарегистрированных решений);
- офисные приложения (163 зарегистрированных решения);
- поисковые системы (70 зарегистрированных решений);
- лингвистическое программное обеспечение (52 зарегистрированных решения);
- системы управления проектами, исследованиями, разработкой, проектированием и внедрением (305 зарегистрированных решений);

- системы управления процессами организации (1172 зарегистрированных решения);
- системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных (539 зарегистрированных решений);
- информационные системы для решения специфических отраслевых задач (2236 зарегистрированных решений).

Несмотря на то что Реестр постоянно пополняется и развивается, работать с ним не всегда удобно. Так, например, по классу «Средства обеспечения информационной безопасности» зарегистрировано 423 продукта, но как найти среди них отдельные типы программного обеспечения – средства антивирусной защиты, средства анализа защищенности, межсетевые экраны и др.? Для ориентира можно использовать таблицу.

Как видим, организациям, ориентирующимся на использование российских программных продуктов для обеспечения информационной безопасности, уже есть из чего выбирать. Аналогично и по другим классам программного обеспечения в Реестре.

Напомним, что существует ряд директив для государственных организаций в отношении предпочтений отечественному ПО, которые среди прочего содержат:

## — Мнение специалиста —



### Дмитрий БИРЮКОВ,

директор направления информационной безопасности, группа «Астерос»

Автор абсолютно справедливо поднимает вопрос о необходимости более жесткого регламентирования использования отечественных разработок программных и технических средств защиты предприятиями ОПК как в АСУ ТП, так и в той продукции, которую они выпускают. В качестве дополнения хотелось бы отметить, что современные программные средства вычислительной техники, в том числе средства защиты информации, носят многофункциональный характер. Поэтому для повышения удобства пользования Единым реестром российских программ для ЭВМ и баз данных было бы не лишним доработать заложенные в нем поисковые механизмы. Кроме того, для обеспечения информационной безопасности ИТ-инфраструктуры объектов ОПК следует обратить внимание на уже назревший вопрос о государственной поддержке вузов, ведущих подготовку специалистов в области программирования перспективных процессоров, которые будут использоваться в изделиях вооружения и военной техники.

- обязательство в десятидневный срок со дня получения указанных директив инициировать проведение заседаний советов директоров (наблюдательных советов) акционерного общества с включением в повестку дня вопроса «О закупках отечественного конкурентоспособного ПО, необходимого для деятельности акционерного общества»;
- текст о необходимости внесения изменений в Положение о закупочных процедурах, проводимых для нужд акционерного общества:
  - ♦ закупка «только такого ПО, сведения о котором включены в единый реестр российских программ для электронных вычислительных машин и баз данных...»;
  - ♦ за исключением случаев, когда «в реестре отсутствуют сведения о ПО, соответствующем тому же классу», или «ПО неконкурентоспособно (по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке ПО)»;
  - ♦ если ПО попадает под указанные исключения, то необходимо не позднее чем в течение семи дней с даты

размещения информации о закупке опубликовать «основание невозможности соблюдения ограничения на допуск ПО, происходящего из иностранных государств». Таким образом, если это пока не серьезные ограничения на закупку, то, во всяком случае, уже «строгая рекомендация» приобретать решения из реестра отечественного ПО.

## Реестр промышленности

Однако в отечественном ОПК до сих пор используются в основном импортные решения. По данным TAdviser, зарубежные производители ПО ежегодно получают от российских потребителей около 285 млрд руб. лицензионных отчислений (45% общего объема российского ПО), 30% этих отчислений приходится на госсектор. Например, по статистике Минкомсвязи, доля импорта клиентских и мобильных операционных систем в целом в России составляет 95%, серверных – 75%. В отечественном ОПК 70% электронных компонентов – импортного производства. Между тем санкции, наложенные на оборонно-промышленные предприятия иностранными государствами, наглядно

продемонстрировали все риски столь широкого и повсеместного внедрения зарубежных решений.

Виталий Сазонов, руководитель управления информационных технологий «Объединенной приборостроительной корпорации» ГК «Ростех», также отмечает, что доля иностранных решений в области военной техники, телекоммуникационного оборудования и ПО, применяемых сегодня в России, критически велика и достигает в большинстве сегментов 90% и выше. Причем не секрет, что зачастую зарубежная техника и ПО таят в себе незадекларированные возможности в части негласного доступа к информации и передачи данных. В связи с этим представляется разумным выполнение оборонно-промышленными предприятиями следующих процедур:

- инвентаризация ПО (общий перечень, срок окончания лицензий, стоимость продления, наличие сертификатов ФСТЭК, количество пользователей);
- определение своего подхода к импортозамещению: заменить все, заменить критичные узлы или заменить только базовые продукты, установить средства контроля российского производства;
- выбор классов ПО для импортозамещения, изучение ПО соответствующего класса;
- разработка и реализация стратегии и плана импортозамещения.

## Заключение

Остается только выразить надежду, что программа импортозамещения ИТ- и ИБ-решений получит максимально широкое распространение в ОПК и дальнейшая информатизация оборонно-промышленных предприятий будет осуществляться на базе отечественных решений. Особенно это относится к средствам защиты информационных систем, выбор которых в приведенном выше реестре достаточно широк. ■

## Опубликовано исследование IDC по российскому рынку ПО ИСУП

Компания IDC опубликовала исследование, посвященное российскому рынку программного обеспечения информационных систем управления предприятием (ПО ИСУП) – Russia Enterprise Application Software Market 2017–2021 Forecast and 2016 Vendor Shares. В отчете представлена информация о долях поставщиков как на всем рынке, так и на его сегментах – рынках приложений для управления ресурсами предприятия, цепочками поставок, операциями на производстве, взаимоотношениями с клиентами, а также приложений для бизнес-аналитики. Кроме того, документ содержит обзор потребителей ПО ИСУП по отраслям и размерам бизнеса, а также прогноз развития рынка до 2021 года.

По данным IDC, в 2016 году объем рынка сократился на 1,1% до 632,72 млн. долларов. При этом в рублевом выражении объем рынка вырос на 8,8%. В пятерке лидеров поставщиков ПО ИСУП изменений не произошло, а российским поставщикам удалось

немного улучшить свои позиции. В 2016 году по-прежнему две трети рынка приходились на приложения для управления ресурсами предприятия и бизнес-аналитики.

Крупнейшими потребителями ПО ИСУП остаются предприятия непрерывного производства и розничной торговли. Их совокупная доля на рынке составила около 44%. В 2016 году в пятерку крупнейших также вошли дискретное производство; сельское хозяйство, строительство и добывающая отрасль; энергетика.

Улучшение общей экономической ситуации хорошо сказалось как на всем рынке ИТ, так и на этом рынке. «Среднегодовой темп роста рынка ПО ИСУП до 2021 года будет положительным, – отмечает старший аналитик IDC Денис Масленников. – Мы ожидаем, что уже в 2019 году этот рынок начнет постепенное восстановление».

<http://idcrussia.com/ru/>

## Airbus совместно со «СКАНЭКС» подписали соглашение с Яндексом

«СКАНЭКС» и Airbus Defence and Space подписали соглашение с Яндексом на предоставление доступа к спутниковому покрытию площадью более 180 млн км<sup>2</sup> на основе платформы One Atlas.

One Atlas – это ежегодно обновляемый и доступный в онлайн-режиме базовый слой, состоящий из высококачественных унифицированных спутниковых изображений земной поверхности. Данные One Atlas будут интегрированы в «Яндекс.Карты»: это обеспечит доступ к актуальным изображениям со спутников SPOT 6/7 с разрешением 1,5 м на пиксель и данным Pléiades с разрешением 0,5 м на пиксель.

«На Яндекс.Картах уже есть подробные схемы большинства стран мира со спутниковым слоем, – прокомментировал соглашение Андрей Стрелков, руководитель управления геопродуктов Яндекса. – Доступ к актуальным и высококачественным снимкам

платформы OneAtlas поможет регулярно улучшать гео-сервисы компании».

«Новое соглашение еще больше укрепит многолетнее сотрудничество между нашими компаниями.

Мы гордимся тем, что оно позволит нам объединить двух мировых лидеров рынка космической и ИТ отраслей – Airbus и Яндекса. Кроме этого One Atlas пополнит линейку продуктов компании Airbus, которую представляет наша компания на российском рынке, – отметил генеральный директор «СКАНЭКС» Валерий Баринберг.

«Мы рады подписанию нового соглашения со «СКАНЭКС» –

нашим давним и надежным партнером, который всегда ценил качество наших продуктов и поддерживал в инновациях», – сообщил Франсуа Ломбард, глава геопространственного направления Airbus DS.

<http://new.scanex.ru>



# Информационно-телекоммуникационные системы в глобализованном мире



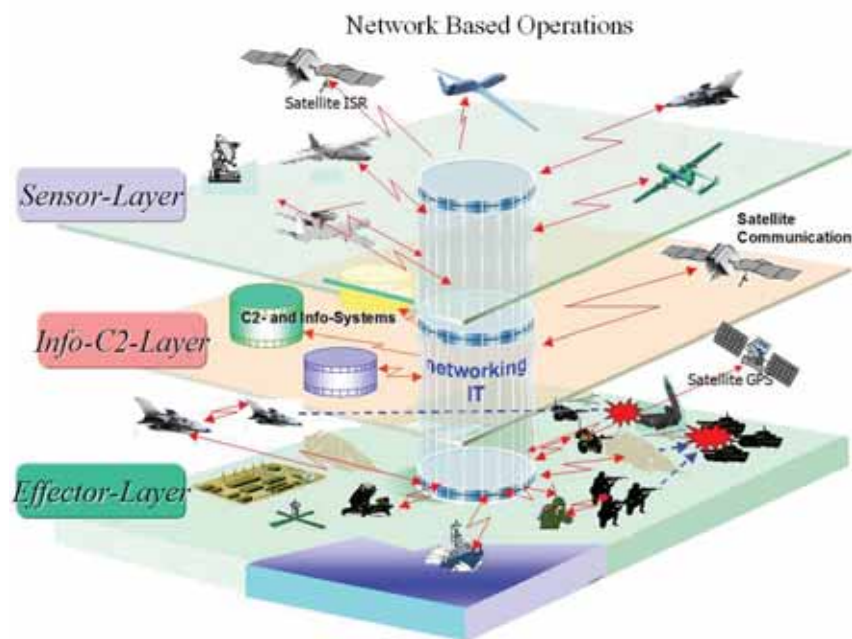
**Игорь ДУЛЬКЕЙТ,**  
к. т. н., ОмГТУ

Автором ставшего уже привычным термина «глобализация» считается американский экономист Теодор Левитт, который в 1983 г. опубликовал в журнале *Harvard Business Review* статью «Глобализация рынков». Сегодня глобализация охватила практически все сферы человеческой жизни. В области систем управления свое развитие она получила в концепции «сетевидной войны» (Network-centric warfare). Ее авторами принято считать начальника штаба ВМС США адмирала Джея Джонсона, вице-адмирала ВМС ВС США Артура Себровски и профессора Джона Гарстка, которые в январе 1998 г. опубликовали в журнале *Proceedings* статью «Сетевидная война: ее происхождение и будущее» [1].

В статье анализируются роль и место информационно-телекоммуникационных систем в современном мире, их взаимодействие на различных уровнях и основные тенденции развития.

Названная концепция была доработана и представлена в книге Джона Гарстка, Дэвида Альбертса и Фреда Стейна [2]. Сегодня сетевидные подходы в той или иной степени реализуются в системе государственного управления, бизнесе, экономике и технике. В концептуальном плане Себровски и Гарстка представили модель сетевидной войны как систему, состоящую из трех подсистем: информационной, сенсорной и боевой (рис. 1).

Основу всей системы составляет информационная подсистема (средства обработки и представления информации), пронизывающая всю систему. На нее накладываются сенсорная и боевая подсистемы. Элементами сенсорной подсистемы являются «сенсоры» (средства мониторинга – источники информации), а элементами боевой подсистемы – «стрелки» (исполнительные средства – потребители информации). Эти две группы элементов объединяются органами управления и командования.



**Рис. 1.** Модель сетевидной войны как системы трех компонентов: информационного, сенсорного и боевого

Несмотря на кажущуюся простоту модели, взаимоотношения между всеми элементами подсистем и самими подсистемами довольно сложные и многоплановые. Международная организация по стандартам (International Standards Organization – ISO) разработала модель, которая описывает различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие задачи должен решать каждый уровень. Эта модель называется моделью взаимодействия открытых систем (Open System Interconnection – OSI) или моделью ISO/OSI и в определенной степени стандартизует это многоплановое взаимодействие [3].

Рассмотрим функции уровней модели ISO/OSI, применительно к информационно-телекоммуникационным системам (рис. 2).

*Физический уровень (physical layer)* имеет дело с передачей сигналов по физическим каналам, проводным (кабельным) линиям или радиоканалам и описывает физические характеристики электрических сигналов и соответствующие им параметры телекоммуникационного оборудования. На этом уровне осуществляется поэлементный (побитный) прием/передача сигналов.

*Канальный уровень (data link layer)* решает задачу повышения частотно-энергетической эффективности информационно-телекоммуникационной системы за счет использования сложных сигнально-кодовых конструкций, с применением различных методов мультиплексирования и разделения физических каналов в целях повышения спектральной эффективности всей системы.

Прием и формирование сигналов осуществляется в целом в рамках используемой сигнально-кодовой конструкции. К информационному сигналу добавляется помехоустойчивое кодирование.

*Сетевой уровень (network layer)* служит для образования транспортной системы, объединяющей несколько канальных уровней. Он имеет дело уже не с сигналами, а с пакетами (packets) данных. Соединения внутри сети осуществляются маршрутизаторами, которые пересылают пакеты сетевого уровня по назначению. Главной задачей сетевого уровня является выбор наилучшего пути – маршрутизация пакетов.

*Транспортный уровень (transport layer)* обеспечивает приложениям или верхним уровням стека – сеансовому и прикладному – передачу данных с заданной степенью достоверности. На пути от отправителя к получателю пакеты могут быть искажены, потеряны или нарушен порядок их следования. Задача транспортного уровня заключается в том, чтобы устранить искажения пакетов в зависимости от надежности системы передачи данных предыдущих уровней и в соответствии с требованиями к ним со стороны последующих. На этом уровне реализуются, например, такие технологии, как прямая коррекция ошибок (Forward Error Correction – FEC) и автоматический запрос повторения неприятых пакетов (Automatic Retention request – ARQ).

*Сеансовый уровень (session layer)* обеспечивает управление диалогом на нем, в частности, реализуется технология автоматического составления канала связи (Automatic Link Establishment – ALE) с автовыбором рабочей частоты. Сейчас в системах профессиональной связи используется третье поколение 3G-ALE, которое позволяет:

- производить вызовы корреспондентов;
- согласовывать сетевое время;
- передавать сообщения о качестве связи;

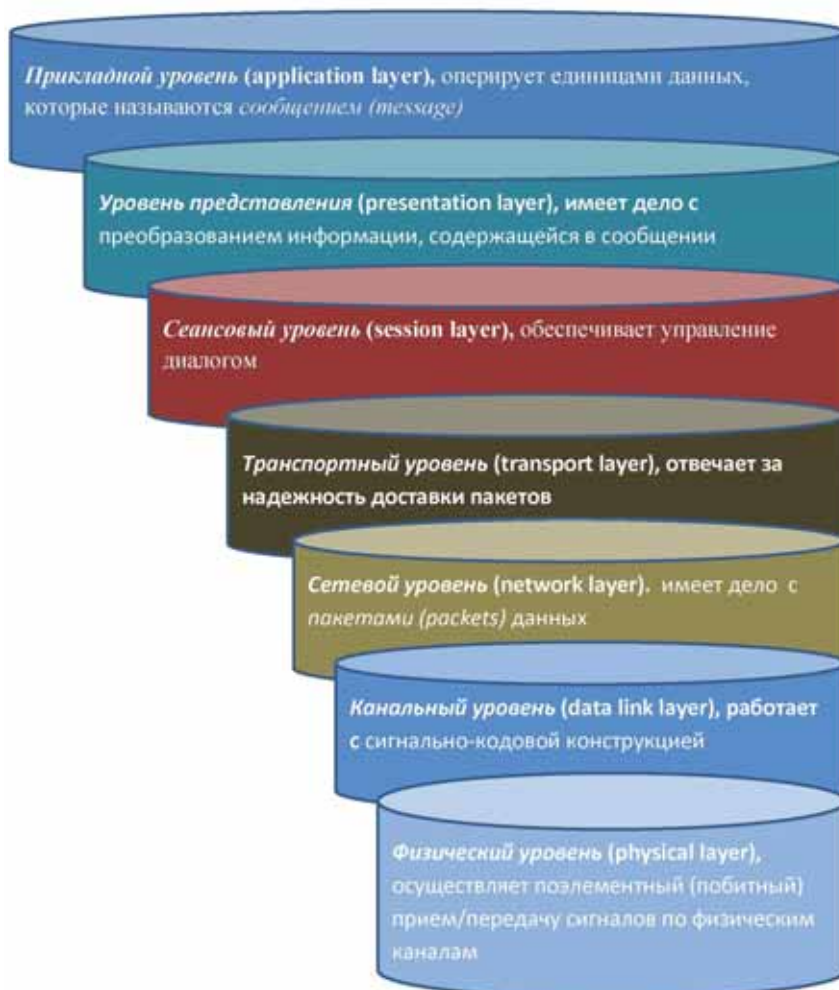


Рис. 2. Уровни модели ISO/OSI

- организовывать зондирование каналов распространения сигналов и определять его режимы;
- устанавливать интервалы и слоты;
- задавать количество сканируемых частот;
- устанавливать лучший канал для ведения связи.

В сетях общего пользования широко внедряется уже четвертое поколение стандарта беспроводной высокоскоростной передачи данных для мобильных телефонов 4G LTE (Long-Term Evolution), основанного на развитии сетевых технологий GSM/EDGE и UMTS/HSPA, включающего в себя стек протоколов различных уровней.

*Уровень представления (presentation layer)* обеспечивает преобразование сообщений, передаваемых прикладным уровнем, к виду, удобному для передачи по каналам связи, которые описываются предыдущими уровнями.

Важность этого уровня можно проиллюстрировать на примере цифрового телевизионного вещания. Теоретическая возможность и основные положения цифровой передачи информации были заложены еще в 30-х гг. прошлого века в работах В.А. Котельникова, Найквиста и Шеннона. Практическая реализация цифрового телевизионного вещания стала возможна только после того, как в конце прошлого века группа специалистов Moving Picture Experts Group (MPEG), сформированная международной организацией ISO, разработала протоколы сжатия цифровой видео- и аудиоинформации для передачи их по каналам связи.

Таким образом, уровень представления, по сути, отвечает за возможность практической реализации передачи информации по каналам связи и за выбор последних.

*Прикладной уровень (application layer)* оперирует единицами данных, которые называются сообщением (message), формируются сообщения в «сенсорной» подсистеме, а их потребителями являются «стрелки» или исполнительные

средства, если оперировать терминами сетецентрического управления.

Описываются сообщения прикладного уровня терминами теории информации, из которой известно [4], что характеристикой, позволяющей оценить информационные свойства источника сообщений, является среднее количество информации, приходящееся на одно сообщение, которое называется энтропией сообщения.

Количество передаваемой информации можно увеличить не только за счет увеличения числа сообщений, но и путем повышения энтропии источника, т. е. информационной емкости его сообщений, с учетом степени осведомленности приемника сообщений. Информацию необходимо передавать такими сообщениями, информационная емкость которых используется наиболее полно. Этому условию удовлетворяют равновероятные и независимые элементы сообщения. Увеличение статистической взаимосвязи между элементами сообщения ведет к снижению его информационной емкости и уменьшению энтропии источника.

Таким образом, два верхних уровня имеют дело непосредственно с информацией, подлежащей передаче по каналам связи, и их задача – максимально повысить информативность сообщения, его энтропию: на прикладном уровне за счет исключения из сообщения информации с высокой степенью вероятности известной получателю, а на уровне представления путем устранения статистической связи между элементами сообщения, поскольку если характер этой связи известен, то часть сообщения является избыточной и может быть восстановлена по известным статистическим связям.

Именно на верхних уровнях решается задача, являющаяся основой концепции сетецентрического управления, – максимальное приближение обработки информации к ее источнику и передача по каналам связи уже обработанной информации с максимальной энтропией.

Однако при передаче сообщения на физическом уровне в него вносятся искажения, обусловленные как каналом распространения, так и несовершенством аналоговой части телекоммуникационного оборудования, что может привести к утрате сообщения полностью или частично. Поэтому на средних четырех уровнях в передаваемые сообщения вносится избыточность, но не информационная, а структурная. То есть вводится известная статистическая зависимость между отдельными элементами сообщения, позволяющая восстановить его на приемном конце.

Практическая реализация такого подхода стала возможной благодаря развитию компьютерной техники, что позволило значительно продвинуться в области обработки информации, и широкому внедрению цифровых методов передачи сообщений, когда подлежащие передаче аналоговые сигналы преобразуются в цифровую форму на передающей стороне до модуляции.

Достижения в микроэлектронике, обеспечившие возможность создавать вычислительные средства, обладающие высоким быстродействием, малыми габаритами, весом и энергопотреблением, обусловили широкое применение цифровой обработки сигналов. Она включает в себя додетекторную обработку (предварительную фильтрацию), детектирование и последетекторную обработку сигналов цифровыми методами на приемной стороне, а также формирование модулированных или манипулированных сигналов на передающей стороне цифровыми методами.

Цифровая обработка сигналов имеет ряд преимуществ перед аналоговой:

- значительно более высокая точность обработки сигналов и возможность использования для этого сложных алгоритмов;
- гибкая перестройка алгоритмов обработки сигналов, обеспечивающая как создание многорежимных устройств, так и реализацию адаптивных систем с оперативной перестройкой;



Рис. 3. Функциональная схема аппаратной части оборудования с цифровой обработкой сигналов

- высокая технологичность изготовления устройств обработки, связанная с отсутствием необходимости настройки при изготовлении и регулировке в эксплуатации;
- высокая степень совпадения и повторяемость характеристик реализованных устройств с расчетными характеристиками;
- возможность построения саморазвивающихся интеллектуальных систем, способных к реконфигурации, поиску и обнаружению неисправностей;
- широкие возможности автоматизации проектирования устройств и обеспечения стабильности их эксплуатационных характеристик.

Структурно аппаратура с цифровой обработкой сигналов включает в себя аппаратную часть и программное обеспечение – виртуальную часть. В свою очередь, аппаратная часть функционально делится на три части (рис. 3).

Аналоговая часть (радиомодуль) включает в себя антенно-фидерные устройства, систему предварительной аналоговой фильтрации, усилители сигналов радиочастоты (предусилитель для радиоприемников и усилитель мощности для передатчиков). Если характеристики аналого-цифровой части не позволяют применять прямое цифровое преобразование частоты, используются аналоговые конверторы (повышающие или понижающие) частоты.

Аналого-цифровая часть включает в себя аналого-цифровой преобразователь – АЦП (Analog-to-digital converter – ADC) для приемной части и цифро-аналоговый преобразователь – ЦАП

(Digital-to-analog converter – DAC) для передающей части.

Между АЦП и цифровым вычислителем в радиоприемнике, как правило, используется цифровой понижающий преобразователь (Digital Down Converter – DDC), который переносит спектр сигнала на нулевую частоту с формированием квадратур, осуществляет предварительную цифровую фильтрацию и понижение частоты дискретизации (децимацию) сигнала.

В передатчике между ЦАП и цифровым вычислителем используется цифровой повышающий преобразователь (Digital Up Converter – DUC), который имеет в своем составе два канала интерполяторов для каждой из квадратур передаваемого сигнала, синтезатор косинусного и синусного компонентов сигнала несущей частоты, комплексный перемножитель для квадратур сигнала и несущей частоты. В результате DUC переносит спектр исходного сигнала на радиочастоту, а ЦАП формирует действительный аналоговый сигнал, предназначенный для передачи по каналу связи.

Цифровой вычислитель собственно и осуществляет цифровую обработку квадратур сигнала на нулевой частоте,

в нем используется цифровой сигнальный процессор (Digital signal processor – DSP). Архитектура сигнальных процессоров по сравнению с микропроцессорами общего применения имеет некоторые особенности, связанные со стремлением максимально ускорить выполнение типовых задач цифровой обработки сигналов, таких как цифровая фильтрация сигналов, дискретное преобразование Фурье и т. п.

Дальнейшим развитием цифровой аппаратуры, является использование принципов открытой модульной архитектуры со стандартными интерфейсами и единой операционной средой, так называемая технология программируемого радио (Software-defined Radio – SDR) [5], позволяющая программно конфигурировать технические средства в зависимости от решаемых задач.

Сама по себе технология SDR включает две основные составляющие:

- технологию программируемой связанной архитектуры (Software Communications Architecture – SCA). Внедрение технологий удаленных аппаратных радиомодулей, связанных между собой и с центром обработки данных высокоскоростными стандартными интерфейсами (рис. 4), влечет за собой расширение функциональных возможностей и обеспечивает более эффективное использование оборудования, так как дает возможность программно конфигурировать аппаратные средства под круг решаемых задач, подключая соответствующие аппаратные модули;
- технологию распределенного информационного взаимодействия на базе объектно-ориентированного программного



Рис. 4. Технология программируемой связанной архитектуры – SCA



Рис. 5. Технология распределенного информационного взаимодействия на базе объектно-ориентированного программного обеспечения

обеспечения (рис. 5), которая обеспечивает взаимодействие аппаратных модулей между собой и другим оборудованием, а также реализует дружественный интерфейс взаимодействия с оператором.

Кроме того, SDR-технология позволяет заменять отдельные аппаратные реализации устройств их программными реализациями. При таком подходе возможно выполнение на одном устройстве нескольких функций, которые раньше осуществлялись разными аппаратными устройствами.

Однако сегодня еще рано говорить о полномасштабном использовании технологии SDR. Речь идет скорее о программно-управляемом оборудовании (Software Controlled Radio – SCR). Эти устройства характеризуются несколько ограниченными функциями программного управления – в первую очередь это возможность программного подключения аналого-цифровых модулей различного назначения и варьирование их параметров в пределах технических характеристик этих модулей.

Основная причина – физический уровень, который ограничивает возможности использования аналоговых устройств. Прежде всего, это антенно-фидерные устройства, которые согласуют на физическом уровне аналого-цифровое оборудование

со средой распространения сигналов и в обозримом будущем останутся аналоговыми.

Только за десятилетний период 1980–1990 гг. количество антенн на боевых кораблях основных классов ВМС США практически удвоилось [6]. Это повлекло за собой массу проблем, начиная с электромагнитной совместимости (повышенное затенение антенн, электромагнитные помехи и увеличение площади радиозаметности корабля для радаров) и заканчивая проблемой обслуживания множества различных радиосистем. Поэтому большое внимание было уделено созданию универсальных антенно-фидерных устройств, т. е. интеграции многофункциональных радиотехнических систем на физическом уровне.

Первой программой по указанной тематике стала «Концепция перспективной многофункциональной системы радиодиапазона» (Advanced Multifunctional Radio Frequency Concept – AMRFC) [6, 7]. Ее реализация началась в конце прошлого века в интересах Военно-морских сил США, после того как она была профинансирована Управлением военно-морских исследований (Office of Naval Research – ONR).

В создании аппаратуры и программного обеспечения для этой программы участвовали такие компании, как Lockheed Martin Corporation, Northrop Grumman

Corporation, Raytheon и General Dynamics Corporation.

В европейских странах для разработки общей архитектуры многофункциональных радиотехнических систем в рамках Европейского оборонного агентства открыта программа «Наращиваемые многофункциональные системы радиодиапазона» (Scalable Multifunction Radio Frequency Systems – SMFR). В 2002 г. группа европейских компаний приступила к работе над проектом «Наращиваемые многофункциональные системы радиодиапазона. Компромиссный анализ» (Scalable Multifunction Radio Frequency Systems Trade-off Studies – STRATA).

Суть этой концепции заключается в переходе от одиночных антенн к антенным системам – активным фазированным антенным решеткам с электронным управлением. Активная фазированная антенная решетка состоит из собственно излучающего элемента и активного устройства – приемопередающего радиомодуля, который усиливает передаваемый и (или) принимаемый этим элементом радиосигнал, а также устройства управления, чаще цифрового, осуществляющего фазирование сигналов, поступающих на излучатели для формирования необходимых характеристик антенной системы в горизонтальной и вертикальной плоскостях.

Наиболее известный и глобальный американский научно-исследовательский проект, использующий фазированную антенную решетку, – «Программа исследования полярных сияний высокочастотным воздействием» (High Frequency Active Auroral Research Program – HAARP) [8]. Его антенное поле показано на рис. 6.



Рис. 6. Антенное поле системы HAARP



Таким образом, сохраняется общая концепция сокращения аналоговой части телекоммуникационного оборудования путем использования достаточно простых излучателей и приемопередающих радиомодулей и переноса основной нагрузки по формированию характеристик антенно-фидерных систем на цифровое диаграммообразующее устройство.

Вводя в состав радиоинтерфейсной части радиосистемы, кроме антенно-фидерных устройств и приемопередающих радиотрактов, среду распространения радиоволн – физическую среду передачи данных, мы переходим к парадигме системы когнитивного радио (Cognitive Radio System – CRS). Международный союз электросвязи определяет систему когнитивного радио следующим образом [9]: «Радиосистема, которая использует технологию, позволяющую этой системе получать знания о своей среде эксплуатации и географической среде, об установившихся правилах и о своем внутреннем состоянии; динамически и автономно корректировать свои эксплуатационные параметры и протоколы согласно полученным знаниям для достижения заранее поставленных целей и учиться на основе полученных результатов».

Таким образом, если до сих пор физический уровень рассматривался как инструмент информационного взаимодействия, то в когнитивном радио ему отводится одна из ведущих ролей обеспечения этого взаимодействия. Главная роль делится между верхним прикладным уровнем, определяющим информационную составляющую сообщения, и нижним физическим уровнем, охватывающим физическую среду передачи данных и определяющим телекоммуникационную составляющую информационного взаимодействия. Эти уровни управляют промежуточными, адаптируя их под задачи информационно-телекоммуникационного взаимодействия.

## Выводы

Глобальное информационное общество в постиндустриальной

экономической системе базируется на обеспечении гарантированного доступа ко всем видам инфокоммуникационных взаимодействий, образующих единое информационное пространство, которое, по сути, стирает национальные особенности и различия. Многоплановый характер взаимодействия информационных систем обусловил необходимость нормирования различных уровней такого взаимодействия и формализации задач информационного взаимодействия на каждом уровне.

Возрастающий объем информации, циркулирующей в информационно-телекоммуникационных системах, стимулирует бурное развитие последних. Благодаря прорывным достижениям в микроэлектронике это развитие идет по направлению все более широкого внедрения цифровых технологий как при передаче самих информационных сообщений, так и при обработке сигналов – носителей информации.

Цифровое телекоммуникационное оборудование состоит из двух частей: виртуальной – алгоритмы и программное обеспечение и аппаратной платформы. Последняя, в свою очередь, включает в себя аналоговую, аналого-цифровую и цифровую части.

Главенствующая роль при создании информационно-телекоммуникационных систем принадлежит верхним уровням, определяющим собственно информативность сообщения, его энтропию. На второе место в системах «умного» радио выходит низший – физический уровень, включающий в себя среду распространения сигналов. Оба эти уровня с точки зрения инфокоммуникационной системы априорно заданы и степень ее влияния на них крайне ограничена. Промежуточные уровни служат для адаптивного согласования информационного сообщения и среды передачи информации. ■

## Литература

1. Cebrowski Arthur K. and John J. Garstka. *Network-Centric Warfare: Its Origins and Future*. U. S. Naval Institute Proceedings, January 1998.

2. Alberts D.S., Garstka J.J., Stein F.P. *Network Centric Warfare: Developing and Leveraging Information Superiority // CCRP Publ., 2nd Edition (Revised)*. Aug 1999, Second Print Feb 2000, P. 284. [Электронный ресурс]. – Режим доступа: [http://www.dodccrp.org/files/Alberts\\_NCW.pdf](http://www.dodccrp.org/files/Alberts_NCW.pdf)
3. ГОСТ Р ИСО/МЭК 7498-1-99. *Взаимосвязь открытых систем. Базовая эталонная модель*. [Электронный ресурс]. – Режим доступа: <http://vak.ru/pub/gost/gost-r-iso-mek-7498-1-99.pdf>
4. Галлагер Р. *Теория информации и надежная связь*. М.: Советское радио, 1974.
5. Сипин А. *Технология Software Defined Radio. Теория, принципы и примеры аппаратных платформ // Беспроводные технологии*. 2007. № 2. С. 22–27. [Электронный ресурс]. – Режим доступа: <http://www.wireless-e.ru/articles/technologies/200>
6. Леонов Е. *Создание многофункциональных радиотехнических систем для надводных кораблей ВМС США и стран Европы // Зарубежное военное обозрение*. 2014. № 5. С. 86–93.
7. G.C. Tavik, I.D. Olin. *The Advanced Multifunction RF Concept (amrfc) Test bed electronics and electromagnetics 2005 NRL Review*. P. 133–135.
8. HAARP [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/HAARP>
9. Report ITU-R SM.2152 «Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)» [Электронный ресурс]. – Режим доступа: [https://www.itu.int/dms\\_pub/itu-r/oth/0c/06/R0C060000560005PDFE.pdf](https://www.itu.int/dms_pub/itu-r/oth/0c/06/R0C060000560005PDFE.pdf)
10. Mitola J. III; Maguire G.Q. Jr. *Cognitive radio: making software radios more personal*, IEEE Personal Communications, Volume 6, Issue 4, Aug 1999 Page(s): 3–8 – Digital Object Identifier 10.1109/98.788210.

# Спутниковая связь для Интернета вещей



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

## Хорошая альтернатива

С развитием сети Интернет и средств электросвязи у корпоративных и государственных структур, а также у индивидуальных пользователей растут потребности в удаленном доступе к информации в режиме реального времени. Многим предприятиям для повышения эффективности своей деятельности сегодня также необходимы непрерывный контроль и дистанционное управление различными технологическими процессами на базе услуг Интернета вещей (IoT/M2M).

В настоящее время рынок услуг Интернета вещей (IoT/M2M) является одним из наиболее динамично развивающихся. Ожидается, что в период с 2017 по 2020 г. ежегодный рост рынка IoT/M2M составит 15,5%.

По данным исследовательской компании Frost & Sullivan, уже к 2022 г. спутниковые технологии связи получат широкое распространение на рынке услуг IoT/M2M



**Александр БАБИН,**  
заместитель генерального директора  
АО «Национальный исследовательский  
институт технологий и связи»  
по работе с государственными  
органами, к. т. н.

и составят конкуренцию наземным системам беспроводной связи.

Спутниковая связь займет существенную долю рынка услуг IoT/M2M среди сетей доступа в сфере автомобильного транспорта, авиации, морского судоходства, вооруженных сил, а также нефте- и газодобычи.

Препятствием для роста спутникового сегмента рынка IoT/M2M могут стать высокие первичные затраты на развертывание сети. Однако такие преимущества, как глобальное покрытие на суше, море и в воздухе, а также гарантируемая передача данных даже во время стихийных бедствий, делают спутниковую связь хорошей альтернативой сотовой связи и наземным проводным линиям связи.

Кроме того, следует отметить, что многие сервис-провайдеры услуг IoT/M2M предлагают свои гибридные решения, объединяющие возможности беспроводных наземных систем связи и спутниковой

Спутниковые технологии в ближайшем будущем получат широкое распространение на рынке услуг Интернета вещей (IoT/M2M) и составят конкуренцию наземным каналам связи за счет полного географического охвата и гарантируемой передачи данных в любых условиях. В статье проведен анализ ключевых направлений развития услуг Интернета вещей (IoT/M2M) на базе сетей подвижной спутниковой и фиксированной спутниковой связи, а также применения глобальных спутниковых навигационных систем для услуг Интернета вещей на подвижных объектах – авиационного, морского, железнодорожного и автомобильного транспорта.

связи, позволяя экономить на услугах связи в местах с развитой инфраструктурой мобильных сетей и при этом обеспечивать сервис в отдаленных местах.

## Особенности построения решений IoT/M2M на базе сетей доступа подвижной спутниковой связи

Развитие подвижных спутниковых сетей (ПСС) и услуг – одно из наиболее перспективных направлений развития спутниковой связи. Сейчас в мире работают девять

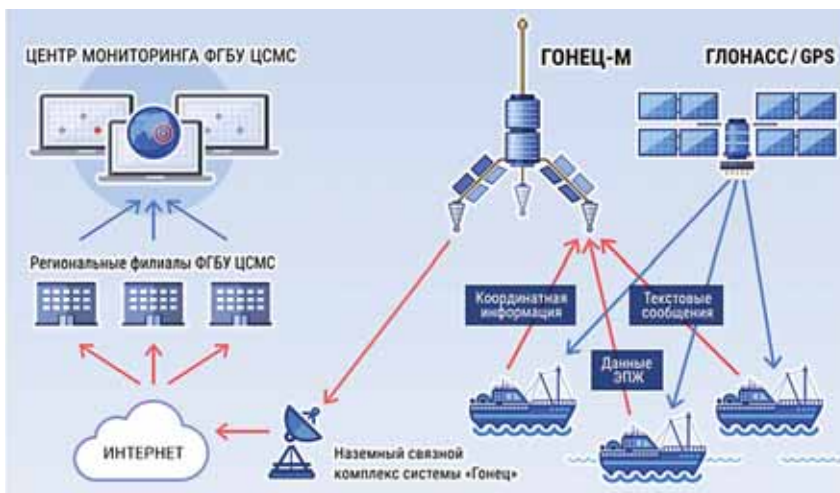


Рис. 1. МСПСС «Гонец-Д1М» для транспортных услуг IoT/M2M

систем ПСС, которые обслуживают более 2,9 млн абонентов. По данным зарубежных аналитиков, ежегодный доход в этом бизнесе составляет около 1,4% доходов всего рынка, или 2,8 млрд долл. Ожидается, что в ближайшие пять лет доход от услуг ПСС будет расти ежегодно более чем на 5% и достигнет 5 млрд долл. через пять лет. При этом количество пользователей спутниковых услуг увеличится до 6 млн.

Сети связи ПСС могут использовать низкоорбитальные и среднеорбитальные группировки спутников, а также спутники на геостационарной орбите.

В настоящее время на низких орбитах (до 2000 км) уже развернуты три глобальные американские системы подвижной спутниковой связи: Iridium, Globalstar и Orbcomm Inc, а также российская система «Гонец-Д1М».

Пример сети подвижной спутниковой связи на базе многофункциональной системы персональной спутниковой связи (МСПСС) «Гонец-Д1М» показан на рис. 1. Терминалы «Гонец», установленные на суда и автомобильный транспорт, способны передавать с необходимой периодичностью информацию о местоположении рыболовецких судов и транспортных средств, а также данные электронно-промышленного журнала и мониторинга в необходимом формате.

В марте 2014 г. компанией O3b Networks была введена

в коммерческую эксплуатацию система подвижной спутниковой связи на средневисотной орбите (8063 км).

На геостационарной орбите развернуты глобальная спутниковая система Inmarsat и региональные спутниковые системы Thuraya (Африка и Азия), ACeS (Азия) и DBSD (США) подвижной спутниковой связи, а также гибридная североамериканская система подвижной спутниковой и наземной связи Terrestrial и LightSquared.

На долю трех ведущих операторов (Inmarsat, Iridium и Thuraya) приходится почти 90% суммарных доходов от услуг подвижной спутниковой связи (рис. 2). По данным 2016 г., доля рынка компании Inmarsat составила 56%, а компания Iridium укрепила свои позиции в качестве второго крупнейшего оператора ПСС с долей рынка 25%.

Крупнейший из региональных операторов ПСС – компания Thuraya – имеет 8% рынка.

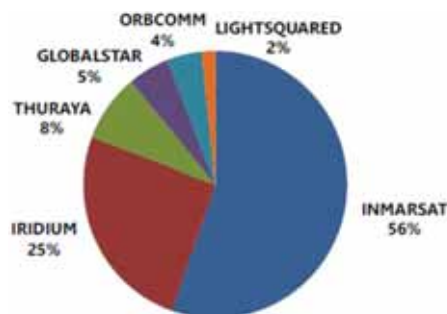


Рис. 2. Доли рынка операторов ПСС

Доля компании Globalstar – около 5% рынка. На долю оператора Orbcomm пришлось примерно 4% доходов рынка, а LightSquared – около 2%.

Из перечисленных операторов ПСС только компания Orbcomm сфокусировала свою основную деятельность на рынке услуг M2M и Интернета вещей. Однако в последнее время ведущие операторы ПСС – Inmarsat, Iridium и Globalstar – тоже активно работают на рынке услуг IoT/M2M. По оценкам компании Euroconsult, до 2023 г. рынок услуг IoT/M2M на базе сетей ПСС будет расти с двузначным показателем годового роста как по количеству терминалов, так и по доходам от основной деятельности.

На настоящем этапе большинство активных низкоскоростных терминалов ПСС развернуто в сухопутном секторе на транспортном рынке IoT/M2M. Сектор коммерческой транспортной логистики является самым большим в области низкоскоростных средств ПСС. Ведущие транспортные и логистические компании уже используют спутниковые средства IoT/M2M на своем транспорте для контроля местоположения, состояния машин, грузовиков, трейлеров, контейнеров, железнодорожных эшелонов, качества работы водителей, уровня потребления топлива и т. д. в целях повышения эффективности организации и безопасности своего транспорта. Например, компания Orbcomm представила на грузовой рефрижераторный рынок свой терминал четвертого поколения RT 6000+, который позволяет регулировать температуру.

Компания Thuraya в 2016 г. разработала спутниковый модем FT2225, функционирующий в двустороннем режиме онлайн для отслеживания наземных транспортных средств, удаленного мониторинга и коммуникаций.

Iridium SBD (Short Burst Data) – простая и достаточно эффективная технология для двусторонней передачи коротких сообщений через сеть Iridium между устройствами IoT/M2M и центральным сервером сбора и хранения данных. Архитектура таких сетей

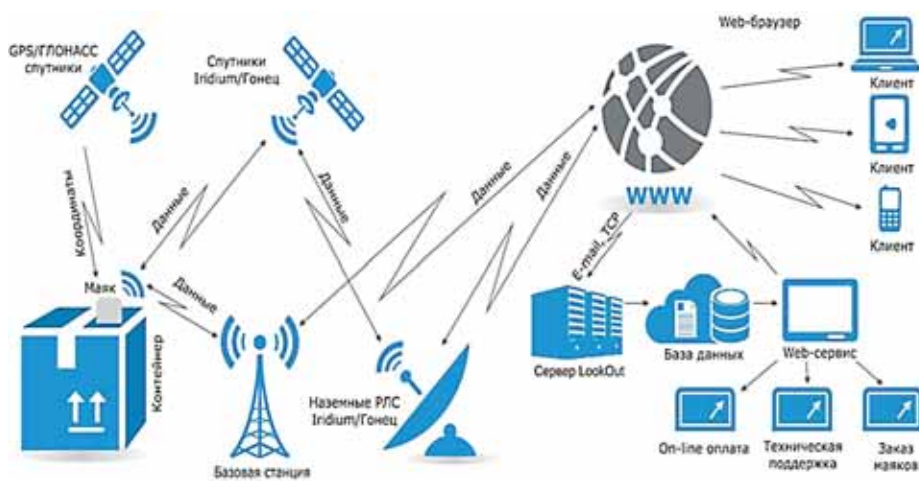


Рис. 3. Архитектура сетей транспортного мониторинга и IoT/M2M

транспортного мониторинга и IoT/M2M представлена на рис. 3. Примерами оборудования в сети Iridium для транспортных услуг IoT/M2M являются:

- «Спектр-ГЛОНАСС», бортовой малогабаритный спутниковый трекер воздушного судна на базе модема Iridium 9602;
- NAVISET GT-101R, автомобильный трекер для спутникового мониторинга транспорта, работающий по каналам GSM и Iridium;
- PM-15M, для организации полудуплексного низкоскоростного канала передачи цифровой информации для БПЛА;
- Tetis R, терминал контроля местоположения, мониторинга и слежения за состоянием сухих и рефрижераторных контейнеров.

Компания Inmarsat может предложить оборудование для оказания услуг IoT/M2M трех видов:

- оборудование серии IsatM2M (терминалы SureLinx 8100, DMR 800, Osprey, SAT-202), обеспечивает передачу информации пачками до 85 бит и прием пачками до 200 бит;
- оборудование серии IsatDataPro (терминалы IDP 680, 690, 800, 780, 100), обеспечивает передачу информации пачками до 6400 байт и прием пачками до 10 000 байт;
- оборудование серии BGAN M2M (терминал Hughes 9502), обеспечивает доступ в Интернет для приложений M2M на скоростях выше 100 кбит/с.

Каждая серия имеет свою нишу приложений. Если терминалы серии IsatM2M подходят для целей мониторинга транспорта, то для приложений, связанных, например, с метеорологией судов, потребуется оборудование серии IsatDataPro или BGAN M2M.

Мониторинг ГЛОНАСС/GPS с нашей системой «Гонец-Д1М» может быть применен на автомобилях, вагонах, судах, дрейфующих буях и пр. Данные о местоположении объектов передаются в виде трека с указанием на карте точек местоположения и временных меток. В работе пользователь использует веб-портал услуг «Гонец», где он отслеживает передачу координатной информации со своих удаленных подвижных объектов. При необходимости возможна передача данных непосредственно на IP-адрес пользователя.

Спутниковые терминалы, традиционно развертываемые в морском секторе, часто бывают многоцелевыми, при этом число специализированных терминалов M2M ограничено. Наиболее широко на морском рынке используются терминалы компании Inmarsat.

Ожидается, что рынок морских служб безопасности будет расти на основе требований регламентного характера. По данным Международной морской организации (International Maritime Organization – IMO), все суда весом 300 т и длиной 20 м (судно Конвенции SOLAS – Safety of Life

at Sea, Международная конвенция по охране человеческой жизни на море), надлежит оснастить средствами передачи коротких сообщений (SMS) как минимум типа Inmarsat C. На данном этапе количество действующих судов с аппаратурой SOLAS составляет примерно 45 тыс. Оператор действующей морской спутниковой низкоскоростной системы ПСС – компания Inmarsat планирует интегрировать свою систему низкоскоростной связи в ведущую широкополосную сеть FleetBroadband, а также развернуть динамическую телеметрическую службу (Dynamic Telemetry Service – DTS) для работы в сети FleetBroadband network, которая обеспечит реализацию массы дополнительных возможностей слежения и мониторинга судов. Эта новая служба DTS будет включать некоторые базовые функциональные возможности системы Inmarsat C.

Введение организацией IMO новых требований LRIT (Long Range Identification and Tracking – дальняя идентификация/опознавание и сопровождение) повысит потребности в целевых терминалах M2M ПСС. Так, компания Orbcomm уже подписала контракт с Европейским агентством морской безопасности ESMA (European Securities and Markets Authority), предусматривающий доставку данных AIS (Automatic Identification System – система автоматического опознавания) для сопровождения судов. Недавно была создана Космическая служба автоматического опознавания S-AIS (Satellite-AIS) в виде нового применения в этом сегменте M2M. Имея терминалы Inmarsat-C и IsatM2M, компания Inmarsat является наиболее значимым провайдером, обеспечивающим выполнение нового требования морского регламента. Однако на крайних северных и южных широтах, где нет зон покрытия спутников Inmarsat, только компания Iridium обеспечивает сегодня выполнение требований LRIT.

Ожидается, что с созданием дополнительных каналов сбыта и новой продукции M2M ПСС количество абонентов на сухопутном рынке составит примерно 7,4 млн в 2022 г. при валовом доходе

отрасли на уровне 400 млн долл., т. е. примерно 95% показателей отрасли M2M ПСС по числу абонентов и доходов.

Распределение годовой выручки от оптовой продажи эфирного времени в горизонтальных сегментах рынка ПСС в 2020 г. приведено на рис. 4.

## Особенности построения решений M2M на базе сетей доступа фиксированной спутниковой службы

Фиксированная спутниковая служба (ФСС) – это вид спутниковой связи, где в качестве наземных станций спутниковой связи используются фиксированные (неподвижные) абонентские терминалы.

Сегодня группировка спутников связи и вещания гражданского назначения Российской Федерации включает 12 космических аппаратов (КА) на дуге геостационарной орбиты от 14° з. д. до 145° в. д. Сейчас уже началась реализация Федеральной целевой программы «Развитие орбитальной группировки спутников связи и вещания гражданского назначения Российской Федерации, включая спутники на высокоэллиптической орбите, на период 2017–2025 годов».

В настоящий момент фиксированная спутниковая связь практически исчерпывается технологией VSAT (Very Small Aperture Terminal – малая спутниковая земная станция). По международной классификации к VSAT относятся спутниковые станции с антеннами менее 2,5 м. Технология VSAT применяется для магистральной передачи данных, доступа в сеть Интернет, а также для IP-телефонии.

Основная конкуренция для широкополосных систем ПСС усиливается со стороны ФСС, подвижных систем VSAT в диапазонах C и Ku. И хотя VSAT-оборудование по-прежнему более дорогостоящее, большей массы и размеров (особенно размеров антенн), в области подвижных систем VSAT в последние годы наблюдается

### — Мнение специалиста —



**Алексей АФОНИН,**

менеджер по развитию бизнеса, Orange Business Services в России и СНГ

С точки зрения бизнеса наших клиентов, которые заинтересованы в M2M- и IoT-решениях, в качестве среды передачи спутниковая связь не является единственным средством. Поэтому в арсенале Orange Business Services есть IoT- и M2M-решения, основанные и на других беспроводных технологиях – GSM, LoRa, Wi-Fi, Bluetooth, RFID и пр.

(с помощью которых собирается информация с датчиков и затем передается через наземные каналы в центры управления). В отличие от спутниковой связи такие решения экономически более эффективны для конечного пользователя и довольно распространены в регионах с развитой инфраструктурой.

Но, конечно, для труднодоступных мест на суше и особенно в море или в воздухе организация спутниковых каналов остается пока единственным способом передать данные IoT или M2M на большую землю. Для этого мы используем наиболее распространенные системы – VSAT, Iridium, Inmarsat. Причем для каждого нашего клиента мы выбираем наиболее оптимальное решение, поскольку каждая из этих систем имеет специфические преимущества. Например, для сложной наземной техники, где нужна компактность, но при этом нет особых требований к скорости передачи данных, подойдет решения Iridium SBD, а если клиент хочет организовать онлайн-конференцию на своих судах в море, где есть особые требования к пропускной способности и качеству сигнала, то в решении применяются VSAT-антенны с системой автоматического наведения. Они стоят дороже, но клиенты понимают, за что они платят.

технологический прогресс у всех крупных производителей, например компаний Hughes, iDirect и Viasat, уделяющих часть своих работы в области НИОКР проблемам оптимизации подвижных широкополосных (ШП) систем VSAT.

Прогнозируемое распределение количества терминалов VSAT на транспорте в 2020 г. представлено на рис. 5. С развитием технологии VSAT фиксированная спутниковая связь начинает занимать другие рыночные ниши. Мобильные станции VSAT сегодня все чаще применяются на морских судах, поездах, самолетах и автомобилях.

Особенностью мобильных станций VSAT является использование автоматизированной высокоточной системы наведения антенны на спутник.

В морское применение спутниковых сетей с технологией VSAT в настоящее время активно внедряются так называемые интегрированные гибридные устройства M2M (VSAT + Iridium + Inmarsat).

По умолчанию все спутниковые сети на базе технологии VSAT поддерживают лишь топологию звезда, когда абонентская станция напрямую может связываться только

с центральной станцией. Однако некоторые сети поддерживают и полносвязную топологию Mesh, при которой абонентские спутниковые станции могут связываться друг с другом непосредственно.

В сухопутном применении спутниковых сетей с технологией VSAT активно используются

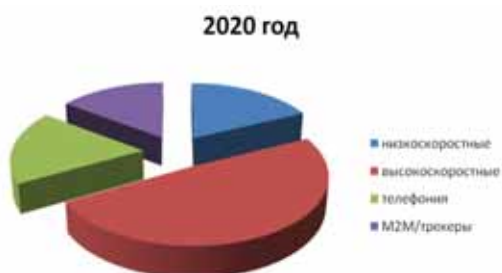


Рис. 4. Распределение годовой выручки от оптовой продажи эфирного времени в горизонтальных сегментах рынка ПСС

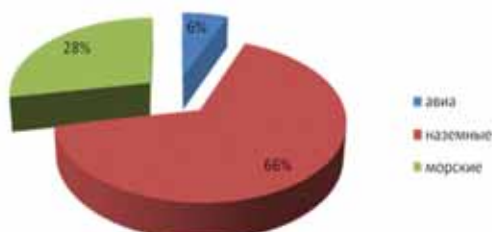


Рис. 5. Прогнозируемое распределение количества терминалов VSAT на транспорте в 2020 г.

транспортные устройства M2M, поддерживающие соединения не только по технологии VSAT, но и с интерфейсами Ethernet (RJ45), USB, RS-232/422/485 и беспроводные соединения на базе сотовых технологий GSM/UMTS/LTE или на основе технологии Wi-Fi.

## Использование глобальных спутниковых навигационных систем для услуг M2M

В последнее десятилетие широкое распространение получили услуги, связанные с отслеживанием положения транспорта (трекингом), людей и других объектов. Для определения точного местоположения заданного объекта используются глобальные навигационные спутниковые системы (ГНСС).

Системы ГНСС обеспечивают глобальный охват на всей поверхности Земли и в околоземном воздушном пространстве с точностью позиционирования до нескольких метров. Кроме того, они позволяют определять скорость и направление движения объекта. В настоящее время единственными спутниковыми навигационными системами, которые обеспечивают полное и бесперебойное покрытие земного шара, являются американская система NAVSTAR GPS (сокращенно – GPS) и российская система ГЛОНАСС.

Другие известные спутниковые системы навигации – китайская BeiDou и европейская Galileo, которые должны быть полностью развернуты к 2020 г. Отличительной особенностью системы BeiDou является использование не только среднеорбитальных спутников, но и спутников, работающих на геостационарной и геосинхронной орбитах.

В качестве абонентских терминалов применяются персональные (носимые) и стационарно устанавливаемые на транспортное средство или груз GPS-трекеры и ГЛОНАСС-трекеры. Компактные трекеры снабжены приемниками GPS/ГЛОНАСС, которые определяют свое местоположение на основе сигналов, поступающих от навигационных спутников.

Платформа трекинга и мониторинга принимает, обрабатывает и хранит полученные координаты в базе данных. Абонент услуги трекинга имеет возможность в любое время и из любой точки планеты зайти на платформу трекинга и мониторинга через сеть Интернет под своим именем и паролем, и платформа визуализирует местонахождение и географию перемещений на цифровой карте.

## Заполнить пробелы наземных каналов

В настоящее время во всем мире наблюдается резкий рост использования приложений Интернета вещей и M2M в различных сферах деятельности. Здесь можно упомянуть и мониторинг подвижных объектов, и мониторинг нефтегазовых трубопроводов, а также экологию, метеорологию, охрану, военные приложения, объекты энергетики и т. д.

Высокие темпы развития спутниковой связи в Интернете вещей и M2M объясняются рядом достоинств, которыми они обладают. К ним, в частности, относятся: большая пропускная способность, неограниченные перекрываемые географические пространства, высокое качество и надежность каналов связи. Эти достоинства, которые определяют широкие возможности спутниковой связи, делают ее уникальным и эффективным средством связи. Спутниковая связь в настоящее время является основным видом международной и национальной связи на большие и средние расстояния. Использование искусственных спутников Земли для организации связи продолжает расширяться по мере развития существующих сетей связи. Многие страны создают собственные национальные сети спутниковой связи. Решения морских перевозок позволяют находить, отслеживать и регулярно контролировать коммерческие и частные суда, чтобы выполнять все требования стандартов SSAS (Ship Security Alert System) и LRIT.

Необходимость транспортных компаний в обеспечении непрерывных рабочих процессов и 100%-ного

функционирования производственного оборудования вскоре приведет к тому, что спутниковая связь станет основной и резервной технологией связи. Согласно новому исследованию Frost & Sullivan, уже к 2022 г. максимум внимания на быстрорастущем рынке IoT компании будут уделять возрастающей роли спутниковой связи, которая способна заполнить пробелы наземных каналов.

Использование спутниковых каналов связи для IoT/M2M-сервисов будет расти быстрыми темпами, предоставляя новые возможности для спутниковых операторов по всему миру. Благодаря глобальному покрытию спутниковая связь позволит использовать IoT-сервисы даже в тех регионах, где раньше была только мобильная связь. Спутниковые технологии дополняют уже существующие наземные сети или даже станут единственной технологией, обеспечивающей работу IoT/M2M-приложений. ■

### Литература

1. Тихвинский В.О., Коваль В.А., Бочечка Г.С., Бабин А.И. *Сети IoT/M2M: технологии, архитектура и приложения // Медиа Паблишер, 2017.*
2. Бочечка Г.С., Минов А.В., Тихвинский В.О. *Отраслевые модели применения промышленного Интернета вещей // Соппест. Мир информационных технологий. 2017. № 3.*
3. Тихвинский В.О., Бабин А.И. *M2M-решения в инфраструктурных областях: трубопроводный транспорт, энергетика, ЖКХ // Соппест. Мир информационных технологий. 2012. № 9.*
4. Тихвинский В.О. *Перспективные бизнес-модели и сферы применения M2M. Оценка эффективности // Соппест. Мир информационных технологий. 2012. № 6.*
5. *Спутниковая связь и вещание. Специальный выпуск // Технологии и средства связи. 2017. № 6.*
6. *Публичная Декларация ключевых целей и приоритетных задач Министерства транспорта Российской Федерации на 2017 год.*

## SAP запускает собственную блокчейн-платформу

Компания SAP выпустила решение SAP Cloud Platform Blockchain, которое поможет клиентам пересмотреть свои бизнес-процессы с помощью блокчейн-технологий. SAP стремится расширить использование технологий блокчейн для всех индустрий и бизнес-процессов, не ограничиваясь только финансовыми сервисами и каналами поставок. Компания стала одним из основателей организации Blockchain Research Institute, премиум-участником проекта Hyperledger, и стремится к тому, чтобы общие усилия по развитию сферы блокчейн совпадали с требованиями клиентов к новым технологиям. Технологии блокчейн, встроенные в платформу SAP Cloud Platform, помогут пользователям упростить и оптимизировать процессы с большим количеством участников.

На запуске сервис SAP Cloud Platform Blockchain получит три важные функции: клиенты и разработчики могут начать создавать расширения с использованием блокчейн для собственных, уже существующих приложений в различных индустриях и бизнес-процессах; решения SAP, включая функции распределенного реестра, будут интегрированы в экосистему блокчейн для создания

синергии, особенно для бизнес-процессов с большим количеством участников; технологии блокчейн будут встроены в сервисы SAP Leonardo, чтобы создавать комбинации с другими новыми цифровыми технологиями, например с Интернетом вещей.

Сервис SAP Cloud Platform Blockchain позволяет быстро создавать блокчейн-узлы и управлять ими. Это поможет клиентам для начала создать простые тестовые приложения, чтобы проверить потенциал блокчейн-технологий. Заинтересованные компании могут зарегистрироваться в программе совместных инноваций SAP для сотрудничества и создания совместных решений. Интеграция с SAP Leonardo также расширит возможности для использования технологий блокчейн в корпоративном секторе.

Расширенная платформа SAP Leonardo объединит различные программные возможности: машинное обучение, Интернет вещей, Big Data, аналитику и блокчейн на SAP Cloud Platform вместе с опытом SAP, глубоким знанием индустрии и продвинутой методологией design thinking. Каждая из этих областей в портфолио SAP может создать значительную добавленную стоимость для клиентов.

## Huawei провела в Турции испытания мобильной технологии 4,5G

Компании Vodafone Turkey и Huawei завершили первые в мире испытания решения для совместного использования спектра GSM-LTE на базе коммерческой сети Vodafone диапазона 900 МГц, которые проходили в городе Диярбакыр (Турция). Это революционное решение, разработанное в рамках сотрудничества Центра мобильных инноваций Huawei Mobile Innovation Centre и Центра передовых технологий Vodafone Networks CoE (Center of Excellence) по разработке решений совместного использования спектра, обеспечивает эксплуатацию общих частотных ресурсов для технологий GSM и LTE с беспрецедентным взаимным наложением двух технологий, что повышает скорость передачи данных и емкость соты в сети LTE, в частотном ресурсе диапазона 900 МГц, доступном в сети Vodafone Turkey. По сравнению с сетью LTE с шириной канала 5 МГц средняя пропускная способность повышается почти на 58% в нисходящем канале и 44% в восходящем канале.

1 апреля 2016 г. компания Vodafone Turkey начала коммерческое использование мобильной

технологии 4,5G. На текущий момент Vodafone в Турции – это оператор с самой большой зоной покрытия данной технологии. Он обслуживает свыше 8 млн пользователей LTE. По мере того как пользователи переходят на LTE, эффективное распределение ресурсов спектра, необходимое для того, чтобы справиться с возрастающим трафиком, является приоритетом для Vodafone Turkey.

Оператор использует в решениях для объединения спектров GSM и LTE патентованные алгоритмы Huawei, чтобы снять с операторов

ограничения стандартной ширины канала LTE. Благодаря этой технологии разделенные ресурсы спектра используются максимально полно, обеспечивая повышение скорости передачи данных. Тестовые сценарии показывают, что совместное использование спектра GSM-LTE обеспечивает увеличение средней пропускной способности в нисходящем канале приблизительно на 58% и на 44% – средней пропускной способности в восходящем канале по сравнению с сетью LTE с шириной канала 5 МГц.



## HyperPOD



**Производитель**  
Schneider Electric

**Поставщик**  
Schneider Electric

**Источник**  
<http://www.schneider-electric.com/b2b/en/solutions/system/s4/data-center-and-networks-hyperpod/>

### НАЗНАЧЕНИЕ

Идеально для модернизации существующих и оснащения новых машинных залов, развивающихся ЦОД и серверных малой или средней плотности.

### ХАРАКТЕРИСТИКИ И ПРЕИМУЩЕСТВА

#### Преимущества

1. Модульная конструкция с возможностью наращивания длины и опционала.
2. Независимое размещение и модернизация от шкафного оборудования.
3. Поддержка шкафов различных размеров.
4. Быстрое развертывание инженерной среды до момента установки ИТ-оборудования.
5. Легкая интеграция со смежными подсистемами (распределение питания, охлаждение, СКУД, пожаротушение).

#### Характеристики

- Поддержка шкафов разной высоты (до 52U) и ширины в одном модуле.
- Высота конструкции до 3,7 м.
- Длина каждого модуля регулируется и позволяет размещать 8–12 стоек (по 4–6 в каждом ряду).
- Нагрузочная способность одного модуля HyperPOD до 900 кг.
- Совместим с периметральными, внутрирядными и централизованными системами кондиционирования.
- Изоляция холодного или горячего коридора.
- Доступны различные варианты крыши и воздуховодов.

### ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

HyperPOD предназначен для оптимизации трудозатрат на монтаж, эксплуатацию, позволяет повысить энергоэффективность ЦОД. Универсальная модульная конструкция имеет самонесущий каркас и может быть установлена как до, так и после монтажа серверных шкафов. Имеется возможность наращивания длины рядов. Шкафы можно устанавливать и демонтировать в процессе эксплуатации без вмешательства в конструкцию HyperPOD. Большой ассортимент опций и конфигураций обеспечивает адаптивность, гибкость, масштабируемость и совместимость со смежными инженерными системами.

HyperPOD может быть оснащен несколькими независимыми ярусами лотков. Поставка осуществляется в разобранном виде. Конструкция максимально функциональна и удобна в сборке. Предусмотрены опциональные сервисы шефмонтажа и сборки сервисными инженерами APC by Schneider Electric.

Schneider Electric

<http://www.schneider-electric.com/ru/ru/>



## «Конвейер инноваций» на форуме «Армия-2017»

22–27 августа 2017 г. в конгрессно-выставочном центре «Патриот» пройдет 3-й Международный военно-технический форум «АРМИЯ-2017» – крупнейшее событие в области вооружения, промышленности и технологий.

Одним из главных объектов форума в нынешнем году станет специальная экспозиция «Инновационный клуб» – конвейер инноваций – экспозиция изобретений и инновационных разработок различных стадий технологической готовности, выполненных молодыми учеными, студентами вузов, научно-исследовательскими организациями, малыми инновационными предприятиями и индивидуальными разработчиками в инициативном порядке.

В «Инновационном клубе» пройдет более 20 различных мероприятий, организованных в современном интерактивном формате, – деловые дискуссии, инвестиционные сессии, презентации, встречи с генеральными конструкторами и мастер-классы.

Каждый участник специальной экспозиции получит уникальную возможность презентовать свою разработку представителям венчурных фондов, бизнес-ангелам и частным инвесторам в ходе инвестиционных сессий.

Отбор инновационных проектов для демонстрации на специальной экспозиции «Инновационный клуб» осуществляется путем открытого конкурса, в котором может принять участие любой желающий. Организатором конкурса выступает Главное управление научно-исследовательской деятельности и технологического сопровождения передовых технологий (инновационных исследований) Минобороны России.

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





## Редакция журнала «Connect. Мир информационных технологий»

Редакционный отдел  
 editor@connect-wit.ru  
 (495) 925-1118

Выпускающий редактор  
 Валерия Назарова  
 vnazarova@connect-wit.ru

Журналисты-обозреватели  
 Светлана Арянина  
 asp@connect-wit.ru  
 Валерий Коржов  
 korzhov@connect-wit.ru  
 Дмитрий Шульгин  
 shulgin@connect-wit.ru

Литературный редактор  
 Елена Шевелева

## ИЗДАТЕЛЬ ООО «ИД КОННЕКТ»

Генеральный директор  
 Евгений Самохвалов  
 evs@connect-wit.ru  
 (495) 925-1118

Заместитель генерального директора  
 Дмитрий Корешков  
 dima\_k@connect-wit.ru

Руководитель отдела развития  
 Наталья Павлова-Шульгина  
 pravlova@connect-wit.ru  
 (903) 798-74-17

Директор по региональным проектам  
 Инга Орлова  
 regions@connect-wit.ru  
 (903) 742-54-71

Отдел рекламы  
 (495) 925-1118

Макетирование и верстка  
 Алексей Григорьев

Цветокоррекция  
 Александра Шанина

Фото на обложке  
 Алексей Шанин

Тел.: (495) 925-1118 (многоканальный),  
 факс: (495) 925-1118  
 E-mail: editor@connect-wit.ru  
 http://www.connect-wit.ru

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), регистрационный номер ПИ № ФС77-54349

Учредитель: ООО «Коннект-ИКТ»

Адрес редакции: 129626, Москва,  
 3-я Мытищинская ул., д. 3, стр. 1

Тел.: (495) 925-1118 (многоканальный)  
 Факс: (495) 925-1118

E-mail: editor@connect-wit.ru  
 http://www.connect-wit.ru

Отпечатано ООО «Полиграфический комплекс «Союзпечать»  
 Тираж 15 000  
 Цена свободная

При использовании материалов ссылка на журнал обязательна.  
 Ответственность за рекламные материалы несет рекламодатель.

Мнения авторов и компаний могут не совпадать с мнением редакции.

© «Connect. Мир информационных технологий»

## Внимание!

Редакционную подписку  
 на журнал **Connect**  
 вы можете оформить  
 в редакции

Общество с ограниченной  
 ответственностью «ИД КОННЕКТ»  
 ООО «ИД КОННЕКТ»  
 Тел.: (495) 925-1118

Платежные реквизиты получателя:  
 р/сч № 40702810340190646901  
 БИК 044525555  
 к/сч № 30101810400000000555  
 ОАО «Промсвязьбанк» г. Москва

Через сайт в Интернете: <http://www.connect-wit.ru>

### Стоимость редакционной подписки (для жителей РФ)

Издание, периодичность		Стоимость подписки, руб.	
		экземпляр	на год
<b>Connect. Мир информационных технологий</b> 8 номеров в год	Российский авторитетный бизнес-журнал. Мониторинг и экспертиза возможностей информационных технологий и телекоммуникаций для оптимизации бизнеса. Информатизация и связь в отраслях, ведомствах и регионах России и СНГ.	250*	2000*

\* Не включает доставку.

Читателям, живущим за пределами РФ, необходимо отправить в редакцию заявку в простой письменной форме на e-mail: [secretar@connect.ru](mailto:secretar@connect.ru)  
 (в этом случае к стоимости журнала будет добавлена сумма почтовых расходов).

### Подписка в альтернативных агентствах

ОАО «Урал-Пресс», г. Москва (495) 789-8636

Выбрать наиболее удобное  
 для вас агентство можно также  
 на сайте [www.connect-wit.ru](http://www.connect-wit.ru)  
 (раздел подписки) или  
 по телефону: (495) 925-1118

### Рекламодатели номера

Информзащита..... 1-я обл., 4–10 ЛМ Софт..... 12–17, 18–19  
 Конфидент..... 66

### Информация о партнерах

АРМИЯ-2017..... 4-я обл.  
 Интерполитех..... 3-я обл.

# Читайте в августовском номере журнала

Тема номера

Кибервойны XXI века: что нас ждет и к чему готовиться



Кибервойны как развитие информационных войн XX века на новом технологическом уровне

Готовность России к ведению современных кибервойн

Мировые тенденции и изменения в области безопасности глобальных информационных сред

Рост таргетированных атак на государственные и корпоративные информационные инфраструктуры

Импортозамещение в области ИБ как необходимое условие появления эффективных отечественных компонентов национальной киберобороны

WWW.INTERPOLITEX.RU

МОСКВА, ВДНХ, ПАВИЛЬОН № 75  
17-20 ОКТЯБРЯ 2017



2017

XXI МЕЖДУНАРОДНАЯ ВЫСТАВКА

WWW.INTERPOLITEX.RU

# INTERPOLITEX



СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА



ВЫСТАВКА  
ПОЛИЦЕЙСКОЙ  
ТЕХНИКИ



ВЫСТАВКА  
«РОСГВАРДИЯ»



ВЫСТАВКА  
«ГРАНИЦА»



ВОЗМОЖНОСТИ  
ПРОМЫШЛЕННОГО  
СЕКТОРА УИС



ФОРУМ НСБ  
«БЕЗОПАСНАЯ  
СТОЛИЦА»

ОРГАНИЗАТОРЫ



МВД России



ФСБ России



Росгвардия

ОРГАНИЗАТОР  
ВЫСТАВКИ «ГРАНИЦА»



ПС ФСБ России

ЭКСПОНЕНТ-КООРДИНАТОР  
ОТ МВД РОССИИ



ФКУ «НПО «СТИС»  
МВД России

ГЕНЕРАЛЬНЫЙ  
УСТРОИТЕЛЬ



ЗАО «ОВК «БИЗОН»



Выставка одобрена  
Всемирной ассоциацией  
выставочной индустрии



Выставка прошла аудит  
Российского Союза  
выставочной индустрии



Выставка одобрена  
Российским Союзом  
выставочной индустрии

Дирекция выставки:  
129223, Москва, а/я 10 ЗАО «ОВК «БИЗОН»  
Телефон/факс: 8 (495) 937-40-81  
E-mail: [info@interpolitex.ru](mailto:info@interpolitex.ru)  
[www.b95.ru](http://www.b95.ru) [www.interpolitex.ru](http://www.interpolitex.ru)



Организатор



МИНИСТЕРСТВО ОБОРОНЫ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

22-27  
августа

  
**ARMY**

**2017**

МЕЖДУНАРОДНЫЙ  
ВОЕННО-ТЕХНИЧЕСКИЙ  
ФОРУМ

Место проведения



ПАТРИОТ  
ЭКСПО

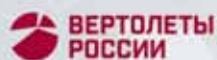
Выставочный оператор



МКВ

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

Генеральный партнер



Генеральный спонсор



Генеральный спонсор



Стратегический партнер

