«Сегодня подходы к обеспечению безопасности на всех уровнях должны быть комплексными»

Первый заместитель генерального директора «Российской корпорации средств связи» (РКСС) ***Андрей Юрьевич Бадалов*** *дал эксклюзивное интервью журналу «Транспорт и Связь Российской Федерации», рассказав о подходах компании к проблемам комплексной безопасности.*

– Андрей Юрьевич, что собой представляет «Российская корпорация средств связи»? Каков ее статус и место в государственной корпорации «Ростехнологии»?

– «Российская корпорация средств связи» – российская частно-государственная компания, учреждена в 2007 году решением Правительства Российской Федерации как совместное предприятие госкорпорации «Ростехнологии» и группы высокотехнологичных ИТ-компаний для создания и производства в России доверенного телекоммуникационного оборудования и систем связи. РКСС входит в состав одного из ведущих холдингов корпорации ОАО «Росэлектроника». В целом холдинг занимается развитием электронной промышленности. Мы же, находясь внутри холдинга, отвечаем за вопросы ИТ, связи, систем комплексной безопасности и построение ситуационных центров. Мы получаем значительную поддержку со стороны руководителей корпорации «Ростехнологии» в вопросах организации производства, взаимодействия с органами государственной власти, крупнейшими международными компаниями.

– В каком направлении развивается производство сегодня?

– Мы приближаемся к такому этапу, когда необходимо перейти перейти от отраслевых подходов к построению комплексных систем территориального уровня, которые позволяют решить вопросы безопасности по направлениям и объединяют эти направления: транспорт, электроэнергетику, нефтегазовую промышленность, муниципальную безопасность и другие. Развивая отраслевые подходы, мы, так или иначе, дублируем решения, строим системы, которые могут «конфликтовать» между собой с точки зрения технологических решений и взаимодействия.

На данный момент у нас большой опыт по созданию систем безопасности. Мы принимали участие в создании комплексной системы безопасности города Москвы, объединив десятки тысяч камер. РКСС также выступила генподрядчиком в создании комплексной системы безопасности Красноярска, разработанной по инициативе краевой администрации. Данная система, получившая название «Безопасный город», позволила сформировать в масштабах Красноярска единое информационное пространство и обеспечить взаимодействие органов государственной власти и местного самоуправления.

Сейчас мы перешли к этапу, на котором повышенное внимание уделяем системам интеллектуальной обработки информации. Мы создаем системы оповещения, которые эффективно доставляют нужные данные нужным людям с описанием сложившейся ситуации.

Мы также работаем над так называемым онтологическим моделированием. Это направление позволяет структурировать информацию, описывать ее в единых терминах. Мы строим модель и раскладываем ее на составляющие объекты и субъекты деятельности, отношения между ними, задачи по месту и времени. Таким образом, мы структурируем заданную предметную область. На основании этой структуризации разрабатывается язык информационного взаимодействия между объектами и субъектами деятельности, который в дальнейшем ложится в основу написания на нем регламентов и организации взаимодействия, без которых приступать к разработке комплексных систем безопасности очень сложно. Название нашей системы подчеркивает, что мы уделяем внимание не только физической безопасности объектов или территорий, но и информационной, технологической и даже природной.

На практике сегодня мы получаем вал плохо структурированной информации. Обработать это практически невозможно. Мы пытаемся ее систематизировать. Например, в области энергетики разрабатываем единый язык энергетика, чтобы люди передавали информацию в соответствии с некоторыми шаблонами.

Мы работаем над так называемым онтологическим моделированием. Это направление позволяет структурировать информацию, описывать ее в единых терминах. Мы строим модель и раскладываем ее на составляющие.

Без моделирования получаются разрозненные системы описания ситуации. Поэтому мы и ведем речь о комплексной безопасности. Если транспортная безопасность будет «говорить» на одном языке, а энергетическая – на другом, то, когда эта информация попадет в единый штаб, ее сложно будет обработать, особенно в условиях сжатых сроков, когда надо принимать важное решение.

– На выставках РКСС представила в этом году комплексную автоматизированную систему управления безопасностью (КАСУБ) и мобильный ситуационно-аналитический центр (МСАЦ), созданные по заказу ОАО «Федеральная сетевая компания» (ОАО «ФСК ЕЭС»). Расскажите, пожалуйста, о них подробнее, какие решения они предлагают?

– Проект по созданию комплексной системы безопасности для ОАО «ФСК ЕЭС» был начат РКСС в 2010 году. КАСУБ предназначена для повышения уровня безопасности энергообъектов, снижения рисков нештатных ситуаций, а также для интеграции систем безопасности и средств автоматизации органов управления. Система позволяет интегрировать инженерно-технические средства охраны (видеокамеры, периметральные сигнализации, системы управления контроля доступом и т. п.) в единое информационное пространство и обеспечить доступ к информации уполномоченных лиц на различных уровнях (объектовый, региональный, федеральный). Так, при возникновении нештатной ситуации, в ситуационно-аналитическом центре ОАО «ФСК ЕЭС», созданном компанией «РКСС», существует возможность контролировать обстановку на объекте и принимать управленческие решения по ее локализации. Для этого используются разработанные специалистами РКСС функциональные системы (поддержки принятия решений, оповещения, мониторинга СМИ и социальных сетей). Система по своему замыслу способна обеспечивать решение вопросов безопасности как на отраслевом уровне, так и на территориальном.

Традиционно мы говорим о физической, антитеррористической безопасности и отдельно об информационной. На практике все эти направления тесно связаны. Люди живут одновременно в реальном и виртуальном мирах. Поэтому под словом «комплексный» мы понимаем в том числе и возможность решения одновременно задач физической и информационной безопасности.

В рамках системы КАСУБ специалистами РКСС был также создан мобильный ситуационно-аналитический центр (МСАЦ), который предназначен для информационной поддержки органов управления власти и бизнеса. МСАЦ разворачивается непосредственно в местах проведения работ и обеспечивает оперативное управление действиями сил и средств при локализации последствий аварий и чрезвычайных ситуаций. МСАЦ позволяет оперативно оценить реальное состояние различных объектов и предусмотреть тенденции развития нештатных ситуаций. Мобильный ситуационно-аналитический комплекс состоит из двух машин (штаб и машина связи). В штабной машине собраны мультимедийные технологии, которые помогают руководству принимать оперативные решения во время чрезвычайной ситуации и обеспечивают его всеми средствами связи с другими центрами реагирования. Машина связи содержит набор технических средств для подключения спутниковых, беспроводных и кабельных каналов, обеспечивая штабную машину вычислительными ресурсами, электропитанием и системой видеонаблюдения.

Заказчики-организации, с которыми мы работаем, имеют распределенную структуру. Их объекты расположены на всей территории России. И естественно, руководитель в момент кризисной ситуации хочет быть как можно ближе к объекту, максимально оперативно получать информацию, обеспечивать руководство соответствующими действиями и при этом находиться в комфортных условиях. Применение МСАЦ дает возможность руководителю корпорации, города или региона

Андрей Юрьевич Бадалов
Первый заместитель генерального директора Российской корпорации средств связи (РКСС)

Люди живут одновременно в реальном и виртуальном мирах. Поэтому под словом «комплексный» мы понимаем в том числе и возможность решения одновременно задач физической и информационной безопасности.

выезжать на место нештатной ситуации и там принимать оперативные решения. МСАЦ – это подвижные объекты, на которых созданы наилучшие условия для получения всей информации, ее отображения, обеспечения связи и комфортной работы руководителя.

Это направление неожиданно бурно развивается. Комплексное, комфортное, универсальное решение, созданное нами, отличается надежностью в кризисных ситуациях, а потому востребовано на рынке. Мы поставляем МСАЦ не только в Россию, но и зарубежные страны.

КАСУБ и МСАЦ – связанные системы. Когда человек работает в МСАЦ, он получает доступ к КАСУБ в любой точке. Могу привести пример: в ходе работы на АТЭС, который проходил во Владивостоке, руководство «Федеральной сетевой компании» работало активно в мобильном ситуационно-аналитическом центре. Мы получили благодарность за обеспечение этой работы.

– Какие технологические решения РККС предлагает государственной системе безопасности, инфраструктуре страны в целом?

– Это очень правильно – говорить об инфраструктуре страны в целом, обсуждая проблемы безопасности. Никакие решения в этой области не работают без развитых телекоммуникационных сетей. Сети должны иметь высокую пропускную способность и быть «доверенными». «Доверенные» сети максимально обеспечивают устойчивость функционирования, непрерывность и целостность передаваемой информации. Это относится не только к государственным сетям для секретных данных. Я говорю о тех сетях, которые не передают государственные тайны, но содержат критически важную информацию. Например, технологические сети для электроэнергетики. По ней идут сигналы для управления различными энергетическими объектами. Понятно, что эти сети тоже должны быть защищенными. А эта проблема сводится к проверке отсутствия в оборудовании связи недекларируемых возможностей. Если они есть, злоумышленник может отключить сеть через эти возможности. Наше оборудование решает данную задачу.

Мы считаем очень важным уделять внимание не только управлению безопасностью, но и технологическому управлению. Безопасностью технологического управления занимаются системы SCADA. Мы знаем много примеров по всему миру, в Иране и других странах, когда вирусы выводили из строя энергетические объекты. Это критично для страны в целом. Настало время инициировать соответствующие программы.

– Охарактеризуйте, пожалуйста, основных пользователей системю Для каких областей они могут предложить свои решения?

– Наши пользователи – от рядовых служащих на объекте до первых лиц крупнейших компаний и органов государственной власти. Поскольку наши системы комплексные, они обеспечивают работу на всех уровнях. Для обеспечения должного реагирования на местах желательно, чтобы у служащего была не только напечатанная на бумаге инструкция, а и программа на компьютере, которая заставит его следовать определенному алгоритму действий.

У нас большой опыт работы в энергетической отрасли, но те решения, которые мы предлагаем (КАСУБ, МСАЦ и другие), могут быть использованы на транспорте, в области безопасности спортивных мероприятий и т. д. Они универсальны и построены на единых методологических принципах.

– Вы упомянули спортивные мероприятия. Участвуете ли вы в проекте «Сочи-2014»?

– Да, мы принимаем непосредственное участие в этом проекте. Не всё, что касается обеспечения безопасности Сочи и систем управления проекта, ограничивается территорией города Сочи или даже Краснодарского края. Тут задействованы структуры по всей стране. Мы являемся разработчиками комплексных систем управления безопасности электросетевым комплексом Олимпийских игр и центров управления группы подстанций региона. То есть занимаемся еще и технологическим управлением, а не только безопасностью. Эта задача непростая, потому что создаются системы безопасности объектов разного уровня. Мы делаем энергетическую систему, кто-то – транспортную, кто-то – морскую... И основная задача, которая в ближайшее время стоит перед нами, – свести все системы в единый комплекс. Это сложная задача, потому что разработки всех систем относительно независимы.

– Какие шаги, Вы считаете, необходимо предпринять в области законодательства?

– Существуют международные стандарты. Россия в целом немного отстает в этом плане. Если в части информационной безопасности у нас более-менее всё в порядке, то стандарты обеспечения непрерывности бизнеса (а обеспечение безопасности информации – лишь средство обеспечения целевой функции бизнеса или любой другой организации) отстают. РККС занимается этим вопросом, создает концепции обеспечения непрерывности бизнеса. Банки, например, несколько впереди, потому что они вынуждены ориентироваться на мировое законодательство. Промышленность, критически важные структуры, тоже, думаю, скоро осознают, что надо соответствовать международным стандартам.

В законодательной области мы активно работаем и с Госдумой, и Советом Федерации. Мы видим, что наша законодательная база должна совершенствоваться, должно появиться понятие «доверенное оборудование». Это понятие довольно сложное. Необходимы стандарты непрерывности бизнеса, защиты критически важной инфраструктуры, соответствующие нормативы и законы. Работа ведется, но нужны совместные усилия государственных структур и коммерческих компаний.

– Расскажите, пожалуйста, о наработанном опыте международного сотрудничества. Что он дал компании?

– С самого начала своего создания РККС занимается взаимодействием с мировыми ИТ-лидерами. Изначально мы брали решение у вендора и предлагали российским заказчикам. Сейчас мы пришли к другой схеме взаимодействия: берём решение, адаптируем его, сертифицируем, обеспечиваем его «доверенность» и предлагаем клиентам.

Еще один вариант сотрудничества, который мы сегодня осуществляем, – это совместные научно-технические разработки. То есть мы в сотрудничестве с партнерами готовим продукт или решение. Так мы вышли на тот уровень, когда к нам относятся с большим уважением. Теперь ведущие компании приезжают к нам и предлагают сотрудничать с ними. Это как традиционные лидеры в области ИТ, так и специализированные компании, которые занимаются узкими проблемами безопасности в Европе, Израиле, США.

И третий вариант взаимодействия – когда у нас есть продукты и решения, которые мы можем предлагать на мировом рынке. Россия до сих пор обладает мощнейшим научно-техническим потенциалом. Но перед нами стоит непростая задача организовать людей и мотивировать их.

Примерно 90 % компаний в мире являются интеграторами, то есть они собирают чужие решения. Генераторов идей не так много, и мы предпочитаем работать именно с ними. В России довольно мощная компания разработчиков. И помимо бизнеса, нам просто творчески интересно работать с людьми, которые думают головой. В нашей стране была уникальная научная школа. И мы часто встречаем ее воспитанников по всему миру, когда начинаем искать самих разработчиков. Мы сейчас поставили себе задачу построения коллективов, пытаемся решить политическую задачу – вернуть «мозги» в Россию, мотивировать их для работы.

И тут я благодарен позиции государственной корпорации «Ростехнологии», она нам дает поддержку и уверенность. Мы чувствуем себя представителями серьезной государственной структуры.

– Как Вы оцениваете состояние отечественной ИТ-отрасли? Какие проблемы Вы видите, и как она должна развиваться дальше, на Ваш взгляд?

– Думаю, что состояние в целом хорошее, потому что это опять-таки связано с нашей историей, образованием и традициями. А среди проблем могу назвать тот факт, что мы мало занимаемся функциональной разработкой и описанием систем. Раньше у нас была школа «функциональщиков», то есть тех, кто занимался строением замысла системы. Она у нас потихоньку теряется, к сожалению. Это объективный процесс. Когда я заканчивал МИФИ, программирование было дорогим и трудоемким, потому что не было ПК. Надо было сначала думать, а потом уже нести перфокарту в большую машину. Поскольку технологии упростились, мы стали меньше думать перед тем, как делать. Поэтому РККС и стала заниматься онтологическим моделированием.

Второй момент – необходимость работы с пользователями. Создается огромное количество систем, их сдают пользователям, а те говорят: «Они нам не нужны». Айтишники стали диктовать свои позиции и делать так, как им удобно. А нужно идти от замысла.

Ирина Степеренкова
Татьяна Иванова