

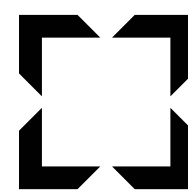
**ГИБРИДНЫЕ ВОЙНЫ  
XXI ВЕКА /8  
ГЕНДИРЕКТОР «РОСТЕХА»  
СЕРГЕЙ ЧЕМЕЗОВ:  
«ПОЛНОГО  
ИМПОРТОЗАМЕЩЕНИЯ  
НЕ ПЛАНИРУЕТСЯ» /5  
ЗАЧЕМ МОЛОДЫМ  
СПЕЦИАЛИСТАМ  
СТОИТ ИДТИ  
В ОБОРОНКУ? /11**

В ОБОРОНКУ?/11

**Вторник, 26 мая 2015**  
Тематическое приложение  
к газете «Коммерсантъ» №17

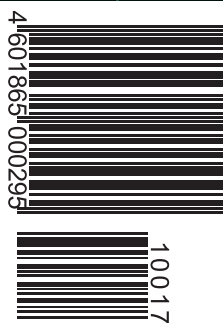
**Коммерсантъ**

# BUSINESS GUIDE



# Ростех

ГЕНЕРАЛЬНЫЙ ПАРТНЕР ВЫПУСКА



CRICKET



**Ростех**

*Партнер в развитии*



СВЕТЛАНА РАГИМОВА,  
РЕДАКТОР BUSINESS GUIDE  
«IT В ОБОРОННО-ПРОМЫШЛЕННОМ  
КОМПЛЕКСЕ»

**БЕСКОНЕЧНАЯ ИСТОРИЯ**  
Поколение родом из СССР привыкло к тому, что нас окружает мир технологий, созданных военными. Трактор может превратиться в зенитный комплекс, как гусеница в бабочку, а корпус чайника изначально должен был стать частью ракеты, но из-за экономических проблем на ракетном заводе руководство решило переоборудовать его в фабрику бытовой техники. Быть окруженным предметами, напоминающими о войне,— это накладывает свой отпечаток: любимые игры детей конца прошлого века — войнушки и «казаки-разбойники». 21-е столетие повернуло ситуацию в другую сторону — информационные технологии, созданные в мирных целях, начинают применяться в оборонке, а дети поголовно увлеклись виртуальными фермами и строительством вселенной Minecraft (которая была бы уже больше нашей планеты, если бы существовала реально). Виртуальная и дополненная реальность, беспилотные шагающие машины и летающие дроны, кибероружие и информационные провокации — оружие новых гибридных войн. Оно выглядит более мирным и уменьшает вероятность гибели на поле боя. Возможно, еще лет через 50 война вообще будет происходить лишь на уровне идей и анализа «больших данных». Единственное, о чем можно сказать уверенно: человечество никогда не перестанет воевать.

Тематическое приложение к газете «Коммерсантъ» (Business Guide-IT в оборонно-промышленном комплексе)  
Владимир Желонкин — президент АО «Коммерсантъ»  
Мария Комарова — генеральный директор АО «Коммерсантъ»  
Азер Мурсалиев — шеф-редактор АО «Коммерсантъ»  
Сергей Яковлев — главный редактор газеты «Коммерсантъ»  
Анатолий Гусев — автор дизайн-макета  
Павел Кассин — директор фотослужбы  
Валерия Любимова — коммерческий директор АО «Коммерсантъ»  
Рекламная служба:  
Тел. (499) 943-9108/10/12, (495) 101-2353  
Алексей Харнас — руководитель службы «Издательский синдикат»  
Светлана Рагимова — выпускающий редактор  
Ольга Боровягина — редактор  
Сергей Цомык — главный художник  
Виктор Куликов — фоторедактор  
Екатерина Бородулина — корректор  
Адрес редакции: 125080, г. Москва, ул. Врубеля, д. 4.  
Тел. (499) 943-9724/9774/9198  
Учредитель: АО «Коммерсантъ».  
Адрес: 127055, г. Москва, Тихвинский пер., д. 11, стр. 2.  
Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).  
Свидетельство о регистрации СМИ — ПИ № ФС77-38790 от 29.01.2010

Типография: «Сканвеб Аб». Адрес: Корьяланкату 27, Коувола, Финляндия  
Тираж: 75000. Цена свободная  
Рисунок на обложке: Леонид Фирсов

# ТРАНСФОРМАЦИЯ ЩИТА И МЕЧА

## РОБОТОТЕХНИКА, АНАЛИТИКА БОЛЬШИХ ДАННЫХ, ДОПОЛНЕННАЯ РЕАЛЬНОСТЬ, 3D-МОДЕЛИРОВАНИЕ, ИНТЕРНЕТ ВЕЩЕЙ И ПРОЧИЕ НАПРАВЛЕНИЯ ДВИЖЕНИЯ ТЕХНИЧЕСКОГО ПРОГРЕССА ОТРАЖАЮТСЯ НА РАЗВИТИИ ОБОРОННОЙ ИНДУСТРИИ НЕ МЕНЬШЕ, ЧЕМ НА ВСЕХ ОСТАЛЬНЫХ. ЦИФРОВИЗАЦИЯ ПРОНИКАЕТ В ЭТУ ОБЛАСТЬ И, ТАК ЖЕ, КАК ДРУГИЕ СФЕРЫ, ТРАНСФОРМИРУЕТ ЕЕ.

СВЕТЛАНА РАГИМОВА

Технический прогресс много лет двигался вперед в основном благодаря гонке вооружений: оборудование и технологии военного назначения находили применение в мирной жизни. Даже тракторы и прочая сельхозтехника разрабатывались так, чтобы их можно было быстро переоборудовать в зенитный комплекс или другое транспортное средство военного назначения. В области информационных технологий наблюдается обратный процесс: частный бизнес создает и осваивает инновации быстрее, чем оборонные предприятия, которым есть чему поучиться, к примеру, у Google с «Яндексом».

По этой причине министр обороны США Эш Картер практически сразу после подписания новой стратегии Пентагона в области кибербезопасности отправился в Кремниевую долину, чтобы встретиться с представителями высокотехнологичных компаний и экспертов и договориться с ними о сотрудничестве, которое будет гарантировать, что американская армия владеет самыми передовыми технологиями в области противодействия киберугрозам. Решения в области информационной безопасности, а также многие другие современные IT из сферы частного бизнеса находят применение сегодня в военно-промышленном комплексе.

**МИЛЛИОНЫ ЧУВСТВИТЕЛЬНЫХ ГЛАЗ**  
Одну из модных тем, которая активно обсуждается во всем мире, не обошли вниманием и военные. Аналитика больших данных (Big Data) может применяться для решения задач самых разных типов. Ученые, работающие в области анализа больших данных, так называемые Data Scientists, по заявлениям Пентагона, одни из самых вос-

требуемых в американской военной индустрии. Различные военные машины, колесный транспорт, беспилотники и прочие мобильные оборонные комплексы сегодня оснащаются сенсорами, с которых транслируется огромный поток информации, дающей представление о ходе сражения. Но проблема заключается в том, что этой информации слишком много. Реджи Бразерс, заместитель помощника министра обороны США по исследованиям, на симпозиуме Ассоциации армии США привел такой пример: один из наиболее совершенных на сегодня сенсоров — Argus-IS может транслировать миллионы терабайт данных и 5 тыс. часов видео высокой четкости в день. Эта информация собирается посредством 1,8-гигапиксельной камеры и с 368 сенсоров, встроенных в Argus-IS, которыми можно оснастить беспилотник MQ-9 Reaper («Жнец»). В Пентагоне рассчитывают, что правильно организованный анализ и визуализация этих данных позволят уменьшить количество операторов, необходимых для управления беспилотной техникой разного типа — сегодня на каждую машину приходится один человек, который ею управляет. Но чтобы накопить что-то полезное во всех этих горах терабайтов, нужны ученые, специализирующиеся на анализе данных, за которых военным приходится вступать в конкуренцию с «мирными» индустриями. В перспективе одного человека будет достаточно, чтобы дистанционно управлять группами беспилотных танков, самолетов и прочей техники.

Инструменты для работы с большими данными пригодятся и в кибервойне, которая сейчас сопровождается изощренной пропагандой, а также информационными вбросами и кампаниями по дезинформации. Для этого ис-

пользуются популярные новые медиа — социальные сети, сервисы для ведения блогов, агрегаторы новостей, видеохостинги и т. д. Анализ текстов из традиционных СМИ и новых медиа — задача либо для армии людей, оценивающих каждую фразу, либо для искусственного интеллекта. «Ростех», к примеру, владеет технологией, которая помогает автоматически анализировать огромные массивы текстов, причем проводить не структурный анализ и поиск ключевых слов, а семантический. Система фактически понимает смысл текстов. В перспективе этот же подход может использоваться для анализа видео и статичного изображения, а также звука.

Но области применения «больших данных», конечно этим не исчерпываются. Например, в армии США используется анализ данных в системах, отслеживающих техническое состояние оборудования и техники. Из миллиардов каналов данных (датчики, системы мониторинга работоспособности, бортовые рабочие станции и т. д.) информация сохраняется и автоматически анализируется на технической платформе Teradata, что позволяет предупреждать поломки, например, в вертолетах Apache. Анализ информации о режимах полета, об отказах оборудования, заключенный техосмотров и т. д. и прогнозы на основе этих данных помогают сделать полеты более безопасными. Кроме того, такие технологии дают прямую экономию: за три года использования системы для мониторинга состояния ракет армия США сохранила \$14,9 млн. Системы наведения в ракетах меняли не планоно «по часам», а только при необходимости, если это требовалось.

Александр Якунин, генеральный директор Объединенной приборостроительной корпорации, входящей в госу- ➔



ДАТЧИКИ СОВРЕМЕННЫХ БЕСПИЛОТНЫХ МАШИН ГЕНЕРИРУЮТ ОГРОМНЫЕ ПОТОКИ ДАННЫХ

## ПЕРСПЕКТИВА

дарственную корпорацию «Ростех», рассказывает, что по заказу нескольких крупных компаний его организация ведет разработку сложных автоматизированных систем мониторинга инфраструктурных объектов. В них интегрируются оптико-электронные устройства, радиолокаторы, беспилотники, датчики, средства передачи данных. Это так называемые умные системы — без участия человека они могут контролировать любые действия на объектах, распределять команды и ставить цели различным модулям, отличать нештатные ситуации от плановых работ и т. д. Такие же технологии применимы в мирных отраслях. В нефтянке они помогают компаниям бороться с хищениями и утечками на нефтепроводах, снижая производственные потери. В энергетике — контролировать состояние объектов, сетей, предупреждать аварийные ситуации и оперативно реагировать на них и т. д.

Как говорят аналитики, очень вероятно, что в перспективе именно правильное обращение с Big Data может стать решающим для исхода отдельных битв и даже напрямую влиять на ход военных кампаний. Именно эти технологии наиболее значительно трансформируют оборонную промышленность и армию.

**С ТРЕХ СТОРОН** Объем мирового рынка 3D-принтеров, по прогнозу аналитиков исследовательской компании Canalys, достигнет к 2018 году \$16,2 млрд. Это значит, что растет он примерно в полтора раза каждый год. На таких устройствах можно печатать украшения, детские игрушки, предметы интерьера, музыкальные инструменты и прочие не самые важные в жизни людей вещи. Но не только — уже пробуют с помощью 3D-печати создавать персональные лекарства, дома и даже искусственные органы. А два года назад мировые СМИ облетела история про американского оружейника-энтузиаста Коди Уилсона, который напечатал из пластика на обычном 3D-принтере пистолет и назвал его Liberator («Освободитель»). Из 16 деталей только одна была металлической (из куска гвоздя) — боек. Коди Уилсон выложил модель в свободный доступ, так что любой желающий может повторить его эксперимент. К слову, это оружие способно было выдержать до 11 выстрелов, а ствол в случае износа можно просто заменить на новый. Еще полгода спустя инженеры из техасской компании Solid Concepts впервые в мире напечатали уже пистолет из металла. Они хотели тем самым продемонстрировать, на что способны 3D-принтеры. На этот раз был напечатан классический культовый M1911 — «Браунинг». Конечно, военная промышленность вряд ли будет массово печатать оружие (впрочем, посмотрим лет через десять). Но 3D-моделирование и даже 3D-печать уже с успехом используются в оборонке для создания концептов и прототипов новейшей техники. Так, на конференции «Беспилотная авиация-2015» в Москве докладчик из госкорпорации «Ростех» рассказал о создании демонстрационной модели нового БПЛА (беспилотного летательного аппарата), комплектующие для которой печатались на 3D-принтере. Устройство, которое назвали «Чирок», получилось нешуточное: весит 750 кг, а размах крыльев — 10 м. Шасси в этом БПЛА отсутствуют — вместо них воздушная подушка, мембрана которой сделана из особого материала по закрытой военной технологии. Для взлета и посадки не требуется специально оборудованной полосы, ею может служить любая относительно ровная поверхность: снег, вода, грунт и проч. Благодаря этому «Чирок» может передвигаться по кочкам высотой до 20 см и ямам шириной до 1 м.

«Чирок» способен нести до 300 кг груза (например, скрытое в корпусе вооружение), максимальная высота его полета — 6 км, а дальность — 2,5 тыс. км. В ближайшем будущем на базе этого аппарата будет создан более продвинутый беспилотник весом 2 тонны. В его

**ПО ОЦЕНКАМ СПЕЦИАЛИСТОВ, СРОК РАЗРАБОТКИ ИЗДЕЛИЙ ПРИ ИСПОЛЬЗОВАНИИ НОВОГО ПОДХОДА К ПРОЕКТИРОВАНИЮ МОЖЕТ УМЕНЬШИТЬСЯ КАК МИНИМУМ НА 30%**



ДЕТАЛИ ДЛЯ ДРОНА «ЧИРОК» ПЕЧАТАЛИ НА 3D-ПРИНТЕРЕ

разработке также будет применяться 3D-печать, которая позволяет быстро придумать устройство и в кратчайшие сроки создать модель, напечатав уникальные комплектующие самостоятельно, а не заказывая их штучное производство на специальном предприятии. Но это еще не все — план по развитию стратегической авиации подразумевает, что уже в следующем году будет создан пятитонный беспилотник, а в 2018-м — двадцатитонный. Вероятно, этот «монстр» сможет перевозить даже группы людей.

Проектирование моделей в трех измерениях сразу — это на сегодня мировой промышленный стандарт. В идеале системы, которые используются для проработки проектов новой техники, должны позволять отслеживать судьбу каждого изделия от эскиза до утилизации. Для того чтобы распространять в России лучшие мировые практики, холдинг «Технодинамика» госкорпорации «Ростех» открыл в 2014 году в Москве Центр проектирования, где применяются наиболее современные подходы к разработке изделий. Сейчас холдинг расширяет сеть центров проектирования в регионы. «Технодинамика» использует для проектирования программные решения Siemens PLM Software. Аналогичное ПО установлено и у крупнейших партнеров холдинга — ОАК, ОДК, «Вертолетов России». Унификация подходов к использованию ПО позволяет существенно упростить процедуры обмена данными между заводами и КБ, заказчиками, сократить затраты и время конструкторской и технологической подготовки производства. Специализированное ПО позволяет экономить время при выполнении типовых трудоемких операций при рисовке эскиза проекта, проектировании, моделировании механически обрабатываемых элементов каркаса и запуска в производство.

Унифицированные цифровые технологии, применяемые в центрах проектирования «Технодинамики», предполагают командный доступ к работе над продуктом, а значит, параллельный инжиниринг, что существенно ускоряет процесс работы над изделием. Все этапы создания продукта: от разработки конструктором 3D-модели до подготовки управляющих программ для станков с числовым программным управлением и контроля геометрических параметров — можно отслеживать в режиме реального времени в единой информационной базе. Центр оснащен передовыми цифровыми системами, хранящими все необходимые инженерные данные: инженерные расчеты, 3D-модели проектирования, технологическую документацию, изменения в проектной и исполнительной документации.

В «Технодинамике» утверждают, что современный подход позволяет сократить количество переработок конструкций, в полтора раза сократить затраты на разработку новых продуктов и время вывода их на рынок. По оценкам специалистов, срок разработки изделий при использовании нового подхода к проектированию может уменьшиться как минимум на 30%.

Отчасти ускорение и удешевление разработки достигается за счет отказа от постройки большого количества натурных образцов. «Мы применяем виртуальное проектирование и виртуальное тестирование, которые позволяют значительно сократить в том числе количество натурных испытаний», — говорит генеральный директор холдинга «Технодинамика» Максим Кузюк.

Как отмечают в холдинге «Технодинамика», ПО способно моделировать и цеховые операции, и процесс производства изделия, что помогает оптимизировать технологические процессы. А интеграция с ERP-системой позволяет отслеживать запасы продукции, требуемый объем сырья.

**«ОБЛАЧНЫЙ» ПРОГНОЗ** Сбор, хранение и анализ огромных массивов данных, работа в сложных PLM-системах, использование другого рода «тяжелого» ПО — все это автоматически рождает потребность в виртуализации и применении «облачных» технологий.

«Облака» на службе оборонной промышленности в развитых странах уже обычное дело. Каждый год правительство США тратит около \$76 млрд на информационные технологии, а именно на поддержку и эксплуатацию более 10 тыс. различных систем в госсекторе. Еще шесть лет назад в стране было объявлено о Федеральной правительственной инициативе облачных вычислений (Federal Government's Cloud Computing Initiative), и уже на следующий год стартовало четыре крупных проекта в этой области. В частности, запущен портал SaaS-инструментов для госучреждений Apps.gov, а позже появился правительственный сайт USA.gov, работающий на «облачной» инфраструктуре. «Облаками» пользуются практически все подразделения армии США — от авиации до пехоты — и, конечно же, кибервойска. В 2011 году президент США Барак Обама подписал бюджет, в котором распространение облачных вычислений было названо основной частью стратегии по развитию новейших эффективных и действенных технологий. За последние годы правительство США перевело около четырех сотен своих ЦОДов на «облака» и закрыло ряд устаревших ЦОДов, а к концу 2015 года планирует остановить работу 40% своих дата-центров, что позволит сэкономить \$5 млрд.

Министерство обороны США широко применяет «облака», хотя и испытывает беспокойство, не будучи уверено

в их полной безопасности, особенно после инцидентов, связанных с WikiLeaks. В 2011 году министерство создало более защищенную «облачную» среду с ограниченным использованием коммерческих продуктов. Агентство перспективных оборонных исследовательских проектов помогает министерству сделать «облако» более безопасным.

«Облака» активно используются и в других странах. По прогнозу IDC, целенаправленная политика Евросоюза в области развития рынка «облачных» решений приведет к тому, что расходы на публичные «облачные» сервисы в этом регионе вырастут с €35,2 млрд до €77,7 млрд евро к 2020 году. Причем, как считают аналитики компании, если власти ЕС не будут вмешиваться в функционирование рынка «облаков», то к 2020 году этот сектор экономики принесет €88 млрд в ВВП. А если ЕС решится на регулирование, то рынок способен сгенерировать до €250 млрд к этому же сроку.

В России «облака» также осваиваются государственными организациями, но не так активно. По инициативе Минсвязи в последние несколько лет стартовало несколько крупных проектов в этой области. Первый масштабный проект по созданию «Национальной „облачной“ платформы 07» был запущен четыре года назад под эгидой «Ростелекома». Это комплекс интегрированных информационных систем разного назначения для предоставления услуг населению.

В распоряжении правительства РФ от 1 ноября 2013 года, касающемся Стратегии развития отрасли информационных технологий в РФ на 2014–2020 годы и на перспективу до 2025 года, говорится, что к 2018 году применение «облачных» сервисов в корпоративной среде в России станет массовым, особенно в сфере малого и среднего бизнеса. Рост этого сегмента бизнеса может превысить 80% в год. По прогнозам аналитиков, мировой рынок «облачных» вычислений возрастет к 2020 году с \$50 млрд до \$240 млрд. «Облака» перечислены в списке наиболее приоритетных направлений исследований и разработок. В российской промышленности и в ОПК «облачные» технологии только начинают применяться. ■



# «ГЛАВНОЕ — МАСШТАБНОЕ ОБНОВЛЕНИЕ ПРОИЗВОДСТВА»

## ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ГОСКОРПОРАЦИИ «РОСТЕХ» СЕРГЕЙ ЧЕМЕЗОВ УВЕРЕН, ЧТО У РОССИЙСКИХ ОБОРОННЫХ ПРОДУКТОВ БОЛЬШОЙ ПОТЕНЦИАЛ. ОН ПРИЗНАЕТ, ЧТО ВОЕННЫЕ СЕГОДНЯ УЧАТСЯ У «МИРНЫХ» ОТРАСЛЕЙ, ОСОБЕННО В ТОМ, ЧТО КАСАЕТСЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, НО СЧИТАЕТ, ЧТО ОБОРОНКА ПО-ПРЕЖНЕМУ МОЖЕТ ПРИНОСИТЬ ПОЛЬЗУ И ЧАСТНОМУ БИЗНЕСУ, И ЭКОНОМИКЕ В ЦЕЛОМ.

**BUSINESS GUIDE:** Оборонная промышленность всегда была источником новейших технологий, которые двигали технический прогресс, в том числе в мирных сферах. Изобретения переносились в жизнь людей, в бизнес, применялись (и до сих пор применяются) в государственном управлении. Это движение инноваций из ОПК в мир продолжается?

**СЕРГЕЙ ЧЕМЕЗОВ:** Такая тенденция в целом сохраняется. Государственные институты могут проводить фундаментальные исследования, которые для бизнес-структур были бы слишком дороги, учитывая, что поначалу не ясно, можно ли будет коммерциализировать ту или иную разработку. Но важно отметить, что тенденция меняется. Сегодня стоит уже говорить о взаимном обогащении, то есть что-то переходит из военки в гражданку, но миграция технологий из гражданки в военку не меньше. Ведь в гражданские сферы инвестируют десятки миллиардов долларов частные компании, фонды, частные инвесторы. А также продукция выпускается более массовыми сериями, в отличие от военных предприятий, где изготавливаются штучные изделия.

**BG:** Работает ли это в обратную сторону? Какие технологии из бизнес-сферы и прочих «мирных» отраслей начинают использоваться в целях укрепления обороны страны? Можно ли сказать, что это в первую очередь информационные технологии?

**С. Ч.:** Да, это именно так, и «Ростех», будучи современной корпорацией, принимает во внимание эти тенденции. В том, что касается сферы ИТ, движение идет в обратном направлении — из гражданского сектора в военный. Дело в том, что компании, работающие на огромный гражданский рынок, могут привлекать большие инвестиции, которые направляются на разработку соответствующих продуктов. Учитывая масштабы рынка, большое число копий, которые можно продать, производство получается дешевым, эффективным. А военным зачастую нужны штучные продукты — слишком дорого создавать под их производство отдельные предприятия. Например, объем российского рынка автоматизированных систем управления в 2013 году в гражданском секторе ориентировочно составил 2,4 трлн руб., в специальном — всего 4,7 млрд руб.

«Ростех» выбрал следующий подход. Гражданский госзаказ позволит сформировать команды, которые будут работать и над решениями для оборонно-промышленного комплекса. Работа большинства наших ИТ-холдингов сосредоточена на продуктах для коммерческого рынка, а потом на этих решениях могут разрабатываться продукты для военных.

**BG:** Какие на сегодняшний день главные задачи стоят перед оборонной промышленностью? Как информационные технологии помогают эти задачи решить?

**С. Ч.:** Главное — масштабное обновление производства, повышение его эффективности, рост производительности труда. Информационные технологии имеют непосредственное отношение к решению этих задач, это один из



ключевых факторов конкурентоспособности оборонного предприятия. Сегодня необходимо, во-первых, выбрать приоритетные ИТ-решения, чтобы системы на разных предприятиях не конфликтовали друг с другом, нужна единая платформа. Во-вторых, нужно централизовать ИТ-закупки, что позволит повысить их прозрачность и добиваться максимальных скидок от поставщиков. Этим в «Ростехе» занимается компания «РТ-Информ». Наконец, необходимо наладить производство собственного софта и «железа». Софтом в «Ростехе» занимаются НЦИ, ЦНИСУ и другие, а «железом» — Объединенная приборостроительная корпорация.

Нужно учитывать, например, что коммерческие системы управления базами данных (СУБД), которые используются в гражданском секторе, имеют закрытый исходный код. Из-за того что нет доступа к исходному коду, нельзя проверить, есть ли там закладки. Кроме того, для работы таких систем нужна их поддержка из-за рубежа. К тому же нельзя влиять на развитие таких СУБД. Нужно учитывать и высокую стоимость лицензий. Это как раз те проблемы, которые мы решаем.

**BG:** Насколько ИТ в российской оборонке и в промышленности в целом зависимы от импорта и какие риски это несет? Как с ними справляются предприятия на сегодняшний день?

**С. Ч.:** Зависимость от импорта ИТ на сегодняшний день колоссальная — от 90% до 100%. Это как раз одна из проблем, над решением которой работают в «Ростехе». Есть ключевые сферы, где импортозамещение, безусловно, необходимо. Это касается, например, каналов обмена информацией между оборонными предприятиями. Понятно, что речь зачастую идет о передаче секретной информации. Здесь необходимы российские решения, поскольку в надежности и безопасности импортных продуктов абсолютной уверенности быть не может.

**BG:** Возможно ли, на ваш взгляд, достичь полного импортозамещения ИТ в промышленности и, в частности, оборонном комплексе? Какими путями можно это сделать и сколько времени это займет? Какова роль «Ростеха» в этом процессе?

**С. Ч.:** Полного импортозамещения не планируется, в этом нет необходимости. Оно нужно лишь там, где речь идет об обеспечении национальной безопасности. Что касается времени, то в ключевых сферах импортозамещение должно произойти в течение ближайших пяти-семи лет. Задачи «Ростеха» — формирование единой техполитики в сфере ИТ для предприятий корпорации, обеспечение прозрачности закупок, производство собственных продуктов, обеспечивающих максимальную защиту информации.

**BG:** Какие на сегодняшний день главные стратегические направления деятельности «Ростеха» и почему? В какие технологии госкорпорация верит больше всего? Какие конкурентные преимущества есть у российской продукции оборонного назначения? Какие продукты российского производства в данной отрасли наиболее востребованы за рубежом? На каких рынках?

**С. Ч.:** В «Ростехе» входит 16 холдингов, которые производят как военную, так и гражданскую продукцию. Одна из принципиально важных задач сегодня — это повышение доли гражданской продукции, которую выпускают оборонные компании, при одновременном увеличении экспорта. К 2020 году доля гражданской продукции оборонных холдингов должна достичь минимум 50%. Такая необходимость объясняется, в частности, тем, что масштабная программа перевооружения рассчитана именно до 2020 года, а потом мощности предприятий, выпускающих сегодня военную продукцию, в любом случае нужно будет переориентировать на выпуск гражданской.

Мы кардинально поменяли систему корпоративного управления, передали основные полномочия по управлению активами холдингам. Задача для них — стать компаниями, конкурентоспособными на мировом рынке. В вопросе технологий необходимо ориентироваться на стандарты наилучших доступных технологий, в особенности на ресурсосберегающие технологии. Это позволит понизить производственные издержки и снизить негативное воздействие на окружающую среду.

На мировом рынке вооружений Россия сохраняет и укрепляет свои позиции. В 2014 году через «Рособоронэкспорт» было экспортировано вооружения и военной техники на \$13,2 млрд, план был немного перевыполнен. Основными конкурентными преимуществами нашей техники являются ее надежность, удобство в эксплуатации, а также зачастую более низкая цена, чем у конкурентов. При этом важно отметить, что мы готовы создавать совместные производства с нашими партнерами, что делает сотрудничество более привлекательным для них. Традиционные партнеры — Индия, Китай, Вьетнам, активно развивается сотрудничество с Латинской Америкой. Особым спросом пользуются вертолеты. По данным на 2014 год, «Вертолеты России» выпустили 24% мирового парка вертолетов военного назначения. Большим спросом пользуются российские боевые самолеты, «Суши», «МиГи», системы ПВО.

**BG:** Как будут меняться подходы и технологии, направленные на укрепление обороноспособности страны, в связи с развитием инноваций, которые все больше и больше переносят деятельность людей в виртуальное пространство? Какие риски это несет для обороноспособности страны и что в связи с этим необходимо предпринимать?

**С. Ч.:** Здесь главное — обеспечить защиту информации, которая переносится в виртуальное пространство. Не секрет, что за рубежом уже создаются кибервойска как раз для действий в киберпространстве. Необходимо работать над защитой от информационного воздействия, в том числе от промышленного шпионажа. Это еще одна причина для проведения импортозамещения в сфере ИТ. Объединенная приборостроительная корпорация уже определила в качестве одного из приоритетных направлений разработку инфраструктуры сетей связи государственных органов власти, силовых структур и сетей связи государственных корпораций. ОПК исходит из необходимости обеспечить независимость жизненного цикла изделия от конкретных зарубежных производителей и внешних угроз. При этом акцент будет делаться на интеллектуальной составляющей разработок, в том числе использовании отечественной ЭКБ и ПО. Основная добавленная стоимость, безусловно, должна создаваться на территории РФ. Напомню, что недавно в России началась продажа опытных образцов первых персональных компьютеров и серверов, собранных на базе отечественного микропроцессора «Эльбрус-4С». Производители — МЦСТ и ИНЭУМ им. И. С. Брука — входят в ОПК. Так что наши усилия уже приносят конкретные результаты.

Интервью взяла СВЕТЛАНА РАГИМОВА

**В 2014 ГОДУ ЧЕРЕЗ «РОСОБОРОНЭКСПОРТ» БЫЛО ЭКСПОРТИРОВАНО ОРУЖИЯ И ВОЕННОЙ ТЕХНИКИ НА \$13,2 МЛРД. ПЛАН БЫЛ НЕМНОГО ПЕРЕВЫПОЛНЕН**



# САМИ С КОДАМИ

СНИЖЕНИЕ ЗАВИСИМОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ — ОДНА ИЗ ПЕРВОСТЕПЕННЫХ ЗАДАЧ, РЕШАЕМЫХ ПРАВИТЕЛЬСТВОМ РФ. ИМПОРТОЗАМЕЩЕНИЕ В ИТ НАПРЯМУЮ СВЯЗАНО С ОБЕСПЕЧЕНИЕМ КИБЕРБЕЗОПАСНОСТИ И ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИИ. НАИБОЛЕЕ ОСТРО СТОИТ НЕОБХОДИМОСТЬ РАЗРАБОТКИ ОТЕЧЕСТВЕННЫХ АНАЛОГОВ ИНФОРМАЦИОННЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ В ОБОРОННО-ПРОМЫШЛЕННОМ КОМПЛЕКСЕ СТРАНЫ, ФЕДЕРАЛЬНЫХ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ И НА ПРЕДПРИЯТИЯХ, РАБОТАЮЩИХ НА НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ.

ЮЛИЯ ВОРОНИНА

В прошлом году Минпромторг разработал программу по импортозамещению в оборонно-промышленном комплексе. Приоритет был отдан созданию Национальной электронно-компонентной базы космического назначения и станкостроению. Необходимость решения этих задач возникла в связи с введением антироссийских санкций. Как заявлял в апреле текущего года заместитель председателя правительства РФ Дмитрий Рогозин, программа уже частично выполнена и завершится до конца 2017 года.

А в марте Минпромторг опубликовал план мероприятий по импортозамещению в радиоэлектронной промышленности до 2020 года. План содержит перечень из 534 видов продукции, производство которой предстоит развивать в стране: телеком-оборудование, полупроводниковая СВЧ-электроника, микропроцессоры, периферийное оборудование и электронные компоненты. Также планируется снизить импорт суперкомпьютеров, серверов, в том числе файловых и почтовых, систем хранения данных и систем управления базами данных (СУБД).

Объединенная приборостроительная корпорация (ОПК), входящая в госкорпорацию «Ростех», будет заниматься разработкой, производством и внедрением телекоммуникационного оборудования и вычислительной техники. Она возглавит процесс импортозамещения в ведущей оборонной корпорации и станет одним из крупнейших ИКТ-предприятий страны, вовлеченных в процесс импортозамещения. «Сегодня перед государством остро стоит вопрос импортозамещения критически важных технологий, в первую очередь в области связи, телекоммуникаций, хранения и передачи данных. Эти технологии являются важнейшим элементом экономической стратегии, промышленной политики, национальной безопасности страны, — отметил генеральный директор «Ростеха» Сергей Чемезов на заседании правления госкорпорации. — Поэтому мы намерены активно развивать разработку, производство, внедрение передовой российской техники и наших технологий».

**ВНУТРЕННИЕ СВЯЗИ** План по импортозамещению в сфере разработки ПО в апреле также утвердило Минкомсвязь. Он включает в себя три блока. Первое направление предполагает предоставление преференций отечественной ИТ-продукции при осуществлении закупок за государственный счет. Сюда входят бизнес-приложения, антивирусное ПО, софт для информационной безопасности и интернет-сервисы для корпоративной среды. Второй блок плана включает поддержку коллективной разработки ПО в тех сегментах рынка, где нет достаточно-го задела в виде конкурентоспособных отечественных продуктов. Это клиентские и мобильные операционные системы (ОС), серверные ОС, системы управления базами данных, средства управления «облачной» инфраструктурой и виртуализацией, пользовательское офисное ПО. Третье направление импортозамещения предполагает государственную поддержку отечественных производителей

**К 1 ИЮНЯ МИНКОМСВЯЗЬ РАЗРАБОТАЕТ ПРОЕКТ СОЗДАНИЯ АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ, КОТОРАЯ ЗАЙМЕТСЯ РАЗРАБОТКОЙ СОФТА ДЛЯ ИМПОРТОЗАВИСИМЫХ СЕГМЕНТОВ ЭКОНОМИКИ. СОГЛАСНО ПЛАНУ, ТАКОЕ ПО ДОЛЖНО БЫТЬ РАЗРАБОТАНО ДО 2025 ГОДА ВКЛЮЧИТЕЛЬНО**



## ОТЕЧЕСТВЕННЫЙ ПРОДУКТ



### СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПО — ЕДИНСТВЕННЫЙ РЕАЛЬНЫЙ ПУТЬ К ПОЛНОЦЕННОМУ ИМПОРТОЗАМЕЩЕНИЮ

лей в сегментах рынка ПО для разных отраслей. Помимо этого к 1 июня Минкомсвязь разработает проект создания автономной некоммерческой организации, которая займется разработкой софта для импортозависимых сегментов экономики. Согласно плану, такое ПО должно быть разработано до 2025 года включительно.

Одной из основных задач Минкомсвязи в рамках программы импортозамещения является переход на свободно распространяемые системы управления базами данных. «Проприетарное импортозависимое программное обеспечение сегодня присутствует в органах государственной власти и государственных компаниях. Ежегодно на его закупку и поддержку тратятся сотни миллионов рублей. Кроме того, что оно дорого обходится государству, оно является и уязвимым с точки зрения возможных санкций, когда ущемляются права и свободы пользователей, — отмечал ранее министр связи и массовых коммуникаций Николай Никифоров. — В текущей геополитической обстановке не-

обходимо развивать и поддерживать любые виды свободного программного обеспечения, способные привести к демополизации рынка разработки ПО, что особенно актуально для такой важнейшей сферы, как базы данных». По словам главы Минкомсвязи России, необходимо достичь баланса, при котором доля каждого разработчика ПО на международном рынке не будет превышать 50%.

Одной из основных проблем в сфере импортозамещения, по мнению генерального директора ОПК Александра Якунина, сегодня является отсутствие единой политики. «Это ведет к такому негативному явлению, как псевдоимпортозамещение. Не располагая собственными компетенциями, экспертизой и производственно-технической базой в области создания и производства сложного оборудования, некоторые компании выдают продукты зарубежных производителей за свои — без трансфера технологий и реальной локализации производства на территории РФ. В результате государственные деньги, выделяемые на инфраструктурные информационно-телекоммуникационные проекты, фактически уходят зарубежным производителям. Создание единого центра компетенций в рамках госкорпо-

рации «Ростех» позволит проводить системные преобразования в данной области. Эта мера должна кардинально изменить ситуацию в пользу российской промышленности», — рассказал Александр Якунин на заседании правления государственного предприятия «Ростех».

По мнению экспертов «Ростеха», основными принципами создания российского оборудования должны стать независимость жизненного цикла изделия от конкретных зарубежных производителей и внешних угроз, возможность «быстрого» перехода на другую элементную базу, локализации производства на других площадках, обеспечение технической поддержки обслуживания.

Корпорация намерена делать акцент на «интеллектуальной» составляющей разработок: отечественной схемотехнике, использовании отечественной электронной компонентной базы и отечественном ПО.

**ОТКРЫТАЯ ОБОРОНА** Ключевым компонентом информационных систем являются системы управления базами данных. От их технических характеристик напрямую зависят защищенность и функциональные возмож-



ности информационных систем. От современных СУБД требуются богатый базовый функционал, отказоустойчивость и высокая производительность.

Большинство современных успешных компаний, таких как «Яндекс», Google, Facebook, RedHat, IBM, Sony и Apple, активно используют свободное программное обеспечение и даже строят на его основе свои коммерческие продукты. Компания EnterpriseDB, например, на основе открытой СУБД разрабатывает коммерческую СУБД PostgreSQL Plus Advanced Server, которая в настоящее время занимает 10% рынка систем управления базами данных в США.

По этому же пути можно пойти и при разработке СУБД для автоматизированных систем специального назначения. Можно максимально использовать результаты работы глобального сообщества разработчиков и сохранить контроль над своими стратегическими разработками.

При выборе проекта с открытым исходным кодом необходимо обращать особое внимание на вид лицензии, его базовую функциональность, зрелость и возможность влияния на процесс разработки. Наличие отечественных специалистов, признанных сообществом и обладающих необходимым авторитетом, может позволить форсировать развитие базового продукта в необходимом направлении.

Проведя глубокий сравнительный анализ различных СУБД, специалисты АО «Концерн „Радиоэлектронные технологии“» (КРЭТ) остановили свой выбор на PostgreSQL. Она обладает свободной лицензией BSD, которая не требует раскрытия исходного кода и позволяет создавать коммерческие продукты.

На базе СУБД PostgreSQL планируется независимо разрабатывать лишь средства защиты информации, а остальной функционал реализовывать в тесном контакте с международным сообществом.

В последние годы СУБД PostgreSQL активно развивается, что дает много новых возможностей для эффектив-

ной, безопасной и надежной обработки данных. Вместе с полноценными средствами кластеризации они позволяют строить территориально распределенные сети центров обработки данных (ЦОД). При этом каждый ЦОД может независимо обслуживать запросы на чтение и запись от клиентов из различных регионов. Параллельно все региональные ЦОДы синхронизируются друг с другом (почти в реальном времени), и при выходе из строя одного или нескольких из них оставшиеся могут перераспределить между собой нагрузку.

Представители отрасли считают, что целесообразно идти по пути внедрения открытых программных продуктов и активно интегрировать российское сообщество программистов в процесс их разработки. При этом можно получить дополнительные выгоды от того, что глобальное сообщество возьмет на себя тестирование и сопровождение отечественных наработок, включаемых в открытый продукт.

«Чтобы получить максимальную выгоду от использования такого подхода, необходимо создавать центры компетенции и развивать систему подготовки специалистов по разработке и внедрению открытого программного обеспечения, поиску и устранению уязвимостей, адаптации средств защиты информации к требованиям российских регуляторов и их сертификации. Кроме наличия специалистов необходимо гарантировать постоянную доступность исходных кодов, которые в основном находятся за пределами России. Поэтому на случай потенциального нарушения связности Сети по политическим или техническим причинам необходимо создавать независимую отечественную инфраструктуру, которая позволит организовать самостоятельную разработку и сопровождение открытых программных продуктов», — считают эксперты КРЭТ.

Минсвязи поддерживает эту позицию. «Что касается критических видов ПО, нужно идти по пути коллективной разработки ПО совместно с другими странами, в первую

очередь странами БРИКС. Таких примеров в мире достаточно много. Можно создать отдельные некоммерческие организации (НКО) по каждому виду критического ПО, и мы готовы рассмотреть варианты государственного финансирования деятельности таких НКО, если эти субсидии будут идти на зарплаты разработчиков. В других отраслях, например в автопроме, ОПК, сельском хозяйстве, индустрии очень быстро формируют конкретные планы действий и объемы финансирования по импортозамещению. ИТ-индустрия всегда развивалась независимо, без государственной подпитки, но сегодня без поддержки государства невозможно совершить прорыв в тех видах ПО, которые не смогут быть созданы на качественном уровне только путем поддержки через госзаказ», — сказал министр связи и массовых коммуникаций Николай Никифоров на годовой расширенной коллегии Минкомсвязи.

Алексей Бадаев, вице-президент по продажам и развитию бизнеса Acronis в России, странах СНГ и Восточной Европы, также считает, что перспективы использования свободного ПО для программных решений для ОПК и стратегически важных отраслей весьма позитивные. «Разумеется, не во всех — тем более сложных, стратегических — индустриях переход может состояться быстро, тем более что не все западные продукты пока можно заменить российскими аналогами, — уточняет господин Бадаев. — Но если мы ставим задачу обеспечить независимость стратегических предприятий страны, то переход на отечественные open source-разработки — это, безусловно, путь».

По его словам, на практике все зависит от потребностей предприятия, задач организации, профессионального уровня разработчиков, которые будут искать конкретные решения. «И очень важно все это понимать, потому что неудачные случаи внедрения тоже есть — могу вспомнить, например, правительство Баварии, где переход на свободное ПО не удался, — комментирует Алексей Бада-

ев. — Отдельно хочу сказать, что сегодня в стране есть российские компании, которые могут заменить зарубежные и успешно с ними конкурировать. При этом им совершенно точно еще есть куда стремиться. Сейчас российские разработчики по большей части берут передовые мировые разработки и качественно переупаковывают их. Это тоже неплохой уровень, но чтобы конкурировать с лучшими глобальными компаниями и получать в качестве клиентов крупных российских клиентов, придется быть более инновационными».

ОПК, входящая в госкорпорацию «Ростех», рапортует, что готова провести стопроцентное импортозамещение в корпоративном сегменте, но в этом начинании необходима господдержка для фиксации рынка госзакупок для отечественных решений. «Для телекоммуникационного оборудования, производимого на территории Казахстана, например, при участии в тендерах на поставку оборудования, закреплено преимущественное право в размере 20% от котировочной стоимости. Законодательно закреплена возможность заключения долгосрочного меморандума на бестендерной основе на поставку телекоммуникационного оборудования, произведенного на территории Казахстана, — отметил Александр Якунин. — В России же законодательно отсутствует понятие отечественного производителя. При участии в тендерах на поставку оборудования отсутствует любое преимущественное право для телекоммуникационного оборудования, разработанного и произведенного на территории России. Для успешной реализации импортозамещения необходима фиксация рынка через ФЗ-223 и ФЗ-44, а также налоговый барьер для ввозимой готовой радиоэлектронной продукции». Так что если и говорить о препятствиях на пути импортозамещения, то кроются они не в отсутствии и не в уровне качества решений, которые способны выдавать российские разработчики, а в том, как этот процесс поддерживается на законодательном уровне. ■

## «БЛАГОДАря ГОСЗАКАЗУ ОТЕЧЕСТВЕННЫЕ ПРОДУКТЫ СТАНУТ БОЛЕЕ КОНКУРЕНТОСПОСОБНЫМИ»

**Руководитель департамента информации, коммуникации и аналитики «Ростеха» ВАСИЛИЙ БРОВКО рассказал корреспонденту ВГ МАРИИ АНАСТАСЬЕВОЙ о том, какую роль играет госкорпорация в импортозамещении, а также почему именно в Татарстане появится российская ИТ-столица.**



**BUSINESS GUIDE:** Какие задачи стоят перед госкорпорацией «Ростех» в области повышения эффективности управления предприятиями холдинга? Над какими задачами в этой области вы работаете в настоящий момент?

**ВАСИЛИЙ БРОВКО:** В целом в этом отношении есть три про-

блемы. Во-первых, у промышленности нет единой стратегии в том, что касается ИТ. Не выбраны приоритетные решения, нет вертикально интегрированной системы управления ИТ, нет единой платформы. Во-вторых, при ИТ-закупках нет достаточной прозрачности, а это, в частности, препятствует снижению издержек. Но самое главное, у нас отсутствуют российский софт и российское «железо». Это очень сильно ограничивает возможность обеспечения безопасности при работе с секретной и совершенно секретной информацией, каковой в оборонно-промышленном комплексе много.

Необходимость решить все эти проблемы и определяется роль «Ростеха», она определяющая и понятная. Во-первых, нужно проводить единую техполитику в части, касающейся ИТ. Во-вторых, нужно сделать закупки прозрачными. Прозрачные закупки через одно окно позволяют получать максимальные скидки, обеспечить оптимизацию, благодаря чему появится возможность реинвестировать в новые продукты и технологии в сфере ИТ на предприятиях. В-третьих, пора, разумеется, создавать свое «железо» и софт.

**BG:** Какова роль компании «РТ-Информ» в составе госкорпорации «Ростех»? Как вы оцениваете ее потенциал? Выполняет ли она проекты исключительно для компаний, входящих в госкорпорацию, или миссия этой структуры более широкая?

**В. Б.:** Здесь нужно говорить в целом о центрах компетенции госкорпорации. В том, что касается ИТ, их три. «РТ-Информ» — это интегратор «Ростеха», его задача — организовывать все ИТ-закупки корпорации, быть поставщиком софта и «железа» на предприятия. Он обеляет рынок, унифицирует закупки, проводит единую техполитику, создает платформу для того, чтобы через два, три, четыре года, когда подоспеют российские продукты, было куда их интегрировать, была общая архитектура информационной системы.

Кроме того, в составе «Ростеха» есть Национальный центр информатизации (НЦИ), это СП «Ростеха» и «Ростелекома». Компания должна разрабатывать софт и различные системы не только для оборонно-промышленного комплекса, но и для госсектора в целом. Благодаря госзаказу отечественные продукты станут более конкурентоспособными, поскольку появятся средства на развитие производства. Будет возможность разрабатывать продукты не только для гражданской сферы, но и для военной.

Раньше было принято говорить, что новые технологии рождаются в военной области и потом идут в гражданскую. Однако сегодня гражданский рынок очень велик, на НИОКР направляются большие объемы инвестиций, частный производитель использует лучший опыт, накопленный в мире, он сегодня доступен в условиях информационного общества. Поскольку гражданский рынок намного шире, то выше и тиражирование: это тысячи и миллионы копий. А в военной сфере нужны сложные, но штучные продукты. Поэтому базовый заказ, разработка софта и платформ для гражданских нужд,

пусть и государственных (а это все равно рынок с большим количеством других игроков, где нужно быть конкурентоспособным, побеждать, доказывать), позволит сформировать команды, способные разрабатывать продукты для оборонно-промышленного комплекса. То есть НЦИ будет концентрироваться на продуктах для коммерческого рынка с возможностью в отдаленной перспективе на этих решениях разрабатывать, возможно, продукты для оборонно-промышленного комплекса.

Наконец, операционные системы, язык базы данных. В «Ростех» входит Объединенная приборостроительная корпорация (ОПК), которая разрабатывает свою операционную систему и уже близка к достижению результата, формирует архитектуру собственного чипа, создание которого позволит значительно продвинуться в вопросах национальной безопасности. Ведь сегодня мы не имеем ни операционной системы, ни «железа», ни чипа. Иностранные продукты все равно имеют «закладки», «черные двери» и так далее.

ОПК сегодня разрабатывает «железо». Она определена «Ростехом» в качестве центра компетенции по программе импортозамещения в области железа ИТ. Они будут отвечать за то, что разрабатывать, как разрабатывать. У ОПК накоплен большой опыт, есть несколько легендарных институтов, сотрудники которых после развала Советского Союза оказались востребованы в Intel и внесли большой вклад в развитие этой компании. При этом в самих институтах остались кадры, в ОПК идет молодежь. Уже начался прием заказов на компьютеры на базе отечественного микропроцессора «Эльбрус-4С». Таким образом, каждая компания — «РТ-Информ», НЦИ и ОПК — занимается в своей области решением общей задачи.

Кроме того, в «Ростех» входит компания Yota Devices, которая производит пер-

вый российский смартфон, а также «Росэлектроника», специализирующаяся на микроэлектронике и компонентах.

**BG:** «Ростех» планировал перейти на централизованную закупку ИТ-оборудования и ПО для своих предприятий. Речь идет об унификации ИТ-решений на предприятиях? В какой степени предприятия могут влиять на выбор решений?

**В. Б.:** «Ростех» действительно переходит на централизованную систему закупок. Это большая работа, которая требует времени.

Предприятия при выборе решений будут ограничены единой техполитикой. Это необходимо для того, чтобы системы не конфликтовали друг с другом. Корпорация не может зависеть от сотен разных решений, которые принимаются на отдельных предприятиях. Если предприятию требуется закупить что-то не входящее в единый перечень, то вопрос будет выноситься на отдельное решение с дополнительным обоснованием. Возможны исключения, однако важно, чтобы существовала единая интегрированная система. Потому что если нет единой платформы, то не будут работать приложения, ERP-система, информационно-аналитическая система, система электронного документооборота, система управления жизненным циклом продукта и многие другие. Необходима унификация в смысле единой платформы при сохранении индивидуального подхода к потребностям предприятий, насколько это возможно в рамках такой большой корпорации.

**BG:** Что вы думаете о перспективах импортозамещения на предприятиях холдинга, в частности в сфере ИТ? Что для этого делает и еще может сделать «Ростех»?

**В. Б.:** Импортозамещение — это процесс, который включает в себя несколько составляющих. Первая и, наверное, самая важная составляющая — это определение ключевых точек, где необходимо замещение импортируемых технологий. Полное импортозаме-

щение никому не нужно, это утопия, такого никто не планирует. Однако есть ключевые вещи, без которых обеспечение безопасности при общей технологической модернизации невозможно. Где-то в импортозамещении мы продвинулись чуть дальше, где-то — чуть меньше. В любом случае «Ростех» сегодня лидер в области ИТ. У нас сосредоточены компетенции, институты, специалисты, производственные площадки, а также большое количество предприятий, которые фактически формируют внутренний рынок, он может стать триггером роста закупки современных российских решений. При этом «Ростех» работает с партнерами, привлекает молодые стартапы, молодых разработчиков, создает условия и среду для этой работы.

**BG:** Каково для «Ростеха» значение сотрудничества с правительством Республики Татарстан? Можно ли полученный опыт перенести в другие регионы, есть ли такие планы?

**В. Б.:** Татарстан, безусловно, один из лидеров в области ИТ в нашей стране наряду с Москвой, Санкт-Петербургом. В республике уделяется большое внимание этой работе. Тот факт, что конференция «Информационные технологии на службе оборонно-промышленного комплекса» проходит в Татарстане, определяется тем, что Иннополис в ближайшее время станет ИТ-столицей нашей страны, где сосредоточатся лучшие умы и будут вырабатываться ключевые технологии. Мы тесно сотрудничаем с коллегами в этом направлении, в Иннополисе будет локализована соответствующая компетенция «Ростеха», там разместятся структуры госкорпорации, специализирующиеся на разработке и внедрении ИТ-решений. Будут собраны научные кадры «Ростеха» для создания прорывных продуктов.

Этот проект интересен, поскольку предполагает создание целого города, удобного для жизни и работы ИТ-специалистов и разработчиков. Туда, возможно, захотят вернуться специалисты из-за границы.

# ВОЙНА ИДЕТ ПО ПРОВОДАМ

В XXI ВЕКЕ ВОЕННЫЕ ДЕЙСТВИЯ ЛИШЬ ОТЧАСТИ ПРОИСХОДЯТ В ФИЗИЧЕСКОМ МИРЕ — БОЛЬШИНСТВО ОПЕРАЦИЙ ПРОВОДИТСЯ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ. ЕСТЬ ПРОГНОЗЫ О ТОМ, ЧТО УЖЕ В БЛИЖАЙШИЕ ГОДЫ ВОЙНА КАК ЯВЛЕНИЕ ПОЛНОСТЬЮ ПЕРЕМЕСТИТСЯ В СФЕРУ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ОКОНЧАТЕЛЬНО ПРИОБРЕТЕТ ВИД КИБЕРВОЙНЫ.

СВЕТЛАНА РАГИМОВА

Беспилотные автомобили и самолеты, интернет вещей, «умная» инфраструктура, подключенные ЛЭП, канализации и водоснабжение, светофоры и холодильники. Звучит как рассказ о прекрасном светлом будущем. Но не стоит смотреть на эти явления сквозь розовые очки. На одной из конференций Иван Новиков, основатель компании Wallarm, защищающей веб-ресурсы от хакерских атак, прямо во время своего выступления взломал чайник, демонстрируя, что уязвимым может стать любой предмет — достаточно лишь подключить его к интернету. Вместо нагревательного прибора бытового назначения «плохие парни» так же легко могут добраться и до оборудования электростанции, использующей технологии Smart Grids. А если удастся взломать атомный генератор или атаковать системы управления нефтяными вышками, то и ядерного оружия не надо.

Три года назад в Иране и на Ближнем Востоке эксперты «Лаборатории Касперского» обнаружили признаки кибервойны, проанализировав код вируса Flame. Этот червь был создан для кибершпионажа, и, как сообщили представители компании, над ним поработала группа профессионалов, создавшая один из самых совершенных на тот момент образцов кибероружия. Flame удалял конфиденциальные данные с компьютеров, расположенных в целевых странах, анализировал сетевой трафик, делал скриншоты, записывал разговоры, перехватывал нажатия на клавиатуре и т. д. Все эти сведения вирус передавал операторам через командные серверы. При необходимости Flame могла запустить один или несколько из двух десятков специальных модулей разного назначения. Предшественник этого червя, атаковавший компьютеры Израиля и США в 2010 году, содержал гораздо менее изощренный программный код.

Гонка вооружений в киберпространстве началась и развивается не менее быстро, чем «мирные» технологии. Первый образец кибероружия в истории человечества — червь Stuxnet, появился всего пять лет назад и смог отключить 900 центрифуг иранского завода по обогащению урана. Хосе Игнасио Торребланка, глава мадридского офиса Совета Европы по иностранным делам, профессор политических наук Национального университета дистанционного образования Мадрида, объясняет, что сегодня гораздо легче атаковать нефтяные вышки страны цифровым путем, чем физическим. «Сегодня цифровые уязвимости быстро становятся главной заботой правительства и бизнеса. По последним оценкам, только 11% компаний нефтяной отрасли сообщают, что чувствуют себя защищенными от подобных атак, и, что еще хуже, 23% признаются в том, что не используют в своих сетях средства мониторинга для обнаружения попыток нападений», — говорит Хосе Торребланка.

Финское правительство в 2013 году обнаружило шпионскую программу неизвестного происхождения, которая в течение многих лет работала на компьютерах чиновников. В США в ноябре прошлого года вирус, чье авторство приписали Китаю, заразил метеорологические спутники, чтобы обнаружить уязвимости в сети, обслуживающей систему глобального позиционирования GPS, играющую существенную роль в обороноспособности страны. Простая USB-флешка может быть более вредоносной, чем



ПЕРВЫЙ ОБРАЗЕЦ КИБЕРОРУЖИЯ В ИСТОРИИ ЧЕЛОВЕЧЕСТВА — ЧЕРВЬ STUXNET, ПОЯВИЛСЯ ВСЕГО ПЯТЬ ЛЕТ НАЗАД

бомба с лазерным наведением; нефтяной поток можно прервать с помощью компьютера; военные спутники можно просто отключить вместо того, чтобы разрушать их. Очевидно, мы являемся свидетелями революции в военном деле. XX век был веком физики, и в это время велись физические войны, XXI век — цифровой, и можно ожидать, что войны также будут цифровыми. И здесь большой вопрос — физическая смерть противника также будет считаться чем-то устаревшим или все еще останется необходимым условием для победы.

**ФИСТАШКОВЫЙ ЗАПАХ** Как правило, проследить стартовую точку, с которой началось распространение вируса, подобного Flame или тому, что действовал в финском правительстве, почти невозможно. Как и доказать, что программу разработали кибервойска какой-либо страны. Составителям отчета о растущей киберугрозе со стороны Ирана под названием «Урожай фисташек» (Pistachio Harvest Project) это удалось. Результаты совместного исследования, проведенного Norse Corporation и командой Critical Threats Project из American Enterprise Institute, были опубликованы в апреле. Исследователи со-

бирали данные о действиях киберармии Ирана, распортив по всему миру несколько миллионов «сенсоров» — фальшивых веб-сайтов с уязвимостями, которые «прикидываются» обычными сайтами банков, университетов, заводов, электростанций и прочих объектов, которые могут быть интересны хакерам. В результате анализа собранных данных выяснилось, что злоумышленники пытаются обнаружить и взять под контроль слабозащищенные системы SCADA (автоматизированные системы диспетчерского управления и сбора данных) — например, те, что обслуживают электроэнергетическую инфраструктуру. При этом зловредное ПО искало уязвимости и, по мнению исследователей, отправляло информацию о них в специальную базу данных.

Кибервойска и группы, разрабатывающие кибервооружение, создаются в рамках специальных программ в США и в других западных странах. Кибероборона в соответствии с подходом, которому следует НАТО, это возможность использования информационных сетей для того, чтобы парализовать органы управления и систему обороны той или иной страны, а после этой информационной атаки уже приступить непосредственно к военному воздействию.

Уже в 2010 году США создали собственное кибернетическое командование. Американские власти уверяют,

что оно занимается исключительно обороной сетей. В том же году, как было установлено экспертами, спецслужбы США провели атаки на иранские ядерные объекты, чтобы вывести их из строя.

Как следует из новых рассекреченных Эдвардом Сноуденом материалов, опубликованных изданием Der Spiegel, США готовятся к кибервойнам за господство в интернете. Доказательством этому являются документы о находившемся в ведении американских спецслужб проекте Politerain. В рамках данного проекта осуществлялся набор и обучение специалистов, способных путем внедрения вредоносного ПО выводить из строя компьютерные системы, контролирующие работу объектов инфраструктуры и телекоммуникации потенциального противника, а также перехватывать его денежные транзакции. Сверхзадачей проекта было воспитать у будущих сотрудников спецслужбы «мышление атакующего».

Глобальная слежка в интернете, которую осуществляет Агентство национальной безопасности США (АНБ), — это лишь часть существующей американской киберстратегии. С военной точки зрения это «Фаза 0» в стратегии кибервойны, к которой готовятся США. Как следует из рассекреченных документов АНБ, цель этой слежки — нащупать слабые звенья в системах противника. Внедрение шпионского ПО (киберагентурная сеть) и получение



постоянного доступа к этим системам означает наступление «Фазы 3», ключевым словом в характеристике которой является доминирование. Как сказано в документах Эдварда Сноудена, в этой фазе предусмотрен целенаправленный контроль/уничтожение критически важных систем и сетей посредством ранее обеспеченного в «Фазе 0» доступа. Критически важными для АНБ являются инфраструктуры, обеспечивающие функционирование общества: энергетическая, телекоммуникационная, транспортная и финансовая.

В одной из подготовленных АНБ презентаций НАТО утверждается, что следующий крупный международный конфликт начнется в киберпространстве. Ориентируясь на эти перспективы, правительство США наращивает мощь военных киберподразделений. В бюджете спецслужб на 2013 год для АНБ на проведение спецопераций в интернете предусматривался \$1 млрд, а на финансирование так называемых «нестандартных решений» — \$32 млн дополнительно.

Как сообщает Washington Post, Соединенные Штаты направляют все возможные усилия на разработку нового поколения кибероружия, которое будет способно нарушать корректную работу компьютерных систем противников, даже если они не подключены к интернету. В 2011 году на ускорение темпов разработки кибероружия и оборонных технологий ведущему научно-исследовательскому агентству Пентагона DARPA (Defense Advanced Research Projects Agency) было выделено \$500 млн на пять лет. Агентство DARPA объявило о новых инициативах в области развития кибероружия, в том числе об «ускоренной» программе. «Наши кибердействия должны быть быстрыми и масштабными», — заявляют представители DARPA.

В Пентагоне отмечают, что кибероружие должно соответствовать темпам развития информационных технологий и угроз. Чиновники планируют разрабатывать технологии, которые используют радиосигналы для встраивания кодов в компьютерные системы удаленно. Стоит отметить, что DARPA намерено нацелить большую часть исследований на решение именно таких военно-специфических вопросов.

«Госструктуры США, включая АНБ, посредством разного рода государственных программ тесно сотрудничают с крупнейшими национальными и транснациональными компаниями — производителями микрoeлектроники и программного обеспечения», — рассказывает Игорь Жуков, заместитель генерального директора по защищен-

ным радиоэлектронным информационным технологиям концерна «Радиоэлектронные технологии» (входит в госкорпорацию «Ростех»). — Суть данного сотрудничества состоит в предоставлении спецслужбам США несанкционированного доступа к информации, обрабатываемой на аппаратных и программных платформах. То есть в свои продукты производители внедряют специальные возможности, так называемые back doors, или закладки, которые позволяют получать доступ к информации в обход встроенных механизмов защиты (например, программа Bullrun)». По словам эксперта, в свою очередь, государственные структуры США оказывают поддержку продвижению на мировых рынках продукции вступивших в «программу» компаний. «В частности, в СМИ неоднократно проходила информация о поставках США ряду государств различного и криптографического оборудования в кредит на льготных условиях либо вообще бесплатно. Также проходила информация об акциях активного продвижения такого оборудования, осуществляемого непосредственно сотрудниками Госдепартамента и МО США», — добавляет Игорь Жуков.

**МЯГКИЙ ЦИТ** В новой военной доктрине, утвержденной президентом РФ в конце декабря 2014 года, среди основных внешних военных опасностей также отмечается массированное использование информационных и коммуникационных технологий в военно-политических целях. Поэтому новая госпрограмма вооружений ставит своей целью создание эффективных информационно-управляющих систем BBCT, защищенных от возможных кибератак.

В феврале 2015 года главой Минобороны России была подписана «Концепция развития информационных и телекоммуникационных технологий вооруженных сил на период до 2020 года». В концепции также содержатся ответы на изменения в военной науке в сфере развитых информационных технологий и информационного управления. В марте было принято решение о создании Совета по кибербезопасности. На совещании по вопросам информационной безопасности в марте в МГУ им. М. В. Ломоносова вице-премьер Дмитрий Rogozin заявил, что в России появится своя собственная система противодействия киберугрозам. Она будет основана на применении «умного» оружия, которое производится «с помощью сложнейших производственных линий и технологических цепей». Сейчас формируется «новая программа вооружений с использованием такого умного оружия».

В указанных документах и заявлениях руководителей страны отмечаются как источники информационных угроз (сильная в отношении возможных кибератак страна, страна, равная по силе, слабый противник в виде организованной преступной или террористической группы), так и особенности современных военных и иных конфликтов противостоящих сторон, где составляющая информационных воздействий играет не последнюю роль.

Особенно сильно эта роль проявляется в ходе проведения новой стратегии «нелинейного ведения войны» в виде гибридной или «мягкой» войны. В ее арсенале присутствуют информационная война или информационные воздействия, как правило предшествующие военной операции или идущие параллельно и включающие информационно-психологическую (дезинформация, пропаганда, использование протестного потенциала населения противника и др.), а также информационно-техническую составляющую (кибератаки и др.) на основные управляющие и организационно-технические системы противника. Такого же определения гибридной войны придерживается и руководство НАТО, которое в этом качестве подразумевает подход, сочетающий «конвенциональные военные действия» и новые сложные кампании по «пропаганде и дезинформации».

«Понятно, что все эти формы ведения гибридной войны начинают использоваться одной из сторон зарождающегося и идущего конфликта тогда, когда нецелесообразно и невыгодно масштабное силовое противостояние со всеми вытекающими последствиями. Уже сейчас началось массовое применение кибератак на другое государство в ряде стран НАТО может рассматриваться как повод для применения статьи о коллективной обороне», — поясняет Игорь Жуков.

**ПОДНЕБЕСНЫЕ ЦЕЛИ** Международные эксперты называют российские киберинструменты и методы более умелыми, а китайские — более масштабными. Впрочем, руководство Китая всегда отвергает причастность к любым инцидентам, связанным с нападениями на западные страны, в первую очередь на США. При этом косвенное доказательство причастности Китая к ведению кибервойн обнаружилось в официальном отчете Народно-освободительной армии Китая (НОАК). О том, что Китай признает существование кибервойск в составе своей армии, говорится в тексте публикации «Наука военной стратегии» (The Science of Military Strategy). Документ готовился ведущими иссле-

довательскими институтами совместно с НОАК и содержит детальный анализ военной стратегии Поднебесной. Согласно отчету, в Китае действует три вида кибервойск.

Первый — это военные специалисты в сфере сетевой безопасности. Они действуют по военным принципам. Их задача — организация кибератак и защита от них. Второй — специальные группы, действующие внутри спецслужб, таких как Министерство государственной безопасности и Министерство общественной безопасности. Третий вид — группы независимых хакеров, которых можно быстро мобилизовать для совершения информационных операций.

Специалисты отмечают, что, по всей видимости, все три группы работают в тесном контакте и подчиняются руководству НОАК. Кроме того, в последнем издании энциклопедии «Наука военной стратегии», выпущенном НОАК на родном языке и представляющем собой «лучшее пособие по китайской военной машине», сообщают The Daily Beast, также говорится о том, что в Китае существуют кибервойска, в задачи которых входит не только защита, но и нападение на сети иностранных государств. В последнем издании военной энциклопедии Китая прямо сказано о наличии у государства специальных хакерских группировок. Вооруженные силы Китая располагают специальными подразделениями, осуществляющими кибератаки на вычислительные сети иностранных государств. Согласно энциклопедии, в Китае существуют два подразделения с хакерами. Одно — при вооруженных силах, второе — при разведывательных службах. Кроме того, существуют некие неправительственные «внешние группировки». Они могут быть организованы и мобилизованы по необходимости, приводит выдержки из энциклопедии The Daily Beast.

Впрочем, пока для России Китай больше партнер, чем угроза. 9 мая правительства стран подписали пакт о ненападении друг на друга в киберпространстве. Международные эксперты назвали соглашение уникальным. Также РФ и Поднебесная договорились обмениваться данными о киберугрозах и технологиями.

Прошло лишь пять лет с момента появления первой «кибербоеголовки», за это время правительства разных стран обзавелись кибервойсками и признали, что «мягкая» война уже идет полным ходом, пока мы читаем эту статью на сайте, изучаем ленту в Facebook и играем в «Злых птиц» на iPhone. О таких битвах сложно рассказывать живописно и невозможно снять шокирующий фоторепортаж, но их последствия могут оказаться еще более разрушительными, чем взрыв ядерной бомбы. ■

## «ГИСП — ЭТО ПРЕЖДЕ ВСЕГО ИСТОЧНИК ДАННЫХ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ КАК ПРАВИТЕЛЬСТВОМ РФ, ТАК И СУБЪЕКТАМИ ПРОМЫШЛЕННОСТИ»

**Министерство промышленности и торговли РФ начало реализацию глобального проекта по созданию Государственной информационной системы российской промышленности (ГИСП). О ходе решения этой задачи „Ъ“ рассказал первый заместитель министра промышленности и торговли России ГЛЕБ НИКИТИН.**



**BUSINESS GUIDE:** Насколько, на ваш взгляд, важна роль государства в поддержке развития ИТ-технологий в индустриальном секторе?

**ГЛЕБ НИКИТИН:** Не открою большого секрета, сказав, что за ИТ-технологиями будущее современной промышленности, поэтому Минпромторгом

уделяется повышенное внимание вопросам информатизации. Например, в рамках программы создания и поддержки инжиниринговых центров мы разработали механизм по возмещению части затрат на приобретение специализированного программного обеспечения. В 2014 году благодаря этим мерам поддержки компании малого и среднего бизнеса, осуществляющие деятельность в сфере инжиниринга и промышленного дизайна, имели возможность приобретать необходимое ПО со скидкой до 75%. Общий размер предоставленной скидки на ПО составил 140 млн руб.

**ВГ:** Насколько сегодня актуальна задача по импортозамещению в области программных продуктов для российского индустриального сектора?

**Г. Н.:** Импортозамещение в сфере ИТ-технологий мы считаем крайне важной задачей, особенно в условиях введения Западом антироссийских санкций. Здесь на первый план выходит уже не столько экономическая выгода, сколько вопросы безопасности. К сожалению, в настоящее время доля российских разработок в ИТ-области невелика. Мы понимаем, что переход на отечественные разработки — процесс длительный, сложный и требующий больших инвестиций, но со временем мы ожидаем прогресса в этом направлении. Например, в план мероприятий по импортозамещению мы включили продукцию радиоэлектронной промышленности, куда входят в том числе вычислительная техника, телекоммуникационное оборудование, периферийное оборудование, электронная компонентная база и прочее. Мы ожидаем, что развитие электроники поможет стимулировать развитие собственных ИТ-технологий.

**ВГ:** Для чего создается Государственная информационная система российской промышленности?

**Г. Н.:** Мы рассматриваем ГИСП прежде всего как источник данных для принятия решений как для правительства РФ, так и для самих субъектов промышленности.

Это новый инструмент промышленной политики. Единый центр по сбору данных и их диагностике в сфере промышленности позволит нам сформировать полную информационную картину планов и потребностей российских промышленных предприятий, даст разбивку по регионам, исключит дублирование запросов и межотраслевой дисбаланс. По сути, ГИСП представляет собой единое окно, включающее в себя весь массив нормативно-правовых актов в сфере промышленности, горячую линию поддержки, открытый каталог потенциальных промышленных площадок и т. д. Система предусматривает исключительно электронный сбор информации.

**ВГ:** В каком виде предстанет ГИСП для конечного пользователя?

**Г. Н.:** Это будет интернет-портал, через который конечные пользователи смогут воспользоваться необходимыми сервисами, зарегистрировав свой личный кабинет. Внутреннее ядро будет включать в себя технологическую платформу и необходимую инфраструктуру для сбора, обработки и хранения данных.

**ВГ:** С какими данными пользователи смогут работать через ГИСП?

**Г. Н.:** ГИСП позволит пользователям получить сведения о состоянии промышленности и прогнозе ее развития, о субъектах деятельности в сфере промышленности, о прогнозах выпуска основных видов промышленной продукции и об их фактиче-

ском выпуске, об объемах импорта промышленной продукции в Россию, а также данные об использовании ресурсосберегающих технологий и возобновляемых источников энергии. Кроме того, сюда будет поступать информация о государственных и муниципальных промышленных программах, о мерах стимулирования промышленности, о показателях эффективности этих мер и о кадровом потенциале. И, наконец, в ГИСП будут выгружаться ежегодные доклады о состоянии и развитии промышленности.

**ВГ:** Чем руководствовался Минпромторг, включая этот проект в свой план работы?

**Г. Н.:** Задача по созданию ГИСП появилась при разработке нами законопроекта «О промышленной политике». Сам закон был принят 31 декабря 2014 года и вступает в силу 1 июля 2015 года. Правительство РФ обязало наше министерство разработать и утвердить требования к ГИСП и наделило нас полномочиями обладателя информации, содержащейся в данной системе.

**ВГ:** Как будет наполняться ГИСП, каковы источники информации?

**Г. Н.:** Для наполнения системы данными промышленные предприятия, органы государственной власти, местного самоуправления и другие субъекты деятельности в сфере промышленности должны будут обеспечить Минпромторгу доступ к своим базам данных посредством единой

системы межведомственного электронного взаимодействия. Часть данных, размещенных в ГИСП, будет открыта и опубликована в интернете в разделе «Открытые данные» официального сайта нашего министерства.

**ВГ:** Каким образом посредством ГИСП предполагается выстраивание системы отраслевых балансов в промышленности?

**Г. Н.:** Действительно, до сих пор остается актуальной проблема отсутствия межотраслевых балансов в стране, что зачастую приводит к созданию искусственных профицитов промышленных мощностей в разных регионах. В настоящее время данные, необходимые для анализа и принятия решений, разрознены и к ним не всегда имеется доступ. Предполагается, что в единой системе они будут аккумулированы и это позволит снять проблему.

**ВГ:** На каком этапе сегодня находится реализация этого проекта, какова его предварительная стоимость?

**Г. Н.:** На данном этапе реализации этой задачи уже завершено общественное обсуждение проекта соответствующего постановления правительства РФ, и сейчас документ проходит этап антикоррупционной экспертизы. Начало работы ГИСП можно ожидать уже в 2016 году. По предварительным расчетам, на реализацию первого этапа потребуется около 47 млн руб., в ноябре 2015 года будет объявлен конкурс.

Интервью взяла МАРИЯ АНАСТАСЬЕВА

# «МЫ НЕ ЗАНИМАЕМСЯ „ПСЕВДОИМПОРТОЗАМЕЩЕНИЕМ“»

АЛЕКСАНДР ЯКУНИН, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ОБЪЕДИНЕННОЙ ПРИБОРОСТРОИТЕЛЬНОЙ КОРПОРАЦИИ (ОПК), СЧИТАЕТ ИМПОРТОЗАМЕЩЕНИЕ ПРИОРИТЕТНОЙ ЗАДАЧЕЙ ОБОРОННОЙ ОТРАСЛИ И УВЕРЕН, ЧТО К 2020 ГОДУ УЖЕ ОКОЛО 90% КЛЮЧЕВЫХ КОМПОНЕНТОВ ТЕХНИКИ, ВЫПУСКАЕМОЙ ЭТОЙ ИНДУСТРИЕЙ, БУДУТ ОТЕЧЕСТВЕННЫМИ. ДЛЯ ЭТОГО НЕОБХОДИМО ИСПО-  
ВЕДОВАТЬ КОМПЛЕКСНЫЙ ПОДХОД, А НЕ ЗАМЕЩАТЬ ОТДЕЛЬНЫЕ ИМПОРТНЫЕ КОМПОНЕНТЫ.

**BUSINESS GUIDE:** Какова на сегодняшний день степень автоматизации промышленных предприятий в России? Насколько высок этот показатель, если сравнивать с мировыми стандартами?

**АЛЕКСАНДР ЯКУНИН:** За рубежом процессы автоматизации управления бизнесом и производством начали развиваться еще в 1960–1970 годах. В России плюсы автоматизации осознали только 15 лет назад, когда наши компании наконец задумались об оптимизации управления, производственных процессов и повышении эффективности с помощью новых технологий. Последние десять лет темп роста рынка военных и гражданских АСУ в стране значительно превосходит среднемировую. В прошлом году объем этого рынка в стране составил более 2,5 трлн руб. В ближайшие восемь–десять лет прогнозируется его дальнейший рост на 10% и более в год.

Это позитивный тренд как в целом для российской промышленности, так и для радиоэлектронного комплекса в частности. Помимо повышения качества управления и производства автоматизация влечет развитие целого ряда сегментов радиоэлектроники. Это в первую очередь вычислительная техника, ПО и операционные системы, средства защиты информации, средства и системы связи. Решение задач в области АСУ также тесно увязано с развитием информационно-поисковых систем, систем сбора и обработки информации, в том числе Big Data, комплексных системы безопасности, искусственно-го интеллекта, робототехники. Это все ключевые направления современных ИТ-технологий, на которые активно растет спрос.

**ВГ:** Насколько сегодня промышленность зависима от иностранных систем для управления предприятиями?

**А. Я.:** В силу понятных причин гражданский рынок автоматизированных систем управления, как и рынок ПО, вычислительной техники, телекоммуникационного оборудования, годами рос на предложениях зарубежных компаний. В результате их доля в различных сегментах гражданских АСУ достигает сегодня 80–90%. Основная масса решений, внедряемых на промышленных предприятиях, традиционно базируется на продуктах SAP, Oracle, IBM, Microsoft, других западных и азиатских производителей.

Для большинства потребителей в этом нет ничего критичного. Однако в государственном секторе, стратегических корпорациях, предприятиях оборонно-промышленного комплекса такая ситуация не может считаться приемлемой. Нормативная, финансовая, проектная, производственная информация должна быть надежно защищена от внешних угроз. Применяемое оборудование и ПО должны гарантировать отсутствие незадекларированных возможностей, негласного съема данных, а также устойчивую работу независимо от санкций и других внешних обстоятельств. В связи с этим перед государством остро стоит вопрос построения доверенных информационных

**НАРАЩИВАНИЕ ПРЯМОГО ИМПОРТОЗАМЕЩЕНИЯ КОМПОНЕНТНОЙ БАЗЫ В ОТРЫВЕ ОТ РАЗРАБОТОК АППАРАТУРЫ ТОЛЬКО ВРЕДИТ ОТРАСЛИ. ПОКА СОЗДАЕТСЯ АНАЛОГ, ЗАРУБЕЖНЫЕ РАЗРАБОТКИ ТОЖЕ НЕ СТОЯТ НА МЕСТЕ**



инфраструктур. Это касается как в целом автоматизированных систем, так и их отдельных модулей (управленческих, финансовых, проектных и т. д.), применяемых операционных систем, программного обеспечения, техники, на которой эти системы работают.

Как вы знаете, за последние годы государство приняло ряд мер, которые призваны изменить ситуацию. В частности, в апреле Минпромторг и Минкомсвязи утвердили планы импортозамещения электроники и программного обеспечения. Если в прошлом году доля импорта в общем объеме рынка бизнес-приложений (ERP, CRM, СЭД, управление проектами и т. д.) составила 75%, то к 2020 году этот показатель должен снизиться минимум до 50%, а к 2025 году — до 25%. Доля зарубежных решений в области ПО для промышленности (PLM, CAD, CAM, CAE) должна уменьшиться с нынешних почти 90% до 50–60%.

**ВГ:** Учитываете ли вы при создании российских АСУ лучшие мировые практики?

**А. Я.:** Мы оборонщики и являемся основным поставщиком средств и систем автоматизации, связи, телекоммуникационного оборудования для Минобороны и других государственных спецзаказчиков. Такая специфика обуславливает высокие требования, которые сегодня предъявляются к качеству наших разработок. Уровень наших компетенций позволяет нам самостоятельно реализовывать системные проекты любой сложности и предлагать решения мирового уровня.

Мы имеем большой опыт построения и интеграции автоматизированных систем различного уровня и назначения, в том числе на платформах отечественных разработчиков. В числе наиболее масштабных проектов, реализованных нами, — система ресурсного обеспечения Минобороны и государственная автоматизированная система оценки финансово-технологических рисков, возникающих при выполнении государственного оборонного заказа. Это системы уникальные, не имеющие прототипов.

У предприятий корпорации есть существенный научно-технический задел, который позволяет качественно реализовать программу импортозамещения по этому направлению. В первую очередь я имею в виду потенциал наших НИИ автоматической аппаратуры имени Семени-

хина, Центрального НИИ экономики, информатики и систем управления, концернов «Системпром» и «Созвездие», ряда других предприятий.

Конечно, если мы хотим быть конкурентоспособными, то должны внимательно следить за всем, что происходит в мире высоких технологий, и быть, что называется, в тренде. Рынок автоматизированных систем управления в мире сегодня все больше приобретает «интеллектуальный» уклон. В работе систем участие человека существенно снижается, при этом наращивается функционал и возможности машин. Среди основных тенденций — рост пользовательского спроса на интеллектуальные устройства, массовое оборудование объектов датчиками и исполнительными устройствами, подключение различных устройств к масштабным сетевым инфраструктурам. Все эти направления мы сегодня реализуем в своих разработках.

В частности, мы серьезно продвинулись в вопросах «технического зрения», СУБД, искусственного интеллекта. Например, мы обладаем технологией, с помощью которой можно научить компьютеры понимать и анализировать большие объемы текстов различной сложности. Эта разработка уникальна с точки зрения возможностей анализа Big Data, интеграции разноформатных баз данных, организации и систематизации оборота документов — технических, правовых и т. д. Разработки такого уровня сегодня под силу только компаниям мирового уровня, таким как Google, Facebook. Это 100-процентное импортозамещение, реализованное без всяких заимствований российскими специалистами — лингвистами, математиками, программистами.

**ВГ:** В российской оборонной промышленности сейчас применяется большое число «самописных» программ, различные информационные системы и ПО, которые плохо интегрируются. Как эту проблему стоило бы решать?

**А. Я.:** Только одним путем: необходимо внедрять единую идеологию в этой сфере и предложить рынку унифицированные отечественные решения.

Именно из-за отсутствия единых подходов сейчас тормозится, например, развитие инженерного ПО и автоматизированных PLM-систем в оборонно-промышленном комплексе. Во-первых, распространенное западное ПО на основе закрытого программного кода не может использоваться при разработке изделий специального назначения. Во-вторых, многообразие «разрешенного» ПО, в том числе кустарного, действительно служит плохую службу. Здесь начинаются конфликты разных программных продуктов, потери данных. Плюс теряется драгоценное время: вместо того чтобы пользоваться готовым продуктом, предприятия подчас сами «изобретают велосипед».

Совместно с Фондом перспективных исследований мы сейчас работаем над созданием унифицированной программной инженерной платформы для проектирования и

производства. Это будет модульный продукт на отечественной платформе, который позволит проводить законченный цикл конструкторско-технологической подготовки любого производства в машиностроении. Сюда входит проектирование изделия с созданием трехмерной модели, проведение расчетов (статических, динамических, термодинамических), разработка конструкторской документации, проектирование процессов изготовления деталей на станках с ЧПУ. Очень важно, что речь идет о полностью доверенном, чисто российском ПО, которое без ограничений может использоваться в оборонной промышленности.

Учитывая, что основной тренд сегодня построение глобальных взаимоувязанных систем, такой же унифицированный подход должен быть и в других областях автоматизации процессов. Как у наших основных заказчиков, так и на предприятиях оборонно-промышленного комплекса. Прежде всего разработчики АСУ должны получить единую базовую программную платформу — полнофункциональный конструктор базовых элементов: доверенные операционные системы и СУБД, имеющие необходимые степени защиты и сертификаты. Это позволит главным конструкторам концентрироваться непосредственно на выполнении поставленных задач по автоматизации и не отвлекаться на самостоятельный поиск сопутствующих решений.

Следующим этапом должно стать создание отдельных готовых модулей для автоматизации различных процессов — движение финансов, кадры, закупочная деятельность, контроль поставщиков и качества продукции — в рамках ERP- и PLM-систем. Это позволит строить и внедрять системы на единых подходах, а также исключить применение иностранного ПО в критических сферах и связанные с этим риски. На сегодняшний день у корпорации уже есть существенный задел по этим направлениям.

**ВГ:** Риски связаны не только с применением иностранного ПО, но и зарубежной ЭКБ, которая широко применяется в российской радиоэлектронике. Как решается эта проблема с учетом того, что в России очень мало компонентов сегодня производится собственными силами?

**А. Я.:** Вы удивитесь, но российские предприятия выпускают достаточно большую номенклатуру современной конкурентоспособной ЭКБ. На сегодняшний день в разработках нашей корпорации стратегического уровня, таких как АСУ РВСН, например, нет ни одного импортного компонента. Все комплектующие, включая чипы, там российско-го производства.

Да, доля зарубежной ЭКБ в отечественных разработках остается пока высокой. Радиоэлектроника, как известно, является одной из самых импортозависимых отраслей, и требуются существенные усилия государства и разработчиков для того, чтобы изменить ситуацию. Но необходимо понимать, во-первых, что в массовом сегменте гражданской продукции 100-процентное импортозамещение не нужно: в этом нет никакого смысла. Оно требуется прежде всего в критически важных областях, связанных с защитой стратегических интересов страны, ее промышленности, экономики. Во-вторых, надо внимательно посмотреть, что сегодня уже делают российские производители. Если на должном уровне провести унификацию блоков и модулей, использование зарубежных компонентов уже сегодня можно существенно сократить. Для этого необходимо создать открытую базу данных, где будут отражены все разработки ЭКБ, встраиваемых модулей, а также организовать в широком доступе обменный фонд, своего рода магазин этих продуктов. Должна также появиться-



# В ПОГОНЕ ЗА КАДРОМ

## РОССИЙСКИЕ ПРОМЫШЛЕННЫЕ КОМПАНИИ, КАК ЧАСТНЫЕ, ТАК И ГОСУДАРСТВЕННЫЕ, ВКЛАДЫВАЮТ ЗНАЧИТЕЛЬНЫЕ СРЕДСТВА В НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЕ РАЗРАБОТКИ И МОДЕРНИЗАЦИЮ ПРОИЗВОДСТВА. ЭТО ПРОИСХОДИТ В РАМКАХ ОБЩЕГО ДВИЖЕНИЯ СТРАНЫ В СТОРОНУ СТРОИТЕЛЬСТВА ИННОВАЦИОННОЙ ЭКОНОМИКИ, УХОДА ОТ СЫРЬЕВОЙ МОДЕЛИ. ОДНО ИЗ ГЛАВНЫХ ПРЕПЯТСТВИЙ НА ЭТОМ ПУТИ — НЕДОСТАТОК КВАЛИФИЦИРОВАННЫХ КАДРОВ.

ЛЕОНИД ХОМЕРИКИ

20 лет назад самыми перспективными профессиями считались юристы и экономисты, спустя десятилетие — маркетологи и программисты, сегодня все хотят стать айтишниками и стартаперами. Мало кто мечтает стать фрезеровщиком, слесарем или токарем. Именно эти специальности наиболее востребованы сегодня в оборонно-промышленном комплексе. Нужны также высококвалифицированные инженеры-конструкторы, инженеры-технологи. Промышленность активно автоматизируется, что вызывает потребность в большем числе программистов. Особый случай — двигателестроительная отрасль. Там очень высокие требования к профессиональному уровню специалистов, длительный период вработываемости. Почти невозможно найти и привлечь готовых специалистов, имеющих практический опыт конструирования газотурбинных двигателей. Поэтому предприятиям приходится заниматься поиском специалистов иногда и за рубежом либо выращивать их со студенческой скамьи. Кадровый голод в оборонно-промышленной индустрии острый. Во многом он вызван тем, что в 1990-е годы из-за глубокого кризиса в этой сфере на предприятия не шла молодежь, отсюда старение кадров плюс демографическая яма, образовавшаяся в то же время: рождаемость после развала Союза была очень низкой. Ситуация понемногу меняется, и школьники идут учиться на специальности, которые востребованы в ОПК.

Так, на КамАЗе доля сотрудников в возрасте до 35 лет на сегодняшний день более 30%. В концерне «Калашников» средний возраст в 2013 году составлял 47 лет, а уже в начале 2015-го — 44 года. В начале текущего года доля сотрудников ОДК до 35 лет составляла 25,6%. «Росэлектроника» планирует омолаживать коллектив до 10% в год от общей численности персонала компании (38 тыс. человек), то есть будет набирать каждый год около 4 тыс. молодых специалистов. В холдинге «Технодинамика» доля специалистов в возрасте 18–25 лет составляет 19%, в то время как в 2011 году она не превышала 14%.

Мотивирует молодых людей возможность самореализации, использования полученных знаний на практике в крупных проектах на серьезных промышленных предприятиях. Впрочем, для тех, кто следует прагматичной логике, работают другие аргументы. Предприятия многое делают в социальной сфере: реализуют программы компенсации расходов на оплату детского сада, органи-

ся разветвленная сеть современных центров проектирования ЭКБ, открытых для квалифицированного общественного пользования.

Вместе с тем надо учитывать, что наращивание прямого импортозамещения компонентной базы в отрыве от разработок аппаратуры только вредит отрасли. Пока создается аналог, зарубежные разработки тоже не стоят на месте. И промышленность раз за разом будет вставать перед выбором, какую ЭКБ применять — импортозамещающую, но устаревшую или самую современную импортную. Необходим системный подход, при котором разработки ЭКБ, отдельных узлов и конкретных образцов аппаратуры являются взаимозависимыми. Для этого нужны комплексные целевые проекты, где мы на выходе получим 100% доверенное радиоэлектронное оборудование на отечественных элементах, а не отдельные импортозамещающие компоненты. В целом мы рассчитываем, что к 2020 году около 90% ключевых компонентов нашей техники будут отечественными.

**ВГ:** Каков ваш план по импортозамещению и в какие сроки планируете его реализовать?

**А. Я.:** Напомню, что в составе «Ростеха» корпорация является головной государственной промышленной структурой, отвечающей за разработку, производство и внедрение средств вычислительной техники и телекоммуникационного оборудования. Это наша прямая сфера ответственности в программе импортозамещения. Ориентиры и сроки здесь определены недавно опубликованными планами Минпромторга и Минкомсвязи до 2020–2025 годов. Они коррелируют с целями, которые мы поставили перед собой в Стратегии развития корпорации. Например, к 2020 году в различных категориях вычислительной техники и телекоммуникационного оборудования доля доверенного оборудования в России должна вырасти с нынешних 0–10% до 30–50%. По отдельным позициям — это касается прежде всего поставок для госсектора — до 70–80%.

Планы амбициозные, но вполне реальные, если они будут подкреплены дальнейшими действиями государства. Со своей стороны мы входим в процесс импортозамещения с конкретными наработками и достижениями.

Основой доверенной техники являются три кита: отечественная схемотехника, отечественная ЭКБ и отечественное ПО. Нашими специалистами уже созданы и внедряются образцы вычислительной техники, телекоммуникационного оборудования, которые отвечают всем этим критериям и не уступают ни в чем западным аналогам.

Например, сейчас мы выводим на рынок новые образцы телекоммуникационного оборудования — IP-АТС «Александрит» и коммутаторы и маршрутизаторы операторского класса, которые полностью базируются на наших схемотехнических решениях и ПО. Одно из главных преимуществ этого оборудования — доверенность и защищенность от негласного съема данных, это подтверждено сертификатом Минобороны.

Подчеркну, что мы не занимаемся «псевдоимпортозамещением» и не ставим свой «лейбл» на китайское оборудование, а сами ведем разработку, создаем технологии разработки и свое ПО, производим оборудование на российских мощностях. Эта техника прошла длительное тестирование под серьезными нагрузками на сетях операторского класса, доказав свой функционал и качество.

Оборудование такого класса рассчитано на корпоративного пользователя, оно может использоваться как государственными, так и коммерческими структурами в открытом и закрытом сегментах связи. Большой интерес к нашим разработкам проявляют государственные структуры и подведомственные им организации, крупные производственные компании, поставщики телекоммуникационных услуг и оборудования, поставщики комплексных автоматизированных решений. Они первыми уловили новый тренд: отказ от небезопасных в информационном плане

импортных решений и переход на качественное доверенное оборудование. На рынок мы готовы поставлять до нескольких десятков тысяч единиц такой техники в год.

Одним из основных сдерживающих факторов в этом направлении является отсутствие на рынке «массовой» модели импортозамещающего чипа с современными характеристиками. Большие надежды здесь мы связываем с линейкой процессоров «Эльбрус», которая разрабатывается при участии нашего Института электронных управляющих машин имени Брука. Последняя генерация «Эльбрус-8С» сейчас проходит испытания. Это восьмиядерный процессор с современным техпроцессом 28 Нм и частотой 1,3 ГГц. Прорывного результата мы ждем также от нашего стратегического партнера компании «Т-Платформы», которая сейчас завершает работу над созданием восьмиядерного процессора «Байкал» с частотой 2 ГГц и таким же техпроцессом 28 Нм.

Создание крупносерийного производства современного российского микропроцессора позволит нам выйти на качественно новый и более «массовый» уровень импортозамещения. Техника на основе подобных чипов позволит обеспечить еще более высокий уровень защиты данных, так как она 100-процентно гарантирует отсутствие программных и аппаратных «закладок». По своему функционалу она без проблем сможет заменить многие зарубежные образцы.

**ВГ:** Чувствуете ли вы нехватку ИТ-специалистов? Вам приходится конкурировать за кадры с частным бизнесом, какие преимущества у вас есть, как у работодателя?

**А. Я.:** Конкуренция за профессиональные кадры всегда была. С учетом того что мы государственная структура, в этой борьбе мы ограничены в выборе средств и не всегда можем, например, банально перекупить специалиста. Но, к счастью, в современном мире не все еще измеряется деньгами. Есть такие понятия, как патриотизм, гордость, причастность к передовым разработкам, готовность трудиться на будущее страны. Многие наши специалисты принципиально хотят работать только в оборонке. Наши предприятия традиционно сильны научными школами, технологиями. Мы даем людям расти в профессиональном и карьерном смысле, не платим в «конверте», на наших предприятиях действуют все трудовые нормы, а также различные социальные программы, в том числе жилищные.

Общая численность работающих на предприятиях корпорации — свыше 43 тыс. человек, в том числе около 4 тыс. ИТ-специалистов. Средняя заработная плата в корпорации в прошлом году составила 45 тыс. руб., при этом высококлассные разработчики могут зарабатывать порядка 80–90 тыс. руб. и выше. Средний возраст сотрудника корпорации сегодня 45 лет, и, что не может не радовать, понемногу растет доля специалистов в возрасте от 20 до 40 лет: таких сегодня у нас уже около 40%.

В отличие от частного бизнеса, которому чаще всего нужны готовые профессионалы, мы начинаем работать с будущими специалистами еще со школы. Некоторые наши предприятия проводят конкурсы, экскурсии, уроки, поддерживают наиболее перспективных учеников, оплачивают их целевое обучение в вузах. Студенты целого ряда вузов уже с третьего курса имеют возможность трудоустройства на предприятиях, параллельно продолжая обучение.

Предприятия корпорации поддерживают работу десяти базовых кафедр и семи филиалов кафедр по различным специальностям. Среди вузов, с которыми мы тесно сотрудничаем, — МФТИ, МГТУ им. Н. Э. Баумана, МГУ, Московский государственный университет связи и информатики, Московский институт электроники и математики, Санкт-Петербургский государственный электротехнический университет, Военмех им. Д. Ф. Устинова, Санкт-Петербургский политехнический университет, Санкт-Петербургский государственный университет аэрокосмического приборостроения, ряд других вузов, в том числе в регионах страны.

На днях была утверждена концепция производственно-технологического развития корпорации, где мы исходим из того, что технологическое движение вперед невозможно без развития системы подготовки кадров. Мы намерены активно участвовать в составлении программ профобучения, шире привлекать студентов к разработкам и производственной практике. Все это поможет нам сформировать кадры новой формации, за которыми будущее отрасли.

Интервью взяла МАРИЯ АНАСТАСЬЕВА

зуют детские оздоровительные лагеря, санаторно-курортное лечение и отдых сотрудников. «Ростех» приступает к реализации масштабной программы по обеспечению сотрудников жильем. Компании, входящие в «Ростех», смогут направить на улучшение жилищных условий сотрудников около 2 млрд руб. до конца текущего года. Участниками корпоративной программы как раз станут квалифицированные специалисты наиболее востребованных профессий, в которых испытывается кадровый дефицит.

Но есть и другая проблема: по мнению собеседников „Ъ“, преподаваемые сегодня в вузах практические знания и навыки существенно отстают от требований передовых предприятий, использующих современные ИТ.

Российская система образования обладает определенной инертностью, которая мешает тому, чтобы на рынке труда вовремя появлялись специалисты, владеющие нужными современными технологиями. Методы контроля качества образования работают по быстро устаревающим требованиям. Пока образовательные учреждения внедряют, адаптируются и начинают использовать новые стандарты, они уже начинают отставать от тех достижений современных информационных технологий, которые появляются на рынке. В результате, по словам заведующего кафедрой новых медиа и теории коммуникации факультета журналистики МГУ Ивана Засурского, сейчас очень многие позиции остаются незаполненными потому, что не удастся найти правильных специалистов. Это характерно для любой высокотехнологичной отрасли, которой, безусловно, является и оборонная промышленность.

Для решения этой проблемы «Ростех» активно взаимодействует с вузами. На данный момент корпорацией заключены соглашения о сотрудничестве более чем с 200 вузами, создаются базовые кафедры для подготовки специалистов. Кроме того, в «Ростехе» прорабатывается вопрос объединения бюджетов предприятий на образовательные цели и создания единого центра обучения — корпоративного университета, где можно будет внедрять ведущие мировые практики. Сотрудничая с вузами, решают проблему подготовки и другие промышленные предприятия. Но дефицит кадров при этом сохраняется.

Эксперты отмечают, что необходимо усиливать связи вузов с работодателями. Например, по словам Ивана За



**«РОСТЕХ» ПРИСТУПАЕТ К РЕАЛИЗАЦИИ МАСШТАБНОЙ ПРОГРАММЫ ПО ОБЕСПЕЧЕНИЮ СОТРУДНИКОВ ЖИЛЬЕМ. КОМПАНИИ, ВОХОДЯЩИЕ В «РОСТЕХ», СМОГУТ НАПРАВИТЬ НА УЛУЧШЕНИЕ ЖИЛИЩНЫХ УСЛОВИЙ СОТРУДНИКОВ ОКОЛО 2 МЛРД РУБ. ДО КОНЦА ТЕКУЩЕГО ГОДА**



сурского, проект «Востребованное образование» предполагает, что работодатели будут формулировать запрос на решение актуальных проблем своего бизнеса, социальных и практических задач в виде тем для проведения конкурсов учебных и дипломных работ. В следующем учебном году начиная с сентября больше десяти вузов примет участие в пилотном, добровольном этапе проекта. Работы выпускников будут опубликованы, а их учащиеся смогут с помощью учебной работы построить себе карьеру — хотя бы в виде практики или стажировки, бюджетных мест в аспирантуре или гранта на продолжение исследований. «Развитие электронных систем для студентов, в том числе для публикации научных работ, безусловно, сдвинет процесс в лучшую сторону», — резюмирует Антон Меркуров, эксперт Institute for State Ideologies.

**БЛИЗКО К ПРОВАЛУ** Отдельная категория сотрудников, которая очень нужна оборонке, — специалисты в области информационных технологий по самым разным направлениям. Сегодня невозможно выпускать современную промышленную продукцию без интенсивного внедрения ИТ в процессы разработки и производства. Поэтому достижение цели новой индустриализации невозможно без перевода в цифровой формат инженерно-конструкторской, производственно-технологической и финансово-экономической деятельности высокотехнологичных предприятий. «К сожалению, руководство промышленных предприятий относится к ИТ не как к стратегической задаче изменения технологического уклада и перехода к новому формату деятельности, а как к второстепенному фактору производства», — отмечает Владимир Рубанов, член общественного совета при Минпромторге РФ. По его словам, топ-менеджеры слабо представляют роль, место и возможности ИТ, а также требования к соответствующей реорганизации предприятия и подготовке кадров при их внедрении. Это требует включения в образовательный стандарт для руководящих кадров компетенции заказчика информационных технологий и систем производственного назначения.

Это критически важная задача, ведь промышленные предприятия сейчас часто работают на устаревших системах, что повышает риск подвергнуться нападению хакеров. В XXI веке задачи ОПК во многом переместились в область кибернетической безопасности. «Для повышения обороноспособности и в том числе кадровой безопасности страны предприятия ОПК должны не только формировать заказ, но и предугадывать его на будущее. Сегодня большой акцент в этой сфере стоит на машиностроении (двигатели, летательные аппараты, спецтехника), последние конфликты показали, что война будущего — это в первую очередь кибербезопасность», — говорит Антон Меркуров. В эту сферу, по его словам, попадают как защитники стратегические объектов, так и наступательные функции. Если раньше нам нужны были солдаты на поле боя, то в ближайшем будущем воевать они будут не выходя из-за компьютера. И задача государства в этой сфере — обеспечить привлекательные рабочие места и формулировать задачи, нацеленные на развитие собственных продуктов для защиты.

В идеале в каждой автоматизированной системе управления (АСУ) материальными и людскими ресурсами уже должны быть встроены средства кибербезопасности. В устаревших решениях их, конечно, нет. При этом ущерб от неправильной работы таких систем, от последствий их взлома может быть огромен. К примеру, подобные АСУ, которые в XXI веке все чаще становятся мишенью кибертеррористов, используются на критических важных объектах: транспортных узлах, АЭС, ТЭС, ГЭС, на крупных производственных предприятиях и т. п.

В большинстве случаев такие АСУ построены на программно-аппаратном обеспечении зарубежного произ-



В РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ ВСЕ ЕЩЕ НАБЛЮДАЕТСЯ ДЕФИЦИТ МОЛОДЫХ СПЕЦИАЛИСТОВ

водства, которое, как говорят эксперты, во-первых, не является доверенным, во-вторых, имеет множественные уязвимости. На всем жизненном этапе АСУ — от проектирования до эксплуатации — задействованный в процессах персонал ввиду не очень высокой компетенции и отсутствия специальных знаний может допускать существенные ошибки, что негативно сказывается на защищенности подобных систем. Во многом подобная ситуация складывается ввиду отсутствия систематизированной подготовки кадров.

Эта проблема касается не только предприятий ОПК, но также и других системообразующих отраслей российской экономики, например нефтегазовой и электроэнергетической. Учитывая особенный характер получаемых при обучении знаний и умений, связанный с двойным вариантом их применения, эта область образовательной деятельности должна иметь особый уровень контроля качества, говорят в «Ростехе». Речь идет не о совершенствовании федерального контроля качества образования в области информбезопасности, а о создании дополнительной системы контроля, основанной на сертификации квалификационного уровня выпускников образовательных учреждений. Для этого необходимо создать комплекс сертификационных требований, определить совокупность доверенных независимых сертификационных центров и предоставить всем желающим возможности пройти испытания и подтвердить соответствующий сертификационный уровень. Разработка сертификационных программ должна вестись на основе создаваемых профессиональных стандартов в области информационной безопасности.

Помимо этого ни у кого не возникает сомнений в том, что нужно обязательно внедрять в сферу подготовки ИТ в России современные образовательные технологии. Есть и такое мнение, что необходимо использовать два вида образовательных программ на каждом уровне обучения: одна — для целевой подготовки обучаемых, выпускаемых на предприятия госсектора (национальная система сертификации), другая — для обучаемых, связавших свою карьеру с коммерческими предприятиями (международная система сертификации). Также нужно выстраивать продуманную кооперацию между образованием, наукой и промышленностью, которая должна формировать заказ на подготовку кадров.

В отличие от многих других областей информационной безопасности, в сфере кибернетической безопасности АСУ ТП критически важных объектов для качественной подготовки кадров требуются большие инвестиции в создание современных учебно-лабораторных баз и испытательно-диагностических лабораторий. Такое положение дел связано с дороговизной систем АСУ зарубежного производства (Siemens, ABB, Schneider Eclectic и т. п.), а также тем фактом, что для подготовки специалистов требуется работа не только с компьютерной системой, но и со сложной иерархической системой контроллеров, причем как на уровне разработки программного кода, так и на аппаратном уровне.

То есть компетенции профессионально-кадрового состава сферы ИТ в России сконцентрированы на решении задач локализации и адаптации импортных решений, программных продуктов и электронной техники, навыках программирования и системной интеграции. Однако как подчеркивает Владимир Рубанов, сегодня общемировой вектор развития ИТ связан с умениями управления информацией, концептуального и логического моделирования и архитектурного проектирования сложных информационных систем. Ожидания от прорывов в сфере ИТ путем концентрации усилий только на индустрии программирования представляются неоправданными, так как успехи в сфере ИТ связаны со знанием предметных областей их применения, умением поставить и формализовать задачи для программирования. Это требует смещения образовательных программ от технических навыков программирования к умениям моделирования и формализации описания деятельности в предметных областях применения ИТ.

Как говорят в «Ростехе», учитывая существующие проблемы с государственным финансированием бюджетных отраслей, можно прийти к единственному оптимальному решению на данный момент, связанному с формированием контингента обучающихся на бюджетной основе исключительно на основе государственного заказа с обязательным распределением выпускников в государственные учреждения. Подготовка специалистов для негосударственных организаций должна вестись на платной основе или при наличии компенсации затрат на обучение, если выпускник, прошедший обучение на бюджетной основе, по тем или иным причинам вынужден трудоустроиться в негосударственную организацию.

«Подходы к организации научно-образовательных экосистем в случае с гражданским сектором и обороной

действительно разные. И там, и там огромную роль сыграют системы открытой публикации и доступа к исследованиям, но в случае с обороной реализация потенциала этих систем упирается в уровни доступа. Понятна потребность в закрытии информации для «внешних» специалистов не только по принципу страновой принадлежности, но и вообще за рамками ОПК или конкретных концернов. Однако сам принцип открытого информационного обмена и конкурсного трудоустройства будет в итоге реализован и там, и там. А образовательные программы должны быть привязаны, на мой взгляд, к конкретным потребностям каждого сектора индустрии», — комментирует Иван Засурский.

**ОБМЕН РАЗУМОВ** Еще одной из причин огромного дефицита качественных ИТ-специалистов на производствах является наследие системы рекрутинга специалистов, ориентированной на несколько вузов, у которых есть соответствующие базовые кафедры по подготовке специалистов. «Вы не можете попасть на работу, к примеру, в ЦАГИ, если вы не учились там, где они набирают специалистов. Поэтому набор ограничен вузами, где такая возможность есть, и теми студентами, которые, поступая в вуз, уже знали, где они хотят работать. Люди из других вузов, даже если они хотят работать, не имеют шансов устроиться в оборонно-промышленный сектор, потому что нет системы рекрутинга, который бы позволил брать специалистов, которые компаниям действительно нужны», — поясняет Иван Засурский. По мнению эксперта, необходимо выстраивать систему рекрутинга по-новому, открывать входы в карьеру в ОПК и индустрию на новых уровнях. В ситуации экономического кризиса карьеры в ОПК может оказаться интересным предложением для молодых людей, особенно в сочетании с программой поддержки в плане жилищно-бытовых условий. К сожалению, пока, по словам Антона Меркурова, «в короткой перспективе ИТ-образование в России — это в первую очередь билет в Европу или Силиконовую долину. В технологических вузах все еще сильное академическое образование, что до сих пор делает российских специалистов востребованными за рубежом».

Но, как говорилось выше, хорошие специалисты не всегда уезжают только из материальных соображений — большую роль играет возможность самореализации, шанс участвовать в интересном научном проекте в сотрудничестве с экспертами, у которых можно многому научиться. Сегодня одним из главных направлений совершенствования подготовки кадров, в частности, в сфере информационной безопасности является создание на базе ведущих учебных заведений современной лабораторной базы, которая позволила бы, во-первых, получить глубокие знания в данной области, а во-вторых, осуществлять качественную подготовку кадров самого различного профиля: проектировщиков, эксплуатационников и специалистов, в том числе в области кибернетической безопасности АСУ. Среди возможных путей за счет начального госфинансирования на базе ведущих вузов могут быть созданы коллективные центры прорывных решений в сфере ИТ (например, кибербезопасности), которые по материально-техническому оснащению находились бы на передовом мировом уровне и в перспективе за счет выполнения НИР и НИ-ОКР смогли бы обеспечить свое последующее финансирование и развитие.

Кроме того, необходимо шире использовать возможности сетевого обучения, отмеченные в новом законе «Об образовании», которые позволят сконцентрировать усилия профессионалов из различных областей (техническая, финансово-экономическая, лингвистическая и др.) по ряду направлений подготовки в сфере ИТ для достижения максимального эффекта по уровню знаний и умений. ■

**В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ АСУ ТП КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ДЛЯ КАЧЕСТВЕННОЙ ПОДГОТОВКИ КАДРОВ ТРЕБУЮТСЯ БОЛЬШИЕ ИНВЕСТИЦИИ В СОЗДАНИЕ СОВРЕМЕННЫХ УЧЕБНО-ЛАБОРАТОРНЫХ БАЗ И ИСПЫТАТЕЛЬНО-ДИАГНОСТИЧЕСКИХ ЛАБОРАТОРИЙ**



# КИБЕРВОЙНЫ XXI ВЕКА

## САМЫЕ ГРОМКИЕ СЛУЧАИ ПРИМЕНЕНИЯ КИБЕРОРУЖИЯ

### УТЕЧКА ДАННЫХ ИЗ JPMORGAN CHASE 2014

Крупнейший американский банк, один из старейших финансовых институтов на планете подвергся серьезной хакерской атаке, в результате чего более 83 млн счетов были скомпрометированы. По одной из версий, за нападением стояли русские хакеры, также атаковавшие другие банки США

### ТИТАНОВЫЙ ДОЖДЬ 2003-2006

В эту группу специалисты записывают серию атак на американские и британские компании, тесно сотрудничающие с правительством: NASA, Lockheed Martin и другие. Точные масштабы нападения неизвестны, однако в нем подозревают китайских хакеров либо кого-то, кто использовал для этого расположенные на территории Китая компьютеры

### НАПАДЕНИЕ НА ЭСТОНИЮ 2007

Серия массированных DDoS-атак на эстонские государственные порталы началась 27 августа, сразу после решения правительства перенести статую бронзового солдата в Таллине. В организации нападения некоторые специалисты обвиняют структуры, близкие к движению «Наши»

### СУХУМИ 2009

Прогрузинский блогер Сухуми, принимавший активное участие в информационной войне между Россией и Грузией в 2008 году, был выбран главной целью хакеров, сумевших «положить» 7 августа на пару часов платформы Facebook, Google Blogger, LiveJournal и Twitter

### НАПАДЕНИЕ НА КОРЕЮ 2009

Более 166 тыс. компьютеров были инфицированы вирусом, сделавшим их частью огромного ботнета, чей атакующий потенциал был направлен против правительственных, финансовых и медийных сайтов Южной Кореи

### ОПЕРАЦИЯ АВАВИЛ 2012

Общее название для серии кибератак на американские финансовые институты, инициированной группировкой Cyber fighters of Izz Ad-Din Al Qassam, названной в честь мусульманского проповедника

### АЗС В БУШЕРЕ, ИРАН 2010

По версии New York Times, компьютерный червь Stuxnet был разработан спецслужбами США и Израиля специально для саботажа иранской ядерной программы. По данным Symantec, вирусом оказалось заражено 58,85% компьютеров Ирана, 18,22% компьютеров Индонезии и 8,31% машин в Индии

### ОПЕРАЦИЯ «АВРОРА» 2009

Серия кибератак, инициированных в 2009 году структурами, близкими к Китайской народной освободительной армии, против американских интернет-гигантов, по большей части Google

### АТАКА НА БИРМУ 2010

Мощнейшая DDoS-атака на крупнейшего интернет-провайдера Бирмы началась незадолго до первых за 20 лет всеобщих выборов, впоследствии признанных фиктивными

### АТАКА «МЕССИИ» 2013

1 июня государственными регуляторными органами Сингапура были приняты новые правила: в течение 24 часов все местные сайты с посещаемостью от 50 тыс. посетителей должны были удалить с серверов любые статьи, призывающие к «нарушению расовой либо религиозной гармонии» в стране. В ответ на это хакерская группировка «Анонимусы» инициировала атаку на государственные сайты Сингапура, в том числе сайт премьер-министра.

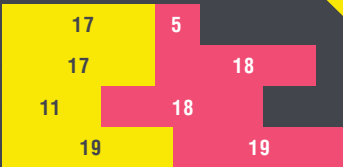
### ОПЕРАЦИЯ CLEAVER 2014

Согласно отчету компании Cyllance, к массовой атаке на 50 объектов из 16 стран (в том числе Korean Air, Qatar Airlines, Pemex) оказались причастны иранские хакеры, тесно связанные с Корпусом стражей исламской революции

## АТАКИ НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ

### ОСНОВНЫЕ ПРИЧИНЫ ИНЦИДЕНТОВ В ИНДУСТРИАЛЬНЫХ СЕТЯХ (%)

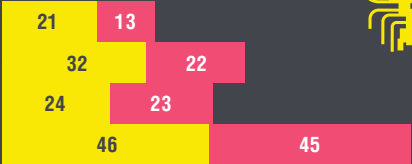
Интеллектуальная собственность  
Информация о клиентах  
Информация о рынке, маркетинговая интеллектуальная собственность  
Информация о внутренних операциях



■ Промышленные компании ■ ЖКХ и энергетические компании

### КАКИЕ ДАННЫЕ У ВАС БЫЛИ УКРАДЕНЫ?

Интеллектуальная собственность  
Информация о клиентах  
Информация о рынке, маркетинговая интеллектуальная собственность  
Информация о внутренних операциях



## ГИБРИДНАЯ ВОЙНА

### КОНВЕНЦИОНАЛЬНЫЕ ВОЕННЫЕ ДЕЙСТВИЯ

#### Обычная война

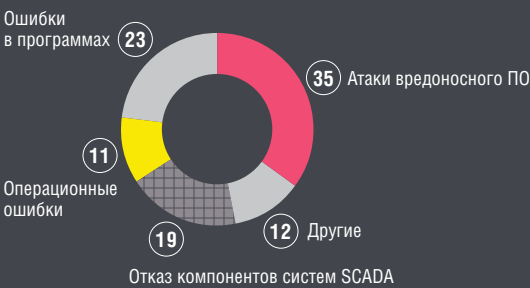
**Малая война**  
(разведывательные, диверсионные, террористические действия малых подразделений; уязвимые цели: мобильные устройства госслужащих; АСУ иностранного производства)

### КИБЕРВОЙНА

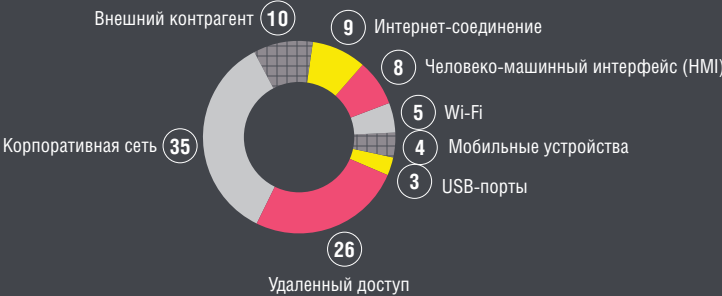
#### Применение кибероружия

**Новые методы пропаганды и дезинформации**  
(крайне эффективны через социальные медиа)

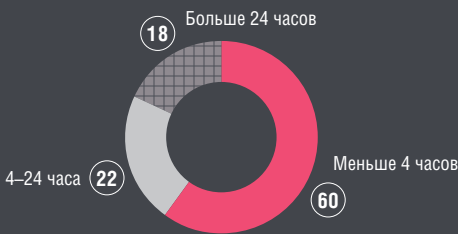
### ОСНОВНЫЕ ПРИЧИНЫ ИНЦИДЕНТОВ В ИНДУСТРИАЛЬНЫХ СЕТЯХ (%)



### ТОЧКИ ПОПАДАНИЯ ВРЕДНОСНОГО ПО В ПРОМЫШЛЕННЫЕ СЕТИ (%)



### ВРЕМЯ БЕЗДЕЙСТВИЯ СИСТЕМЫ В РЕЗУЛЬТАТЕ ЗАРАЖЕНИЯ (%)



ИСТОЧНИКИ: SECURITYINCIDENTS.NET, KASPERSKY LAB, 2014.

# УПРАВЛЯЕМЫЕ АВТОМАТЫ

## Крупнейшие мировые компании в области как гражданского, так и военного машиностроения — Airbus, Sikorsky, Safran, Pratt & Whitney, Honeywell — внедряют или уже используют автоматизированные системы управления, которые охватывают все этапы создания продукции, начиная с закупки комплектующих и заканчивая сбытом. В России высокоуровневая организация управления производством пока редкость.

ЛЕОНИД ХОМЕРИКИ

Как показывает опыт, с помощью правильно подобранной и профессионально инсталлированной автоматизированной системы управления (АСУ) можно добиться более высокой точности производственного планирования до уровня 98%, роста производительности персонала на дополнительные 30% и повышения удовлетворенности клиентов на 10–20%. Это также ведет к снижению издержек за счет более эффективной загрузки оборудования и сотрудников, уменьшению запасов материалов на складах, сокращению цикла производства, а также снижению рисков выполнения заказов за счет предсказуемости сроков изготовления с учетом загрузки и сроков поставки материалов. Также система позволяет повысить качество и скорость принятия управленческих решений, что прямо отражается на эффективности использования ресурсов. А прозрачность системы позволяет снизить риски и повысить привлекательность предприятия для инвесторов и банков. Новейшие технологии автоматизированного управления производством охватывают еще более широкий набор процессов, сопровождающих выпускаемую продукцию в течение всего периода ее жизни: от проектирования до утилизации. Но до уровня такого рода систем в России доросли лишь некоторые предприятия.

На сегодняшний день в нашей стране идет переход от «лоскутной» автоматизации на промышленные системы, созданные на базе международных стандартов, охватывающие все ключевые процессы. Эта волна автоматизации затрагивает не только частные компании, но и производственные предприятия оборонно-промышленного комплекса страны. Тренд наблюдается на фоне стремления к импортозамещению: внедряемые системы по новым требованиям должны быть отечественного производства, даже если разработаны на базе иностранных платформ.

Центральный научно-исследовательский институт экономики, информатики и систем управления (ЦНИИ ЭИСУ) работает над созданием автоматизированных систем управления вооруженными силами, предназначенных для широкого спектра задач: начиная от боевого управления и заканчивая системами ресурсного обеспечения для повседневной жизни Министерства обороны. Сейчас система ресурсного обеспечения с кодовым названием «Алушта» поэтапно вводится в эксплуатацию. Она позволяет в едином центре видеть и контролировать учет всех средств от Калининграда до Владивостока, осуществляя таким образом централизованный мониторинг и контроль. Это сделано для прозрачности закупок и своевременного реагирования на изменение ситуации.

Одна из самых главных задушек ЦНИИ ЭИСУ — это унификация всей IT-системы в рамках Министерства обороны, потому что сейчас IT-структура крайне разнородна. Это характерно не только для армии, но и для предприятий ОПК.

В настоящее время система «Алушта» базируется на платформе SAP, а работает на ОС Windows. При этом планируется перевести ее на отечественную ОС «Заря» и собственную платформу в целях повышения безопасности.

Другой пример. Холдинг «Технодинамика» госкорпорации «Ростех» внедряет у себя решение SAP Enterprise Resource Planning. Проект является крупнейшим в Восточной Европе. Планируется, что информационная платформа SAP ERP будет полностью внедрена на ключевых предприятиях холдинга к 2017 году. Экономический эффект для «Технодинамики» будет достигнут за счет ускорения оборачиваемости и высвобождения оборотного капитала, повышения эффективности работы персонала, повышения загрузки оборудования и снижения производственных издержек. Платформа охватит все участки: от производственного планирования до финансового и управленческого учета компании, объединит процессы производства, закупки и сбыта продукции.



ГЕНДИРЕКТОР «ТЕХНОДИНАМИКИ» МАКСИМ КУЗЮК ОБЕЩАЕТ ЗАВЕРШИТЬ ВНЕДРЕНИЕ СИСТЕМЫ SAP ERP В КОМПАНИИ В 2017 ГОДУ

**МАРШ-БРОСОК** Эксперты в один голос говорят, что высокоуровневая организация производства не самое сильное место отечественной экономики, и не слишком оптимистичны относительно планов по созданию российских систем в этой сфере с нуля. «Нагнать конкурентов теоретически возможно. Но для этого требуется иная модель развития, основанная на участии в международной конкуренции. Как это нам демонстрирует Китай, научившийся писать и продавать, например, системы АСР для операторов сотовой связи», — отмечает аналитик агентства MForum Analytics Алексей Бойко. Говорить о каких-то российских успехах можно было бы, по его словам, не ранее чем наши продукты в области автоматизации производств начали бы массово выигрывать международные тендеры. Сейчас этого не происходит. Создать большую и эффективную АСУ в условиях ограниченного рынка России вряд ли возможно, констатирует эксперт.

Между тем внутренний рынок для таких систем может быть вполне достаточным для того, чтобы нарастить компетенции и превратить отечественные решения в конкурентоспособные. Большинству машиностроительных предприятий ОПК неизбежно предстоит заниматься автоматизацией и роботизацией многономенклатурного единичного или мелкосерийного производства. При нормировании названных производств основными особенностями являются: отказ от прямого использования норм для начисления заработной платы (вследствие гибкости операционных норм, широкой номенклатуры деталей и быстро меняющихся технологий), возрастание роли диспетчирования (из-за высокой вариативности очередей единичных производственных заданий) и необходимостью интерактивной информационной поддержки со стороны специальных терминалов ручных операций (в результате повышения уровня их сложности).

Рынок двигает и политика импортозамещения. В апреле текущего года Минпромторг и Минкомсвязь утвердили планы импортозамещения электроники и программного обеспечения. Если в прошлом году доля импорта в общем объеме рынка бизнес-приложений (ERP, CRM, СЭД,

управление проектами и т. д.) составила 75%, то к 2020 году этот показатель должен снизиться минимум до 50%, а к 2025 году — до 25%. Доля зарубежных решений в области ПО для промышленности (PLM, CAD, CAM, CAE) должна уменьшиться с нынешних почти 90% до 50–60%.

«Уровень наших компетенций позволяет нам самостоятельно реализовывать системные проекты любой сложности и предлагать решения мирового уровня», — утверждает генеральный директор Объединенной приборостроительной корпорации Александр Якунин. По его словам, в настоящее время имеется большой опыт построения и интеграции автоматизированных систем различного уровня и назначения, в том числе на платформах отечественных разработчиков. В числе наиболее масштабных проектов, реализованных ОПК, собеседник называет систему ресурсного обеспечения Минобороны и государственную автоматизированную систему оценки финансово-технологических рисков, возникающих при выполнении государственного оборонного заказа. Это системы уникальные, не имеющие прототипов.

У предприятий корпорации есть существенный научно-технический задел, который позволяет качественно реализовать программу импортозамещения по этому направлению. В первую очередь Александр Якунин обращает внимание на потенциал НИИ автоматической аппаратуры имени Семенихина, Центрального НИИ экономики, информатики и систем управления, концернов «Системпром» и «Созвездие».

Рынок автоматизированных систем управления в мире сегодня все больше приобретает «интеллектуальный» уклон. В работе систем участие человека существенно снижается, при этом наращиваются функционал и возможности машин. Среди основных тенденций — рост пользовательского спроса на интеллектуальные устройства, массовое оборудование объектов датчиками и исполнительными устройствами, подключение различных устройств к масштабным сетевым инфраструктурам. По словам господина Якунина, все эти направления сегодня реализуются в отечественных разработках.

По мнению Алексея Бойко, процесс внедрения продвинутых АСУ безусловно идет в российской оборонке, но с заметным отставанием от ситуации за рубежом. Притом

кроме массы технических проблем, есть и проблемы системные. В частности, несоответствие нормативных актов развитию процесса автоматизации. Нет стандартов «вход-выход» АСУ и производственных комплексов различного назначения. Нет навыков создания удобных интерфейсов для пользователей элементами АСУ.

В то же время, как говорят в «Ростехе», у российских компаний есть серьезные наработки в инновационных сферах: в области «технического зрения», нового типа СУБД, искусственного интеллекта. «Например, мы обладаем технологией, с помощью которой можно научить компьютеры понимать и анализировать большие объемы текстов различной сложности. Эта разработка уникальна с точки зрения возможностей анализа Big Data, интеграции разноформатных баз данных, организации и систематизации оборота документов — технических, правовых и т. д. Разработки такого уровня сегодня под силу только компаниям мирового уровня, таким как Google, Facebook. Это стопроцентное импортозамещение, реализованное без всяких заимствований российскими специалистами — лингвистами, математиками, программистами», — отмечает господин Якунин.

**КРЕПКИЙ ФУНДАМЕНТ** Однако для того, чтобы российские IT-разработки для ОПК стали конкурентоспособными как по качеству, так и по стоимости, разработчики АСУ должны получить единую базовую программную платформу — полнофункциональный конструктор базовых элементов: доверенные операционные системы и СУБД, имеющие необходимые степени защиты и сертификаты. Это позволит главным конструкторам концентрироваться непосредственно на выполнении поставленных задач по автоматизации и не отвлекаться на самостоятельный поиск сопутствующих решений.

Разработки в этой сфере сегодня уже активно ведутся. Холдинг «Системы управления» работает над созданием интегрированной инженерной программной платформы по заказу Фонда перспективных исследований. Платформа призвана существенно упростить и унифицировать процессы создания ПО, используемого в проектировании и производстве на предприятиях оборонно-промышленного комплекса. Инновационный программный продукт, создаваемый в рамках проекта под кодовым названием «Курс», будет размещен на специальном портале, куда получат доступ разработчики и потребители такого «софта». Демонстрационный образец «Курса» будет готов к концу 2016 года. Интерес к проекту уже проявил ряд крупных предприятий и корпораций.

Следующим этапом должно стать создание отдельных готовых модулей для автоматизации различных процессов — движение финансов, кадры, закупочная деятельность, контроль поставщиков и качества продукции — в рамках ERP- и PLM-систем. Это позволит строить и внедрять системы на единых подходах, а также исключить применение иностранного ПО в критических сферах и связанные с этим риски. На сегодняшний день у Объединенной приборостроительной корпорации уже есть существенный задел по этим направлениям.

В целом оборонные производства сегодня испытывают серьезные проблемы в области автоматизации производства, решение которых вряд ли возможно в сжатые сроки и в условиях курса на определенную конфронтацию со странами, обладающими основными компетенциями в этой области, подводит итог Алексей Бойко. Однако это не значит, что за сложные задачи не стоит и браться: превратить российские промышленные производства в поистине высокотехнологичные возможно, хотя и непросто, и этот процесс уже начался. ■

# KOMMERSANT.RU

**BUSINESS GUIDE** ТЕМАТИЧЕСКИЕ ПРИЛОЖЕНИЯ К ГАЗЕТЕ **КОММЕРСАНТЪ**



# BUSINESS GUIDE

Тематические приложения к газете  
**Коммерсантъ**

ТЕОРИЯ И ПРАКТИКА  
ПЕРЕДОВИКИ ПРОИЗВОДСТВА  
СМЕЖНИКИ  
ИНВЕСТОРЫ  
КОНКУРЕНТЫ  
АДМИНИСТРАТИВНЫЙ РЕСУРС