МЕЖДУНАРОДНЫЙ СТАНДАРТ БЛАГОНАДЕЖНОСТИ

В ФЕВРАЛЕ КОМПАНИЯ МТТ, ИЗВЕСТНЫЙ ОПЕРАТОР МЕЖДУГОРОДНОЙ И МЕЖДУНАРОДНОЙ СВЯЗИ РФ, ОБЪЯВИЛА ОБ УСПЕШНОМ ЗАВЕРШЕНИИ СЕРТИФИКАЦИОННОГО АУДИТА НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001:2005. ПО ЕГО РЕЗУЛЬТАТАМ КОМПАНИЯ ПОЛУЧИЛА СЕРТИФИКАТ НА СИСТЕМУ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (СУИБ). ЭТО ПЕРВЫЙ СЛУЧАЙ НА РОССИЙСКОМ РЫНКЕ, КОГДА ОПЕРАТОР СВЯЗИ ПОДТВЕРЖДАЕТ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ОКАЗЫВАЕМЫХ УСЛУГ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНОГО СТАНДАРТА. МИХАИЛ ШАРОВ

ОАО «Межрегиональный транзиттелеком» (МТТ) — национальный оператор междугородной и международной связи. Компания основана в 1994 году для обеспечения взаимодействия между региональными сетями операторов подвижной связи. МТТ предоставляет широкий спектр телекоммуникационных услуг и обеспечивает организацию эффективного взаимодействия более 300 сетей сотовых операторов и более 100 сетей операторов фиксированной связи в России между собой. В мае 2005 года компания получила лицензию Россвязьнадзора №32042 на оказание услуг междугородной и международной связи конечным потребителям на всей территории Российской Федерации и вышла на рынок международной связи.

В 2005 году доход компании составил около $220 млн, объем трафика в сети МТТ превысил 4,2 млрд минут. Система менеджмента качества ОАО МТТ в июле 2006 года сертифицирована на соответствие международному стандарту ИСО 9001–2001.

КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО Эта история начиналась в середине 2005 года. К тому моменту специалисты компании МТТ, занимающиеся информационной безопасностью, осознали, что множество технических средств безопасности, работающих на площадках провайдера, живут сами по себе. Не существовало понимания того, что это оборудование работает по общепризнанным мировым стандартам.

Более того, появились проблемы. Во-первых, не было прописано четкого разделения ответственности между пользователями СУИБ, что для комплексной задачи по защите информации вопрос первостепенный. Во-вторых, с ростом числа угроз, изменением сервисов, постоянным строительством сети передачи данных встал вопрос обеспечения непрерывности информационной безопасности как процесса. Из этого следовало, что необходимо построить систему, которая мобильно изменялась бы вместе со средой и адекватно ей.

Решение задачи специалисты ОАО МТТ начали с изучения существовавших на тот момент стандартов, которые делятся на два типа. Первые — сугубо технические — регламентируют конкретные и узкие задачи информационной безопасности. Фактически они декларируют, каким инструментарием и в какой ситуации необходимо пользоваться, чтобы защититься от тех или иных угроз.

Второй тип стандартов — процессные, основанные на цикле Деминга, или PDCA-цикле. Они содержат рекомендации по построению в организации эффективной системы управления информационной безопасностью, функционирующей в контексте общей системы управления. С помощью этого типа стандартов необходимо определить, какие активы для бизнеса критичны; выяснить, какие угрозы возможны для них; рассчитать предполагаемый ущерб для бизнеса; создать план по обработке этих рисков; согласовать план с высшим руководством; начать внедрение СУИБ; производить постоянный мониторинг и модификацию плана работ согласно изменениям, которые происходят в компании.

К моменту, когда в МТТ определились со своим типом, британский стандарт управления информационной безопасностью BS 7799 с некоторыми изменениями стал международным стандартом ISO 27001:2005. Появилось еще одно преимущество работы с ним: официальная, признанная во всем мире сертификация системы.

Это немаловажный вопрос для компании, работающей на международном рынке связи. Иностранные компании, тем более такие старожилы, как Vodafone или British Telecom, в первую очередь спрашивают: «Как у вас решены проблемы информационной безопасности?» Сертификаты и лицензии российских силовых органов впечатления, как правило, не производят, ибо вся информация о правилах получения подобных документов скрыта в недрах российских спецслужб.

В то же время документ от Международной организации по сертификации не требует дальнейших разъяснений, тем более когда аудит на соответствие стандарту проводит

ИНОСТРАННЫЕ КОМПАНИИ, ТЕМ БОЛЕЕ ТАКИЕ СТАРОЖИЛЫ, КАК VODAFONE ИЛИ BRITISH TELECOM, В ПЕРВУЮ ОЧЕРЕДЬ СПРАШИВАЮТ: «КАК У ВАС РЕШЕНЫ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?» РОССИЙСКИЕ СЕРТИФИКАТЫ И ЛИЦЕНЗИИ ВПЕЧАТЛЕНИЯ НЕ ПРОИЗВОДЯТ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР МТТ КОНСТАНТИН СОЛОДУХИН (СПРАВА) ВМЕСТЕ С ПРЕДСТАВИТЕЛЕМ BSI РОБЕРТОМ ВИТЧЕРОМ КРЕПКО ДЕРЖИТ В РУКАХ СЕРТИФИКАТ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001:2005

НЕИЗВЕСТНЫЙ ISO27001/IEC 27001:2005

Стандарт на систему управления информационной безопасностью ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» имеет британские корни. В его основу лежит английский стандарт BS 7799, разработанный Британским институтом стандартов (BSI, British Standards Institution) совместно с рядом коммерческих организаций, таких как Shell UK, British Telecommunications, Association of British Insurers, Unilever, Marks &Spencer и др.).

BSI удалось увязать воедино 126 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определенных на основе лучших практик мирового опыта в данной области. С 1995 года BS 7799 имеет статус государственного стандарта Великобритании. Стандарт состоит из двух частей: Часть 1: Практические правила управления информационной безопасностью и Часть 2: Спецификация системы управления информационной безопасностью.

В 1999 году первая часть BS 7799 после доработки была передана в Международную организацию по стандартизации. В 2000 году претерпев ряд незначительных правок документ был утвержден в качестве стандарта ISO/IEC 17799:2000. Вторая часть BS 7799 стала основой для принятого ИСО стандарта ISO/IEC 27001:2005.

Чуть позже, в сентябре 2002, после внесения нескольких дополнений и изменений, версия обновилась до BS7799-2:2002. 15 октября 2005 года Международная Организация по Стандартизации (ISO) приняла стандарт BSI BS 7799-2:2002 в качестве международного — ISO/IEC 27001:2005. Основная цель стандарта — создание общей методологии для разработки, внедрения и оценки эффективности СУИБ, применимой для коммерческих компаний и государственных некоммерческих структур. В 2007 году ожидается развитие стандарта: на смену ISO/IEC 17799:2005 должен прийти ISO/IEC 27002:2007.

ISO/IEC 27001:2005 не является техническим стандартом, он не предписывает использование определенных способов шифрования данных или устройств защиты от сбоев. Стандарт определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска и другие аспекты в контексте информационной безопасности. Внедрение Системы на основе этого стандарта и последующая сертификация в BSI даёт компании инструмент, позволяющий управлять конфиденциальностью, целостностью и доступностью важного актива компании — информации, и может с одинаковым успехом применяться в компаниях разного размера — от индивидуальных предпринимателей до предприятий с численностью сотрудников в десятки тысяч человек.

ISO/IEC 27001:2005 предполагает управление защитой любого вида информации: финансовой, кадровой, удаленных партнерских баз данных — словом всего, что уязвимо с точки зрения безопасности. Хакеры, промышленный шпионаж, внутренние утечки, пиратство, сбои в работе ПО, вирусы — все эти риски в результате подготовки к сертификации сводятся к минимуму.

СУИБ, разработанная в соответствии с ISO/IEC 27001:2005 обеспечивает наличие отлаженной структуры, которая инициирует, реализует, поддерживает в рабочем состоянии и управляет информационной безопасностью внутри предприятия. Процедура разработки и внедрения СУИБ занимает от полугода до нескольких лет в зависимости от количества охватываемых СУИБ активов, процессов, их сложности и количества персонала компании. Затраты на проекты внедрения и сертификации сильно варьируются в зависимости от перечисленных факторов.

ISO — Международная организация по стандартизации (ИСО) была создана в 1946 году двадцатью пятью национальными организациями по стандартизации. СССР был одним из учредителей организации. Дважды за всю историю глава Госстандарта избирался председателем ИСО. Россия является правоприемницей СССР в рядах ИСО, а с сентября 2005 года входит в Совет ИСО.

Вопреки распространенному заблуждению, название организации не является акронимом. При выборе названия главной целью ставилось одинаковое звучание на всех языках мира. Для этого было решено использовать греческое слово isos — равный, которое многими неверно истолковывается как сокращение от International Organization for Standardization.

ЕВГЕНИЙ ЧЕРЕШНЕВ, МИХАИЛ ШАРОВ