Конференция «Обеспечение информационной безопасности. Региональные аспекты»

11–15 сентября 2007 года в Сочи прошла VI Всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты», организатором которой выступает Академия информационных систем (АИС).

Традиционная встреча представителей рынка информационной безопасности собрала на Черноморском побережье России – площадке, которую АИС закрепила за собой 6 лет назад – около 350 специалистов.

Конференция прошла при поддержке компаний AMT Group, IBM, Microsoft, КРОК, Infotecs, ВНИИНС, Jet Infosystems, TrendMicro, Dr.Web, Oracle, SyTech, «Лаборатория Касперского» и «Элвис Плюс». Среди участников конференции были представители аппарата Совета безопасности РФ, сотрудники аппарата полномочных представителей Президента РФ в ряде федеральных округов, и администраций субъектов федерации, государственных ведомств, ИТ-компаний, банков и крупных коммерческих компаний, представляющих основные отрасли промышленности, такие как металлургия, энергетика, машиностроение, топливно-энергетических компаний, телекоммуникации, транспорт и другие.

В рамках пленарного заседания после обычных для такого рода мероприятий приветственных слов прозвучали порядка полутора десятков докладов, осветивших проблемы и тенденции их решения в сфере государственного регулирования вопросов информационной безопасности (ИБ), а также опыт работ в области безопасности информации в ряде субъектов федерации, ведомств и организаций. В последующие дни состоялись заседания нескольких секций и круглых столов. На них обсуждались проблемы нормативно-правового регулирования в области ИБ, практика обеспечения ИБ в государственных и коммерческих структурах, вопросы стандартизации ИБ в банковской сфере, проблемные аспекты подготовки специалистов в области технической защиты информации, теория и практика аналитической работы и др.

По традиции мы предоставляем слово действующим лицам сочинской конференции, предложив им высказать свое мнение как относительно всего мероприятия в целом, так и об отдельных его составляющих, в работе которых они принимали наиболее активное участие.

В. Г. Герасименко,
начальник института ГНИИИ ПТЗИ ФСТЭК России

Владимир Григорьевич, какова, на ваш взгляд, роль мероприятий, подобных VI Всероссийской конференции «Обеспечение информационной безопасности. Региональные аспекты», в разрешении проблемных вопросов государственного регулирования в области ИБ? В состоянии ли они оказывать реальное влияние на проблему?

Отношение к информационной безопасности у каждого участника процесса ее обеспечения свое. Государственные регуляторы вкладывают в это понятие, прежде всего, создание условий, позволяющих выполнить требования законодательства в этой области путем совершенствования нормативного правового регулирования. Производители средств и систем защиты информации и организации, оказывающие услуги в этой области, оценивают информационную безопасность с точки зрения рынка и возможности развертывания бизнеса на этом поле. В организациях, использующих и эксплуатирующих конкретные информационные технологии, отношение к ИБ еще более неоднозначное: для службы безопасности предприятия системы обеспечения ИБ – инструмент, позволяющий обеспечить конфиденциальность, доступность и целостность информации, для бизнес подразделений – мешающий работать фактор, для руководства – не всегда оправданная статья расходов.

Разноплановость интересов участников процесса обеспечения ИБ, стремление их всестороннего учета предопределяет ценность форумов, подобных прошедшей конференции. Встречи и обмен мнениями участников различных категорий полезны всем. Они позволяют государственным регуляторам глубже понять, как работает выстроенная ими система обеспечения ИБ по информации из низов, «с земли», ознакомить участников с новыми и перспективными направлениями нормативного правового регулирования в области ИБ, выслушать их проблемы, понять кто есть кто, в конце-концов: на таких форумах сразу видно, кто дело делает, а кто «щеки раздувает». Производителям и оказывающим услуги в области ИБ подобные конференции дают возможность не только себя показать и на других посмотреть, но и определить направления своего развития, скорректировать бизнес-планы, выдвинуть свои конкретные предложения. Для организаций, использующих и эксплуатирующих информационные технологии, участие в таких конференциях дает возможность понять, что день грядущий им готовит, услышать из первых уст что сделано, что делается и что будет делаться в области обеспечения ИБ, обменяться опытом.

Правоту моих слов и заинтересованность в подобных мероприятиях подтверждает растущее из года в год количество участников сочинского форума, ставшего уже традиционным.

Отвечая на вторую часть вашего вопроса, в состоянии ли мероприятия, подобные прошедшей конференции, оказывать реальное влияние на решение проблемных вопросов государственного регулирования в области ИБ, отвечу: безусловно. Приведу только два примера.

1. Анализ результатов обсуждения вопросов, включенных в программы всех шести конференций, их актуальности и глубины, позволил всем участниками процесса обеспечения ИБ, в том числе и государственным регуляторам, понять, что ИБ нужна не сама по себе – она является инструментом поддержки управленческих процессов органов власти или функционирования бизнеса, что формировать требования по ИБ необходимо исходя из задач конкретных органов исполнительной власти и организаций, учитывая при этом степень готовности их организационной инфраструктуры и соизмеряя затраты на обеспечение ИБ с рисками ее нарушения.

Тенденции изменения приоритетов в идеологии и организации работ в области ИБ, характеризующиеся развитием существующих, главным образом технических требований к системам защиты информации в направлении организационных требований к системам управления ИБ, явно просматриваются в последних нормативных правовых документах государственных регуляторов.

2. Предложения, прозвучавшие на Пятой всероссийской конференции в 2006 году, дали толчок к активизации работ по дальнейшему развитию системы подготовки кадров в области ИБ. В этой сфере на протяжении 2007 года ФСБ России и ФСТЭК России проведен целый комплекс конкретных мероприятий, о которых расскажет мой коллега.

Н. Т. Шевцов,
ведущий научный сотрудник ГНИИИ ПТЗИ ФСТЭК России, к. т. н., доцент, член-корреспондент РАЕН

Пожалуй, эта тема потребует отдельного и более обстоятельного разговора, нежели предполагается форматом данного репортажа. Скажу лишь, что участники впервые организованной на сочинской конференции секции «Проблемные вопросы подготовки специалистов в области технической защиты информации» одобрили усилия ФСТЭК России и ФСБ России по методическому руководству подготовкой кадров в области ИБ. Говоря же о ее работе в целом, отмечу, что секция № 8 вобрала

в себя большинство проблемных вопросов по совершенствованию методического руководства подготовкой кадров в области информационной безопасности.

Работа секции проходила под руководством заместителя начальника Академии ФСБ России Андрея Петровича Коваленко – председателя учебно-методического объединения высших учебных заведений страны по информационной безопасности и Евгения Анатольевича Беляева – советника директора ФСТЭК России.

В организации и проведении секции приняли участие более 40 специалистов из ведущих образовательных и научных организаций страны, а также представители бизнес-сообществ.

Прозвучавшие на секции выступления были посвящены проблемам:

- организации межведомственной системы подготовки кадров в области защиты информации;
- совершенствования системы дополнительного профессионального образования специалистов по защите информации;
- разработки квалификационных требований к специалистам по защите информации;
- разработки типовых образовательных программ дополнительного профессионального образования;
- сотрудничества образовательных учреждений и бизнес-сообществ в области подготовки специалистов по информационной безопасности;
- менеджмента информационной безопасности.

Кроме того, был обсужден опыт подготовки кадров в области информационной безопасности различных вузов страны, в том числе проблемы дистанционного обучения специалистов по защите информации на базе современных обучающих технологий.

Высказав одобрение усилиям ФСТЭК России и ФСБ России в деле методического руководства подготовкой кадров в области ИБ, секция приняла ряд рекомендаций и пожеланий.

1. Всем заинтересованным сторонам провести необходимые мероприятия по ускорению внедрения в учебный процесс научно-технической продукции, разрабатываемой по заказам ФСТЭК России, в частности Типовые образовательные (72–100 часов) программы дополнительного профессионального образования (ДПО), Типовые лабораторные практикумы для обеспечения общепрофессиональных дисциплин и дисциплин специализации, а также по внедрению в практику работы образовательных учреждений квалификационных требований к специалистам по защите информации.

2. Разработать предложения по совершенствованию механизма формирования государственного заказа (целевой подготовки) имеющим государственную аккредитацию образовательным учреждениям на профессиональную подготовку и ДПО специалистов для государственной системы защиты информации.

3. Подготовить предложения по развитию нормативной базы по закреплению выпускников вузов, обучаемых в рамках государственного заказа, в государственной системе защиты информации.

4. ФСТЭК России ускорить внедрение отечественной отраслевой системы аттестации специалистов по защите информации с введением обязательного периодического профессионального повышения квалификации.

5. Установить, что важнейшей задачей государственной системы защиты информации является кадровое обеспечение учебного процесса профессиональной подготовки, профессиональной переподготовки и профессионального повышения квалификации специалистов по защите информации. Одним из путей реализации является активное участие вузов, а также головных научно-исследовательских организаций (НИО) по проблемам защиты информации в развитии и реализации системы ДПО по защите информации и обеспечению безопасности информации в КСИИ государства.

6. Рекомендовать головным НИО по проблемам защиты информации создать научно-образовательные комплексы по изучению проблем информационной безопасности, профессиональной подготовке и ДПО кадров в области информационной безопасности, используя опыт сети региональных учебно-научных центров высшей школы по данным проблемам.

7. Привлечь специалистов бизнес-сообществ к разработке квалификационных характеристик должностей руководителей и специалистов по защите информации, государственных образовательных стандартов и профессиональных компетенций выпускников вузов, в том числе на условиях софинансирования.

8. Расширить в образовательном процессе подготовки специалистов по защите информации воспитательные аспекты и морально-этические нормы «защитников информации», которые включить для изучения в блок гуманитарных и социально-экономических дисциплин государственных образовательных стандартов направления по образованию «Информационная безопасность».

В. А. Бурмин,
заместитель начальника по развитию ГНИИИ ПТЗИ ФСТЭК России

Владимир Алексеевич, не могли бы вы очертить круг основных проблем, рассмотренных в ходе работы секции «Стандарты информационной безопасности в банковской сфере».

Как вы оцениваете сложившееся на сегодня положение в области стандартизации национальной банковской системы и в чем видите перспективы ее развития?

Говорить об актуальности проблемы обеспечения безопасности информации в такой стратегической отрасли экономики России, как кре-

дитно-финансовая сфера, в настоящее время излишне. В то же время насущной необходимостью являются новые подходы, средства, методы и технологии защиты информации. Понимание этого позволило собрать в Сочи в рамках работы секции «Стандарты информационной безопасности в банковской сфере» представительный форум более чем из 40 специалистов – практиков кредитно-финансовой сферы, понимающих проблемы информационной безопасности и непосредственным образом участвующих в их реализации.

С участием разработчиков банковских стандартов рассмотрен и обсужден достаточно широкий круг вопросов от проблем нормативного правового регулирования в области информационной безопасности до опыта их решения на основе внедрения стандартов информационной безопасности в Банке России. Участники секции поделились практическими аспектами внедрения стандартов Банка (А. Н. Велигура, председатель Комитета по информационной безопасности Ассоциации российских банков), опытом проведения работ по оценке соответствия информационной безопасности кредитных организаций требованиям стандартов, обсудили особенности проведения самооценки информационной безопасности (С. Л. Зефиров, заместитель научного директора ООО НПФ «Кристалл»). Не обошли вниманием и практические решения в области совершенствования внутренних документов по обеспечению информационной безопасности кредитной организации (В. Б. Голованов, ответственный секретарь ПК № 3 ТК362 «Защита информации», заместитель научного директора НПФ «Кристалл»). Большой интерес аудитории вызвали доклады представителей ведущих мировых аудиторских фирм об особенностях проведения аудита информационной безопасности на основе международной практики и в соответствии с рекомендациями стандартов Банка России (А. В. Дроздов, вице-президент российского отделения ISACA, старший менеджер KPMG, Н. А. Самодаев, CISA, MBCI, старший менеджер «Эрнст & Янг»). Интересные результаты совместных исследований ABISS и Infowatch привел в своем докладе «Стандарт Банка России по ИТ-безопасности 2007: внедрять или не внедрять» А. А. Доля, руководитель аналитического центра Infowatch. В рамках работы секции проведено седьмое заседание Сообщества пользователей стандартов Банка России по обеспечению информационной безопасности организаций банковской системы РФ ABISS (П. В. Гениевский, секретарь Совета Сообщества ABISS, исполнительный директор ЗАО «Метробанк»).

На мой взгляд, основная задача секции – проведение разъяснительной работы об актуальности, полезности и необходимости стандартизации и унификации работ по информационной безопасности в кредитно-финансовой сфере – выполнена.

Основные выводы из выступлений участников секции, в целом, сводятся к следующему:

- в основе большинства выявленных инцидентов информационной безопасности в организациях кредитно-финансовой сферы лежит отсутствие, несовершенство или несоблюдение регламентации деятельности в этой области. В силу этого стандарты Банка России – один из наиболее эффективных инструментов повышения уровня информационной безопасности, предполагающих усиление механизмов контроля, мониторинга и аудита;
- настоящий этап стандартизации в области информационной безопасности Банка России характеризуется развитием существующих требований по защите информации от чисто технических аспектов в направлении специфики управления, аудита и оценки информационной безопасности;
- требования и рекомендации стандартов Банка России, не претендуя на статус нормативных документов в области обеспечения безопасности информации, составляющей государственную тайну, а также информации ограниченного доступа, относимой в соответствии с законодательством Российской Федерации к охраняемой, позволяют грамотно и обоснованно организовать обеспечение безопасности информации, обладателем которой является кредитно-финансовая организация.

Говоря об оценке сложившегося положения в области стандартизации национальной банковской системы, необходимо отметить, что Банк России сегодня является пионером создания системы стандартов организации в области информационной безопасности, работу в этом направлении он проводит крайне взвешенно и последовательно, активно привлекая к ней ПК №3 технического комитета ТК-362 «Защита информации». При этом основные направления развития стандартизации для организаций национальной банковской системы ориентированы, прежде всего, на развитие в практической плоскости положений стандарта СТО БР ИББС-1.0 для Банка России и кредитных организаций и должны обеспечивать методическую поддержку для разработки и совершенствования политики информационной безопасности, развертывания и эксплуатации системы управления информационной безопасностью, определения уровня зрелости процессов управления на основе результатов аудита и самооценки информационной безопасности организации.

П. В. Гениевский,
исполнительный директор ЗАО «Метробанк»

Павел Владимирович, как вы считаете, может ли опыт внедрения отраслевых стандартов ИБ

в банковской системе России рассматриваться как образец решения проблем нормативно-правового регулирования в данной области для других отраслей?

На счет того, образец это или не образец, судить сложно, скорее всего – это один из хороших примеров, которому могут следовать и уже следуют другие отрасли. И это нормальное явление. Например, Стандарт Банка России по информационной безопасности тоже не создавался «с нуля», он разрабатывался на основе уже существующих хороших практик, изложенных в международных стандартах, а создавая сообщество ABISS, мы также предварительно изучали деятельность подобных европейских сообществ.

В. Ю. Скиба,
начальник отдела информационной безопасности Федеральной таможенной службы

Владимир Юрьевич, различаются ли взгляды на проблематику нормативно-правового регулирования поставщиков и потребителей решений в области ИБ? Если да, то насколько существенны эти различия и существует ли необходимость в сближении этих позиций?

На мой взгляд, более правильно говорить не столько о различиях во взглядах поставщиков и потребителей решений в области информационной безопасности, сколько о проблемах в области нормативно-правовом регулировании обеспечения информационной безопасности. В зависимости от проблемы в области нормативно-правового регулирования (международный информационный обмен, электронная торговля, защита персональных данных и т. д. и т. п.) взгляды поставщиков и потребителей решений в области информационной безопасности могут либо практически не отличаться, либо отличаться просто диаметрально. Приведу несколько примеров.

Пример первый. Имеются проблемы в нормативно-правовом регулировании использования средств криптографической защиты информации в телекоммуникационном оборудовании импортного производства. Поставщики считают, что для продвижения решений достаточно использовать сертифицированные программные криптоядра, в то же время, руководствуясь ПКЗ-2005, заказчики считают необходимыми дополнительные исследования и согласования с ФСБ России.

Пример второй. Отсутствует нормативно-правовое регулирование применения средств электронной цифровой подписи при международном информационном взаимодействии. И поставщики, и потребители решений в области обеспечения информационной безопасности заинтересованы в принятии соответствующих правовых актов. При этом их позиции хоть и отличаются в частностях, но все-таки схожи в главном: необходимо создание процедур признания международных стандартов в РФ и продвижение отечественных стандартов в международное сообщество.

В. Н. Мамыкин,
директор по информационной безопасности, Microsoft Corp.

Владимир Николаевич, корпорацию Microsoft всегда можно видеть в числе наиболее активных участников конференций по информационной безопасности. Это, что называется, имиджевые акции или же компания действительно считает для себя важным высказать свое мнение по обсуждаемым на них вопросам и выслушать мнение других?

Для Microsoft участие в конференциях важно, прежде всего, потому, что именно здесь можно выслушать независимые мнения участников рынка. Ведь только обратная связь с пользователями позволяет объективно судить о качестве собственных продуктов. Конечно, мы используем трибуну конференций и для объяснения нашей стратегии, и для рассказа о новых качествах наших продуктов. Кроме того, на конференциях всегда можно почерпнуть интересную информацию о перспективах развития рынка, о применении законодательства и о разработках других игроков рынка. Ведь без наличия конкурентов, а у нас их достаточно, невозможно создать хорошие продукты.

На пленарном заседании вы выступили с докладом «Новый пласт информационной безопасности Microsoft». Звучит интригующе. Не могли бы вы изложить его основные тезисы для тех, кто не имел возможности его прослушать.

В докладе я сфокусировал внимание на новом направлении в обеспечении информационной безопасности, которому в Microsoft в последнее время уделяется все больше внимания. Речь идет о линейке продуктов Forefront, которая специально предназначена для обеспечения информационной безопасности. Если ранее мы все средства безопасности интегрировали внутри своих базовых продуктов – операционных систем, баз данных, то теперь настало время, когда наши разработки в области информационной безопасности выходят на рынок в виде самостоятельных продуктов.

Прежде всего, это относящиеся к линейке продуктов Forefront межсетевой экран ISA Server 2006, уже сертифицированный ФСТЭК по

Ответственный секретарь Оргкомитета Всероссийской конференции «Обеспечение информационной безопасности. Региональные аспекты» Юрий Малинин проинформировал нашу редакцию о дальнейших планах Академии Информационных Систем. В частности, 25–27 октября 2007 года на III Международной научной конференции по проблемам безопасности и противодействия терроризму МАБИТ 2007 будет продолжено обсуждение затронутых в Сочи вопросов. Кроме того, проблемы информационной безопасности как составной части управления непрерывностью бизнеса и восстановления жизненно важных систем после катастроф Академия Информационных Систем предлагает к обсуждению на II Международном научно-практическом семинаре «Информационная безопасность в контексте проблем непрерывности бизнеса», который состоится в апреле 2008 года в Германии (Гармиш-Патеркирхен, Мюнхен) при поддержке Аппарата Совета Безопасности РФ и при участии Европейского Центра им. Джорджа К. Маршалла, Университета Кембриджа, Университета штата Нью-Йорк, программы «Россия – НАТО», Института проблем информационной безопасности МГУ им. М. В. Ломоносова и BCI.

3-му классу, что выше других аналогов, и антивирусные продукты Forefront для рабочих станций (Forefront Client), для почтовых серверов Exchange и серверов документооборота Sharepoint. Особенность этих антивирусов состоит в том, что наряду с собственным антивирусом Microsoft (а он недавно успешно прошел престижные тесты VirusBulletin100, выловив 100 % вирусов, чего не смогли сделать продукты известнейшей российской компании), Forefront для серверов работает одновременно с восемью антивирусными движками от других производителей, в том числе и от российской Лаборатории Касперского. Это значительно повышает качество защиты от вирусов и этого не умеет делать никакой другой продукт в мире. Кроме того, эти антивирусы максимально интегрированы в информационную инфраструктуру предприятия (active directory, применение корпоративных политик безопасности), что делает управление ими простым в организациях любого размера. В ближайшие дни заканчивается сертификация всех этих антивирусных продуктов.

Кроме того, в докладе я анонсировал появление на рынке еще одной компании, специализирующейся на поставках сертифицированных продуктов, – ООО «Сертифицированные информационные системы» (www.c-i-s.ru), которая вместе с компанией «Алтэкс-строй-2002» под руководством ФГУП «Предприятие по поставкам продукции Управления делами Президента РФ» занимается распространением сертифицированных продуктов Microsoft. Так что нашим клиентам теперь станет проще и удобнее выбирать поставщика.

И. А. Шамилов,
заместитель генерального директора ОАО «КАМАЗ» по безопасности

Ильдар Асхатович, своих представителей ОАО «КАМАЗ» направило на данную конференцию впервые. Что побудило компанию принять такое решение?

Как уже отмечалось в докладе ОАО «КАМАЗ», прозвучавшем на этой конференции, до 2006 года вопросы безопасности рассматривались нами в большей степени в ракурсе проведения контрольных мероприятий по соблюдению внутриобъектового режима ОАО «КАМАЗ».

В 2006 году Генеральным директором ОАО «КАМАЗ» было принято решение о модернизации существующих систем информатизации, в том числе о создании комплексной системы информационной безопасности предприятия.

На наш взгляд, «КАМАЗ» является по-своему уникальным предприятием машиностроительной промышленности страны, поэтому решение вопросов, связанных с обеспечением информационной безопасности, должно строиться с использованием самых передовых и современных технологий. Мы также осознаем необходимость получения и анализа уже накопленного опыта экспертными организациями и специалистами в этой области для его последующего практического применения на своем предприятии.

Ежегодная конференция, проходящая в Сочи, показала нам именно тот результат, который мы и ожидали. Надеемся, что здесь же в 2008 году ОАО «КАМАЗ» сможет достойно продемонстрировать реализацию опыта, полученного нами в ходе работы нынешней конференции.

А. Н. Антоненков,
главный специалист по информационной безопасности ОАО «КАМАЗ»

Александр Николаевич, насколько полезным для вас оказалось первое посещение конференции? Свежий взгляд всегда интересен. Каковы ваши общие впечатления о конференции?

О всероссийской конференции в Сочи, посвященной вопросам информационной безопасности, мне было известно еще в 2003 году, со времени работы в ОАО «АКИБАНК» в должности специалиста по информационной безопасности. По роду деятельности я часто посещал курсы обучения и переподготовки, семинары, выставки, проводимые в Москве, где и почерпнул информацию о конференции.

Впервые же осуществить свое стремление попасть на нее мне удалось благодаря организаторам конференции – «Академии информационных систем», которые активно помогали нам в течение этого года проводить обучение руководителей и специалистов ОАО «КАМАЗ» в области обеспечения информационной безопасности. Наряду с этим необходимо подчеркнуть всестороннюю поддержку и понимание руководством ОАО «КАМАЗ» масштабности и значимости работ, которые необходимо проводить предприятию для построения комплексной системы информационной безопасности.

Основное и наиболее значимое впечатление от участия в конференции, с которым я возвращаюсь на «КАМАЗ», это присущая сочинской конференции легкость, с которой в простой и неформальной обстановке приобретаются новые деловые контакты и решаются многие вопросы. Также хочется отметить очень высокий профессиональный уровень и компетенцию специалистов, присутствующих на конференции и принимающих участие в работе секций и круглых столов.

К примеру, для решения вопроса об обязательном проведении внутреннего аудита объектов информатизации ОАО «КАМАЗ» в ходе беседы с представителем компании IBM удалось найти приемлемое решение, которое позволит повысить привлекательность акций предприятия при их размещении на международной бирже в 2008 году.

Т. М. Бортащенок,
начальник Удостоверяющего центра ФГУП ГНИВЦ ФНС России

Татьяна Михайловна, вы не в первый раз принимаете участие в работе конференции, какие секции Вас, как начальника УЦ, интересуют в первую очередь?

Да, я уже в третий раз принимаю участие в этой конференции.

В первую очередь интересует все, что связано с нормативно-правовыми актами. К сожалению, закон «Об электронной цифровой подписи» 2002 года – фактически единственный, где определен статус удостоверяющих центров, но в нем мало конкретики. Поэтому приходится собирать всю информацию, имеющую отношение к работе удостоверяющих центров, чтобы соответствовать текущему моменту – ведь за пять лет многое изменилось.

Кроме того, есть еще много вопросов, которые находят свое освещение на конференции и которые тем или иным образом необходимы в работе.

Не считаете ли вы, что, учитывая растущий интерес к работе удостоверяющих центров, можно было бы порекомендовать организаторам включение в план следующей конференции отдельной секции, посвященной этому вопросу?

Хочется верить, что организаторы услышат эту рекомендацию. Есть, конечно, и другие конференции и форумы, например, PKI-конференция в Санкт-Петербурге, но секция в рамках сочинской конференции была бы совсем не лишней для развития удостоверяющих центров в России.

По итогам сказанного выше можно констатировать, что VI Всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты» помимо интересной и насыщенной программы предлагает своим участникам эффективную площадку для ведения переговоров и предоставляет широкие возможности по поиску потенциальных партнеров среди участников конференции!

О значении подобных площадок для общения специалистов немало говорилось и в кулуарах конференции – именно за рамками официальных мероприятий происходит основной обмен мнениями между всеми участниками.

Более того, в нынешнем году организационный комитет пошел в этом направлении еще дальше, предложив участникам новые возможности и инструменты для повышения эффективности своего участия в конференции. Им была введена новая услуга – «Организация деловых встреч», в результате реализации которой каждый участник мог пригласить на деловую встречу интересующего его делегата для обсуждения насущных вопросов.

В рамках мероприятия состоялось торжественное вручение учрежденной в 2006 году организационным комитетом конференции премии за вклад в развитие информационной безопасности Российской Федерации, которой отмечаются лица и компании, которые своей деятельностью или своими разработками внесли существенный и признаваемый специалистами вклад в развитие рынка безопасности в России.

Не забыли организаторы и о досуге: впервые среди участников прошел теннисный турнир с вручением победителю переходящего кубка.