IX Всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты»

С 7 по 11 сентября в сочинском отеле «Рэдиссон САС Лазурная» состоялась IX Всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты». Традиционно открывая начало делового сезона в сентябре, конференция представляет собой площадку, в рамках которой рассматриваются самые акту альные и насущные вопросы в области информационной безопасности, а кроме того, подводятся итоги предыду щего года и озвучиваются перспективные планы. Эта особенность – задавать ориентиры – своеобразная визит ная карточка мероприятия.

На этот раз в Сочи съехались более 270 представителей федеральных органов исполнительной власти России, министерств и ведомств, администраций городов, краев и областей субъектов Российской Федерации, отечественных предприятий различных отраслей промышленности, финансовых и кредитных учреждений, ведущих компаний-разработчиков систем и средств информационной безопасности, а также организаций, осуществляющих свою деятельность в области защиты информации, ведущих телекоммуникационных компаний, операторов связи.

Все эти люди – высококвалифицированные специалисты в сфере ИБ – собрались вместе для обсуждения тем, которые на данный момент являются высокоприоритетными для их профессиональной деятельности. При этом можно отметить, что высокий статус участников в очередной раз подтвердил важность и значимость данного мероприятия для ИТ-рынка, а особенно – для сегмента ИБ.

Ни одна поднятая тема не осталась без внимания и без жаркой дискуссии. Будь то вопросы защиты персональных данных и обеспечения информационной безопасности в телекоммуникационном секторе, проблемы развития программы «Электронное правительство» для оказания государственных и муниципальных услуг в электронном виде, подводные камни при обеспечении безопасности облачных вычислений и создании свободного ПО – любое секционное заседание было интересным, насыщенным, активным, эмоциональным. И каждый раз участники старались прийти к консенсусу и единому пониманию ситуации, договориться о взаимных действиях – это особенно чувствовалось в диалогах между представителями регулирующих органов и бизнеса. А это не может не радовать: одной из основных целей конференции всегда было налаживание эффективного взаимодействия министерств, федеральных ведомств, администраций субъектов Российской Федерации и бизнес-структур на благо развития информационных технологий и обеспечения информационной безопасности РФ.

Впервые в рамках конференции «Обеспечение информационной безопасности. Региональные аспекты» прошли международные студенческие соревнования Sochi CTF 2010. В последние годы в мире и России развивается международное движение, получившее название White Hackers (Белые хакеры), которое базируется на студенческих командах ведущих университетов, развивающих исследования и подготовку в области современных информационных технологий. Соревнования проходят по международным правилам Cupture The Flag – CTF (Захвати флаг), согласно которым противоборствующим сторонам необходимо обнаружить и устранить уязвимости собственной сети, одновременно успев воспользоваться уязвимостями чужих для захвата «флагов» команд-соперников. Отметим, что подобные соревнования уже становятся доброй традицией для мероприятий, организуемых Академией информационных систем, – аналогичные состязания состоялись во время конференции «РусКрипто-2010» в апреле текущего года.

Далее, подробнее об этом и других, не менее интересных событиях

★ Сочи–2010 ★

конференции расскажут ее непосредственные участники.

Члены оргкомитета: Ю. В. Малинин, В. И. Комогоров, А. П. Баранов, В. А. Смирнов

Н. Е. Конкин, *председатель совета директоров ООО «КАБЕСТ»*

В этом году конференция «Информационная безопасность. Региональные аспекты» проводилась уже в 9-й раз. И это как нельзя лучше свидетельствует о ее важности и востребованности среди специалистов в области ИБ. То, что конференция традиционно проводится в Сочи, имеет символическое значение, подчеркивающее роль этого региона в укреплении престижа и авторитета нашей страны в связи с предстоящими зимними Олимпийскими играми 2014 года.

Важное значение этой конференции заключается в том, что она дает возможность широкого общения как руководителей регулирующих органов в области информационной безопасности (ФСБ России, ФСТЭК России, Минкомсвязи России и Роскомнадзора) и регионов России, так и представителей крупных компаний, работающих на рынке ИБ. Она позволяет в ходе пленарных и секционных мероприятий, а также в свободной неформальной обстановке взвешено обсудить текущее состояние и перспективы различных направлений ИБ, пути решения актуальных задач в этой весьма важной для страны области. Подчеркну, именно в ходе неформальных бесед становятся более очевидными потребности и проблемы, имеющиеся на региональном уровне, быстрее намечаются пути и подходы к их решению.

Особенно важным является то, что конференция обеспечивает обратную связь между разработчиками законодательной и нормативной правовой базы в области информационной безопасности и, если можно так сказать, «потребителями» этой базы – регионами и крупными предприятиями, а также компаниями, работающими на рынке ИБ. В частности, на этой конференции было сделано довольно много конкретных предложений по совершенствованию № 152-ФЗ «О персональных данных» и нормативных правовых актов по защите персональных данных, которые, смею надеяться, будут учтены в ходе работы законодателей и регуляторов в этой области.

Особенностью прошедшей конференции явилось то, что впервые на ней были подняты вопросы комплексного обеспечения всех видов безопасности на уровне региона, города, крупного предприятия, в том числе, разумеется, и задач обеспечения ИБ.

Большой интерес, как обычно, вызвало пленарное заседание, на котором были представлены весьма интересные доклады представителей регулирующих органов, позволяющие оценить перспективы развития направления информационной безопасности в стране.

Хотелось бы отметить весьма интересные выступления на многих секциях, таких как «Нормативно-правовое регулирование в области защиты персональных данных» (это на сегодняшний день одно из самых актуальных направлений защиты информации в связи с вступлением с 1 января 2011 года в полную силу № 152-ФЗ «О персональных данных»), «Нормативное регулирование защиты информации в государственных информационных системах» и «Обеспечение информационной безопасности при предоставлении государственных услуг в электронном виде» (государственные и региональные органы власти являются одними из основных Заказчиков ООО «КАБЕСТ»), «Образование в области информационной безопасности» (в настоящее время остро встала проблема нехватки специалистов в области ИБ). Особенно следует отметить блестящее руководство последней Л. Г. Осовецким.

Наконец, мне бы хотелось отметить большой труд, вложенный в подготовку и проведение конференции ее бессменными организаторами – коллективом Академии Информационных Систем и ее руководителем – Ю. В. Малининым и пожелать им дальнейших творческих успехов.

А. Г. Сабанов, *заместитель генерального директора ЗАО «Аладдин Р. Д.»*

На прошедшей конференции отмечу два наиболее значимых, на мой взгляд, события, непосредственно связанных с актуальными изменениями в нашем стремительно изменяющемся законодательстве.

Впервые в 2010 году на трибуне ИБ-мероприятий можно было увидеть представителей Ростелекома и получить актуальную информацию по состоянию вопросов ИБ в строящемся на наших глазах «Электронном правительстве», как говорится, из первых рук. На пленарном заседании выступал директор проекта «Электронное правительство» ОАО «Ростелеком» В. С. Зубаха, а в секционном заседании «Обеспечение ИБ при предоставлении госуслуг в электронном виде. Социальные карты. Вопросы защищенного ЭДО» – начальник отдела ИБ-систем проекта «Электронное правительство» ОАО «Ростелеком» А. В. Платицын. Из их выступлений понятно,

Оживленная работа и дискуссии на профессиональные темы не прекращалась даже в перерывах

что теперь вопросы ИБ поставлены во главу угла и включены во все подсистемы. Для успешного развития проекта «Электронное правительство» также необходимо создание инфраструктуры государственного пространства доверия, организации защищенного документооборота как основы для оказания госуслуг в электронном виде, налаживание межведомственного обмена защищенными сообщениями и других сервисов безопасности.

Также впервые состоялся открытый разговор об основах и возможных путях создания единой универсальной смарт-карты. Вопрос в том, сколько чипов надо размещать на универсальную электронную карту. Для пояснения рассмотрим один аспект, сразу же приходящий на ум. Технически на одной смарт-карте кроме фотографии и ФИО владельца легко можно разместить два чипа (для платежных приложений и для организации защищенного доступа к информационным ресурсам – со строгой аутентификацией), одну или две RFID-метки для автоматической идентификации и оплаты муниципальных (например, транспортных услуг). Также на этой карте можно разместить индивидуальный штрих-код и уже давно известную пользователям банковских приложений магнитную полосу. Однако себестоимость такой карты, а главное, стоимость ее перевыпуска в случае потери оригинала будет весьма существенной, поскольку новую карту надо будет «научить идентифицироваться и аутентифицироваться» сразу в нескольких пока не интегрированных разнородных системах или хранить образы выданных идентификационных и аутентификационных данных в одном месте – там, где выдавали оригинал. Как оно будет защищено? Сколько таких защищенных хранилищ надо создать? Как будет организован доступ к столь чувствительной к действиям мошенников информации? Кто сможет гарантировать, что эта информация не попадет к злоумышленникам и на чем будут основаны такие гарантии? Вопросы можно продолжить. Кроме того, для такой «навороченной» карты на сегодня отсутствует необходимая инфраструктура и создать ее за несколько месяцев весьма непросто.

Что делать? Для того чтобы снять часть заданных вопросов, одним из возможных решений может быть разработка и внедрение глобальной защищенной системы управления жизненным циклом выданных универсальных электронных карт с развитой инфраструктурой и сервисами. Впрочем, возможность реализации такой системы на 141 миллион граждан – это, скорее, из области фантастики.

Другим из возможных путей может стать тактика «съедания слона по частям». Эту до гениальности простую и более легко осуществимую на практике тактику высказал на сочинской конференции старший вице-президент ЗАО «ТрансТелеКом», руководитель экспертно-консультационного совета по Национальной системе платежных карт РСПП В. А. Пярин. Для постепенного ввода и развития не только услуги, но и необходимой для ее существования инфраструктуры можно предложить ввод отдельно взятой транспортной карты, медицинской карты, карты доступа к информационным ресурсам, платежным услугам и т. д., причем делать это параллельно для ускорения и упрощения задачи. Добавим, что при этом можно разделить вопросы аутентификации и электронной подписи (генерировать внутри чипа карты две ключевые пары и держать на смарт-карте два сертификата: один – для доступа, второй – для подписи). Для выпуска сертификатов доступа в подавляющем большинстве случаев будут применимы сертифицированные решения по требованиям ФСТЭК России для информационных систем до класса 1г включительно, для усиленной электронной подписи – сертифицированные по требованиям ФСБ России решения для выпуска квалифицированных сертификатов. Когда системы будут отлажены и необходимые отраслевые инфраструктуры построены, можно будет вернуться к вопросу выпуска единой карты.

Понятно, что строгая двухфакторная аутентификация потребуется не для всех обращений граждан. Например, для решения вопросов информирования (первый этап системного проекта построения электронного правительства) будет достаточно идентификации. Однако для информационного обмена ответственных госслужащих с гражданами по запросам, имеющим юридические последствия (например, оформления прав собственности), надо вводить в регламент обязательность использования двухфакторной строгой взаимной аутентификации.

Г. В. Емельянов, *председатель совета МОО «Ассоциация защиты информации»*

Конференция «Обеспечение информационной безопасности. Региональные аспекты» всегда привлекает, во-первых, актуальностью тематики и очень демократичным форматом обсуждений и дискуссий, во-вторых, активным участием в ее работе наших уважаемых «регуляторов» и высоким профессиональным и административным уровнем их представительства. Вот и на этот раз участники конференции смогли узнать из первых уст интересующие их подробности относительно обеспечения ИБ важнейших российских ИТ-проектов, в частности по «Электронному правительству», по региональным приемным Президента РФ. Последняя тема была прекрасно изложена первым заместителем Центра ФСБ России А. П. Барановым.

Примечательно, что организаторы прибегают к помощи сторонних организаций при формировании программы конференции. Так, я поддерживал образовательную тематику и тему обеспечения ИБ сочинской Олимпиады, как очень важную составляющую комплексной безопасности этого важнейшего для страны мероприятия.

Участники конференции в Конгресс Холле отеля «Рэдиссон Лазурная»

К сожалению, в этот раз организаторам не удалось привлечь репрезентативный пул участников. В частности, не было представителей важнейшей в этой проблематике структуры – УМО по проблемам информационной безопасности при Министерстве образования. Однако и наличествующим составом был поднят важный вопрос о более представительном участии России в мировом движении «Белых хакеров», имеющем серьезный интеллектуальный потенциал в области исследования проблем обеспечения ИБ. Более подробно об этом мог бы рассказать руководитель секции по образованию и большой энтузиаст развития этого направления Л. Г. Осовецкий. Со своей же стороны я готов оказать организаторам конференции всестороннюю помощь в решении проблемы более широкого представительства на образовательной секции.

О. Н. Кузьмин, *директор департамента информационной безопасности ЗАО «Ай-Теко»*

В данной конференции меня привлекает, прежде всего, возможность одновременного общения с представителями различных государственных структур, вендоров, заказчиков, причем, и это особенно важно, неформального общения. Дело в том, что в ходе плановых выступлений, жестко ограниченных регламентом, докладчики порой не успевают в должной мере донести до слушателей главные мысли по заявленной теме или же в полной мере их раскрыть. В результате у слушателей может сложиться впечатление, что ничего нового докладчик по сути поднятых им вопросов и не сказал. В ходе неформального общения специалист, выступивший ранее с докладом, уже не волнуясь и не торопясь, может продолжить изложение поднятой им проблемы. Это достаточно важно для понимания практической стороны вопросов информационной безопасности и связанного с этой сферой бизнеса. Кроме того, меня интересует личное мнение участников конференции по различным вопросам ИБ, которое не всегда может быть высказано ими с трибуны, но вполне выражается в ходе обсуждения в перерывах официальной части мероприятия.

На этот раз основное внимание участников конференции, на мой взгляд, привлекли секции «Нормативно-правовое регулирование в области защиты персональных данных» и «Нормативное регулирование защиты информации в государственных информационных системах».

Их работу я бы оценил на твердую четверку (по пятибалльной шкале). Если говорить о первой, то поставить максимальную оценку не позволяет незаслуженно, как мне представляется, оставшийся за бортом обсуждения аспект неавтоматизированной обработки персональных данных. Все прозвучавшие в ходе секции выступления были достаточно интересными, но затрагивали лишь проблемы автоматизированной обработки персональных данных и их защиты в ИСПДн. Ни один докладчик не остановился подробно на правовых составляющих 152-ФЗ «О персональных данных» и, соответственно, на практических проблемах операторов ПДн с ними связанных.

Применительно ко второй из упомянутых мною секций балл снижен ввиду некоторой однообразности докладов и отсутствия у докладчиков каких-либо новых конструктивных предложений по раскрываемым ими темам и связанным с ними проблемным вопросам.

В. Г. Швед, *советник генерального директора ООО «НПК «СпецПроект»*

Первым делом хотелось бы отметить высокий профессионализм участников конференции, глубокое знание ими проблем в области информационной безопасности и основных путей их решения. Главный ее плюс состоит, на мой взгляд, в том, что в выступлениях участников прозвучали конкретные рекомендации по модернизации процессов обеспечения информационной безопасности как в организационной, так и технической сферах. Их реализация на практике позволит существенно обезопасить информационные процессы в органах власти, в государственных и коммерческих организациях.

Так, достаточно перспективным мне представляется новое направление, представленное на конференции, – «белое» хакерство. Связанные с ним вопросы были рассмотрены не только теоретически, но и практически с привлечением студентов из России, стран ближнего и дальнего зарубежья.

Весьма актуальным является своевременная постановка задач обеспечения информационной безопасности в ходе реализации облачных вычислений. Особенно интересен в ходе работы соответствующей секции был доклад руководителя комитета по вопросам ИБ ЗАО «Лаборатория СКАТ» А. В. Соколова.

Ни для кого не является секретом то, что в настоящее время вопросами защиты информации, как правило, занимаются специалисты, не имеющие базового образования в области информационной безопасности. В этой связи работа секции «Образование в области информационной безопасности» и рассматриваемые на ней вопросы были

У стенда с методической литературой

направлены на повышение качества образовательной деятельности в этой области, комплексного решения вопросов повышения квалификации специалистов, занимающихся защитой информации.

Кстати, возможно, было бы более целесообразно заседания секций осуществлять в виде вебинара.

Т. С. Старшинова, *генеральный директор ООО «НПК «СпецПроект»*

Такие мероприятия, как IX ежегодная всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты» являются мощным стимулом для расширения горизонтов делового партнерства.

Обмен мнениями и практическим опытом позволяет выработать единое понимание проблем обеспечения ИБ и согласовать наиболее рациональные решения по созданию и совершенствованию многоуровневых систем защиты информации.

В связи с тем, что организация и технология технической защиты информации о персональных данных государственных гражданских служащих и граждан РФ является одним из видов деятельности ООО «НПК «СпецПроект», работа в секции «Нормативно-правовое регулирование в области защиты ПДн ЭДО» позволила специалистам нашего предприятия обсудить проблемные вопросы практики применения нормативно-правовой базы в области защиты ПДн как с представителями уполномоченных органов в данной области, так и с практическими работниками других специализированных предприятий.

Мы благодарны организаторам конференции, сумевшим динамично выстроить программу ее проведения, совместив актуальное деловое общение с насыщенной культурно-досуговой программой.

А. С. Марков, *генеральный директор ЗАО «НПО «Эшелон»*

IX сочинская конференция, как и 9-й месяц года, символизировала собой спелые плоды исследований новых методов и технологий в области информационной безопасности. В первую очередь, это коснулось защиты ПДн, изысканий по оценке соответствия, организации ЭДО.

В нормативном плане наиболее дискуссионными стали вопросы защиты личной, интимной и семейной тайн, а также инновации в области ЭЦП. Специалистов, конечно же, взволновало, каким образом будет нормативно реализован полученный за последние два года гиперположительный опыт в области организационно-технической защиты конфиденциальной информации, ориентированный на реальные угрозы, а не античные директивные процедуры.

Несмотря на задекларированный региональный аспект, центральным событием конференции являлись, конечно же, выступления регуляторов, задающие критерии оптимизации рынка в области безопасности. Если в прошлом году тон конференции определили аналитические выступления по персональным данным представителей ФСТЭК России и Роскомнадзора, то в этом внимание общественности привлек футурологический доклад, прозвучавший из уст представителя ФСБ России.

Несмотря на ряд откровенно прокоммерческих докладов и «декларативно проблемных» выступлений, некоторые «круглые столы» были настолько увлекательными, что многие участники в первые два дня смогли добраться до моря только при Луне.

Приятно, что организаторы на этот раз выставили большинство презентаций в открытый доступ, что позволило еще раз сориентироваться в степени профпригодности выступающих.

Обязательно надо отметить душевный оптимизм и исключительно высокий уровень организации самой конференции как культурного саммита. Это обеспечило благоприятную атмосферу для решения глубоко научных задач, стоящих перед топ-менеджментом российских организаций, функционирующих в непростой сфере ИБ.

Л. Г. Осовецкий, *заведующий кафедрой безопасных информационных технологий Санкт-Петербургского государственного университета ИТМО*

Несмотря на несомненную полезность и важность всех без исключения секций конференции для меня на этот раз на первом плане стояли соревнования Sochi CTF 2010, поскольку в них принимала участие команда нашей кафедры. Мы приняли участие примерно в 15 таких соревнованиях (в том числе в очном турнире, организованном АИС под Москвой, где наша команда заняла первое место) и два организовали в удаленном варианте. К сожалению, на этот раз явочный тур организовать не удалось, но удаленный вариант получился весьма представительным – 73 команды, в том числе 15 иностранных.

Участие в таких соревнованиях и их организация требует подготовки высококвалифицированных специалистов, разработки специфических заданий, специальных технологических средств и ресурсов. Особенно важное значение приобретают научный анализ угроз безопасности информации и патриотическое воспитание участников команд. Поэтому электронная Россия обязательно должна участвовать в международном движении «Белых хакеров» в интересах собственной безопасности и высококвалифицированного использования средств автоматизации обработки информации.

По нашему опыту участия в соревнованиях, за спиной каждой из иностранных команд стоят соответствующие силовые или банковские структуры, фирмы-разработчики информационных технологий. И нам тоже необходимо привлекать ресурсы Министерства обороны, банков и ИТ-компаний, заинтересованных в тестировании уязвимостей своих продуктов. ■