«IT Диалог» 2017. Часть 2

текст: Ольга Попова

В прошлом номере мы рассказывали о том, как на правительственной площадке К2 в Санкт-Петербурге проходил IV Всероссийский форум «IT Диалог». А конкретно — как руководители региональных министерств и ведомств по информатизации развивают электронное правительство. Сегодня мы продолжим отчет о мероприятии и познакомим вас с не менее актуальными темами, поднятыми на форуме.

Россия защищенная

Государственные порталы и информационные системы все чаще подвергаются целенаправленным атакам, поэтому вопросы информационной безопасности выходят на первый план. Об устойчивости информационной инфраструктуры государственных органов к угрозам безопасности, о практике обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, о соответствии информационных систем российским требованиям по ИБ шла речь на второй секции.

По традиции вначале перед аудиторией выступили регуляторы. Доклад начальника отдела УФСТЭК России по СЗФО Виктора Сторожека был посвящен подходам при реали-

зации основных направлений государственной политики в области кадрового обеспечения ИБ. Спикер рассказал, каким образом ФСТЭК России осуществляет методическое руководство по разработке и согласованию программ дополнительного профессионального образования при подготовке кадров в области информационной безопасности, а также отметил, что на ФСТЭК России в настоящее время возложены полномочия центра ответственности по определению ежегодных контрольных цифр приема по укрупненной группе направлений подготовки «Информационная безопасность».

Представитель Управления ФСБ России по городу Санкт-Петербургу и Ленинградской области познакомил собравшихся с опытом ведомства — Регионального центра мониторинга системы СОПКА ФСБ России по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы госорганов. Он привел примеры официальных сайтов СЗФО, взломанных злоумышленниками.

С 1 января 2016 года в России действует так называемый закон «о праве на забвение». Закон обязывает поисковые системы по заявлению гражданина и без решения суда удалять из результатов поиска ссылки на незаконную, недостоверную или неактуальную информацию о заявителе. При этом закон предусматривает возможность удаления неактуальной информации независимо от того, наносит ли она вред чести и достоинству заявителя. О пресечении распространения персональных данных в Интернете рассказал заместитель начальника отдела по защите прав субъектов ПДн и надзора в сфере ИТ УРКН по СЗФО Эрнест Бирих. По данным Роскомнадзора, наибольшее количество претензий граждане предъявляют к банкам, кредитным организациям, интернет-сайтам и социальным сетям.

Критически важные объекты городской инфраструктуры требуют повышенных мер защищенности. К таким объектам безусловно относятся железная дорога и аэропорт. Созданный в 2014 году в ОАО «РЖД» ситуационный центр мониторинга информационной безопасности обеспечивает защиту ИТ-ресурсов компании и оперативное реагирование на инциденты. Персонал центра постоянно отслеживает специализированные информационные порталы, чтобы вовремя получать данные об уязвимостях операционных систем, системного программного обеспечения, сетевого оборудования или иных угрозах ИБ, информацию о вредоносном ПО, а также о методах и средствах осуществления компьютерных атак. О защите инфраструктуры ОАО «РЖД» рассказал участникам секции начальник отдела контроля и эксплуатации средств ЗИ Санкт-Петербургского ИВЦ ОАО «РЖД» Михаил Бородулин.

Международная организация гражданской авиации (ИКАО) все чаще предпринимает определенные действия, направленные на решение вопросов обеспечения информационной безопасности объектов гражданской авиации. Александр Костин, руководитель отдела экспертов ИТ-дирекции ООО «Воздушные ворота Северной столицы», отметил, что наиболее эффективное обеспечение информационной безопасности реализуется при наличии единого механизма — централизованной системы, позволяющей рационально управлять всеми ресурсами. Александр рассказал о защите периметра информационной инфраструктуры, о том, какие механизмы и решения применяются на практике в Пулково. Среди них использование единой инфраструктуры и протоколов шифрования, создание центра сертификации, разделение сетей, контроль радиоэфира.

Практике защиты государственных сайтов в Астраханской области была посвящена презентация директора ГБУ АО «Инфраструктурный центр электронного правительства» Валентина Косарева. Он привел примеры успешных взломов. Так, в качестве новости 23 мая злоумышленниками был выложен «официальный пресс-релиз» под названием «Экстренное совещание правительства Оренбургской области о неотложных мерах в связи с трагическими событиями в северных районах республики Казахстан». В ложном сообщении, размещенном хакерами, говорилось, что Берг провел экстренное совещание о неотложных мерах в связи с трагическими событиями в северных районах Казахстана. От имени глав

МВД, МЧС и ФСБ Оренбуржья сообщалось об усилении мер безопасности в приграничных районах и надвигающейся гуманитарной катастрофе для жителей области. В пресс-службе правительства Оренбурга сообщили: «Сайт взломан, принимаем меры». Эта и другие истории наносят существенный урон репутации государственных порталов. Валентин Косарев рассказал о том, как можно обезопасить ресурсы, перечислил организационные и технические меры для защиты и пояснил их эффективность.

Добавим, что секция прошла при модерации руководителей ИБ-структур Комитета по информатизации и связи Андрея Лихолетова и СПБ ГУП «ИАЦ» Владимира Колосова. Участники получили возможность напрямую задать вопросы регуляторам и обсудить с коллегами насущные вопросы информационной безопасности, а также принять участие в симуляционной игре от «Лаборатории Касперского».

Россия объединенная

Тема АПК «Безопасный город» изначально была заявлена основной темой форума «IT Диалог» ‘2017. Многие руководители информационных министерств приехали в Санкт-Петербург для того, чтобы познакомиться с опытом Комитета по информатизации и связи и ГУП «АТС Смольного». В преддверии Кубка конфедераций в нашем городе были реализованы механизмы физической защиты жителей и гостей Северной столицы. Сегодня во всех районах Санкт-Петербурга установлено свыше 19 тысяч камер. В их поле зрения — сложные перекрестки, оживленные магистрали, дворы спальных районов. В мае в Московском районе открылся городской ситуационный центр «Безопасный город», который должен объединить все службы, отвечающие за безопасность в Санкт-Петербурге, в том числе центр управления кризисными ситуациями МЧС. В центр поступает информация с систем городского видеонаблюдения, экстренных служб, показания датчиков социальных объектов. Заместитель начальника Главного управления (по защите, мониторингу и предупреждению чрезвычайных ситуаций) — начальник управления гражданской защиты Главного управления МЧС России по Санкт-Петербургу Роман Емельянов рассказал о том, как быстро комплекс позволяет реагировать на происшествия.

В настоящее время наиболее полно в Санкт-Петербурге реализованы требования функциональных блоков «координация работы служб и ведомств и их взаимодействие» и «безопасность населения и муниципальной (коммунальной) инфраструктуры». Их основой стали Автоматизированная информационная система обеспечения безопасности жизнедеятельности Санкт-Петербурга, введенная в действие в 2006 году, и Автоматизированная система управления Единой дежурной службы Санкт-Петербурга, сформированная в 2003 году. В 2017 году началось создание блока «Транспортная безопасность», основой которого стал Региональный центр управления транспортом. Блок «Экологическая безопасность» планируется организовать в 2017–2018 годах.

Участники секции обсуждали вопросы обеспечения безопасности во время проведения спортивных массовых мероприятий. Рассказывали о том, как будет работать АПК «Безопасный город» при проведении чемпионата мира по футболу ФИФА 2018.

Заместитель председателя Комитета по информатизации и связи Санкт-Петербурга Андрей Соколов сказал: «В настоящее время во всех регионах страны ведется активная работа по созданию и внедрению элементов АПК «Безопасный город». И уже сейчас можно сделать выводы, что проблемы у всех регионов общие: это и механизмы организации межведомственного взаимодействия, и интеграция ранее созданных информационных систем в АПК «Безопасный город» в соответствии с федеральной концепцией, и поиск источников финансирования. А вот подходы к решению проблем, как мы далее увидим, у всех разные. Но можно выделить три ключевых понятия, которые являются общими для всех регионов и субъектов нашей страны, если речь идет о создании и внедрении АПК «Безопасный город»: комплексный подход, взаимодействие, интеграция. Поэтому мы и назвали нашу конференцию именно так: «АПК "Безопасный город": комплексный подход, взаимодействие, интеграция».

География участников третьей секции действительно всероссийская. Министр связи и информационных технологий Архангельской области Николай Родичев поделился опытом построения АПК «Безопасный город» в своем регионе. Не обошлось и без трудностей: «Следует отметить, что техническая реализация комплекса на территории пилотных зон в Архангельской области в целом завершена, подрядчик отрабатывает возникающие в ходе опытной эксплуатации замечания. Но если технические проблемы решаются, то вопросы межведомственного взаимодействия большого количества организаций стали самым сложным моментом проекта. Схема информационных потоков в системе очень сложная, есть противоречия между руководящими документами по АПК и реальными полномочиями служб», — сказал Николай Родичев. Заместитель председателя Государственного комитета по транспорту и связи Кабардино-Балкарской Республики Аслан Бештоков привел примеры внедрения аппаратно-программных решений для организации взаимодействия на различных уровнях в рамках АПК «Безопасный город».

В секции приняли участие представители Ханты-Мансийской администрации, правительства Пензенской области, Роскомнадзора, Главного управления Росгвардии по СПб и ЛО и АО «Пассажирский порт Санкт-Петербург «Морской фасад», а также многие другие специалисты по АПК «Безопасный город».

***

Во второй день форума на той же площадке К2 состоялись два круглых стола — «Цифровая трансформация городов» и «Ключевые задачи и решения в подготовке городской инфраструктуры к чемпионату мира по футболу 2018. Комплексный подход», а также прошло награждение победителей II Международного студенческого хакатона Code4Piter. Дипломы и сертификаты вручили председатель Комитета по информатизации и связи Денис Чамара и заместитель директора департамента проектов по информатизации Министерства связи и массовых коммуникаций Российской Федерации Даниил Сорокин, которые поздравили победителей хакатона, а также отметили уникальность, а главное — востребованность разработанных ими проектов.