известная британская фирма BSI. Это большое конкурентное преимущество для работы с внешними партнерами-операторами, не скованными условностями российских сертифицирующих органов.

Еще одним голосующим фактором за начало сертификации на этот стандарт послужила репутация компании-аудитора.

Компания BSI Management Systems — это не просто автор-разработчик стандарта информационной безопасности. BSI в России развернула очень серьезную кампанию по пропаганде ISO 27000, обучению персонала заказчика. А главное, BSI — это мировой лидер: более 40% всех сертификатов на соответствие этому стандарту в мире выдано именно этой компанией.

КОРПОРАТИВНЫЙ ЭФФЕКТ В качестве подрядчика была выбрана компания «Инфосистемы Джет» — один из ведущих системных интеграторов, входящий в Топ–20 российского ИТ-рынка, и поставщик решений в области информационной безопасности. Системы, разработанные этой компанией, имеют государственные сертификаты на высокие уровни доверия и применяются в госучреждениях на территории РФ.

«Проект по внедрению СУИБ в соответствии с требованиями стандарта ИСО 27000 длился ровно год,— рассказывает Борис Симис, начальник центра информационной безопасности компании „Инфосистемы Джет“.— Это не считая времени, потраченного на тендер, когда компания обошла ряд крупных консалтинговых фирм, в том числе и из „большой четверки“ — Deloitte & Touche, Ernst & Young, PricewaterhouseCoopers и KPMG. Поставленные задачи были тяжелыми, но интересными. Заказчики очень быстро поняли, что проект выходит за рамки одного подразделения, занимающегося исключительно информационной безопасностью. Надо привлекать все отделы МТТ. Это, кстати, одно из требований стандарта, так как задача обеспечения информационной безопасности не может существовать вне контекста общих бизнес-задач компании».

Чтобы не пытаться объять необъятное, в качестве первого объекта для сертификации был выбран биллинг компании. И, кстати, стандарт ISO 27000, равно как и любой стандарт, основанный на процессном подходе, позволяет сертифицировать не только всю деятельность компании в целом, но и отдельные бизнес-процессы. В описательной части сертификата всегда указывается, в какой области, на каких задачах проводился аудит соответствия стандарту.

Борис Симис поясняет: «В случае с МТТ проверялась система управления информационной безопасностью биллинга компании. С точки зрения компании, биллинг — это почти всегда „черный ящик“. Люди внутри него знают, что они делают, люди из бизнес-подразделений, не связанных с биллингом, практически никогда не в курсе их деятельности. В рамках своих работ мы формализовали бизнес-процессы, связанные с биллингом, то есть конкретно описали, что делают сотрудники, вплоть до малейших инструкций. Проводилась просветительская работа — мы читали курсы, организовывали тренинги. Проводили ликбезы по информационной безопасности для специалистов финансового отдела, отдела продаж, секретариата, то есть людей, не связанных с ИТ напрямую. И такая работа с персоналом дала позитивные результаты. Все очень живо восприняли эту тему, задавали много интересных вопросов. И, мне кажется, это еще один из плюсов стандарта, что темой информационной безопасности прониклись люди, которые по долгу службы напрямую не занимаются этим».

Как показал результат, все было не зря. Пользователи из самых различных подразделений МТТ в процессе внедрения и освоения требований системы очень активно и со знанием дела стали принимать участие в процессе обеспечения ИБ — сообщали об инцидентах, которые могут повлиять на защиту системы; стали интересоваться, как повлияют их действия на общую защищенность компании, и т. д.

Вполне закономерный эффект дала работа по анализу рисков и описанию активов заказчика в области информационной безопасности и возможных финансовых ущербов. Сегодня руководство ОАО МТТ по стандартной отчетности ИТ-отдела, заложенной в механизм СУИБ, может точно подсчитать, сколько денег было сэкономлено благодаря тем или иным средствам по защите информации. Это очень важный момент для понимания самого механизма защиты информации. Раньше средства на это выделялись, но не было четкого понимания, сколько необходимо и сколько денег тратится впустую.

«То есть прежде в МТТ высший менеджмент и сотрудники ИТ-службы,— по мнению Бориса Симиса,— разговаривали на разных языках. И в ответ на вопрос об эффективности средств, затраченных на покупку оборудования, получали лишь число отраженных за отчетный период атак и предотвращенных утечек информации. Понятно, что подобные цифры невозможно понять неспециалисту. Теперь же с внедрением международного стандарта ISO/IEC 27001:2005 для руководства компании будет очевиден и экономический эффект от действия подразделения».

Одним из косвенных подтверждений успешности реализованного решения стал договор МТТ о межсетевом сотрудничестве с английским провайдером British Telecom, подписанный в марте этого года на выставке CeBIT'2007. Одним из оснований сделки послужила сертификация МТТ на стандарт ISO 27001:2005. ■

ИТАР-ТАСС

КОМПАНИЯ МТТ ТЕПЕРЬ ДАЖЕ НА СТОЛЕТНЕМ ДЕЙСТВУЮЩЕМ КОММУТАТОРЕ КОМПАНИИ ERICSSON МОЖЕТ ПРЕДОСТАВЛЯТЬ СВЯЗЬ ПО МЕЖДУНАРОДНЫМ СТАНДАРТАМ

ДОКУМЕНТ ОТ МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИИ ПО СЕРТИФИКАЦИИ НЕ ТРЕБУЕТ РАЗЪЯСНЕНИЙ, ТЕМ БОЛЕЕ, КОГДА АУДИТ ПРОВОДИТ ИЗВЕСТНАЯ БРИТАНСКАЯ ФИРМА BSI. ЭТО БОЛЬШОЕ КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО ДЛЯ РАБОТЫ С ВНЕШНИМИ ПАРТНЕРАМИ-ОПЕРАТОРАМИ

ОСВЕДОМЛЕННОСТЬ РОССИЙСКОГО БИЗНЕСА О СТАНДАРТЕ ISO27001 ОСТАЕТСЯ НЕДОСТАТОЧНОЙ

В декабре 2006 года компания «МТТ» обратилась в крупнейший международный орган по сертификации BSI (Британский Институт Стандартов) для проведения сертификационного аудита СУИБ. Аудит был проведен специалистами российского офиса BSI и подтвердил соответствие СУИБ МТТ требованиям международного стандарта ISO/IEC 27001:2005». ЕВГЕНИЙ ШИПИЛОВ, директор по продажам BSI Management Systems CIS, LLC ответил на вопросы ЕВГЕНИЯ ЧЕРЕШНЕВА.

Компания BSI (Британский институт стандартов) является признанным мировым лидером в области обучения и сертификации Систем менеджмента, одним из основателей Международной организации по стандартизации (ISO), автором британских стандартов, ставших впоследствии самыми известными международными стандартами ISO серий 9000, 14000, 18000, 22000, TS 16949, 17799, 27001. На долю BSI приходится 40% мирового рынка услуг по сертификации Систем управления информационной безопасностью.

BUSINESSGUIDE: Я понимаю, что вы хорошо оцениваете инициативу компании «МТТ». И все же, какие у компании были реальные основания и мотивация получения сертификата ISO27001?

ЕВГЕНИЙ ШИПИЛОВ: Когда весной 2005 года компания «МТТ» получила лицензию на оказание международной связи на всей территории Российской Федерации, у руководства появился дополнительный стимул минимизации рисков нарушения целостности абонентской базы и построении эффективной системы взаимодействия с зарубежными партнерами. Внедрение Системы Управления Информационной Безопасностью (СУИБ) было определено как одно из ключевых составляющих новой ветви развития бизнеса.

BG: Насколько я понимаю, процесс подготовки к сертификационному аудиту — процесс не быстрый? Сколько времени занял проект «МТТ»?

Е. Ш.: Процесс разработки и внедрения СУИБ по избранному компанией международному стандарту ISO/IEC 27001:2005 «Системы управления информационной безопасностью. Требования» занял почти полтора года и потребовал от компании определенных финансовых и временных вложений на пересмотр существующей системы управления информационной безопасностью, оптимизацию бизнес процессов и разработку и внедрение авторской методологии управления рисками, внедрение нового оборудования и переподготовку кадров.

BG: Во всем мире приведение информационных потоков компании в соответствие с международными стандартами безопасности — процедура закономерная и логичная. Чего нельзя сказать о России. С чем это связано? Приведет ли опыт МТТ изменению ситуации, формированию некоего положительного тренда?

Е. Ш.: Компания МТТ, став первой российской телекоммуникационной компанией, получившей международный сертификат по данному стандарту, смогла привлечь внимание Российского рынка к проблеме и показать эффективность применения лучших мировых практик для защиты ключевых активов компании и критичной для бизнеса информации. Несмотря на то, что Стандарт существует уже 11 лет, только за последние полтора года в России появился положительный тренд. В сравнении 2005 годом, который можно было охарактеризовать как этап становления и продвижения стандарта, начиная с первой в России и на постсоветском пространстве сертификации на соответствие требованиям BS 7799, разработки детальных и многоплановых курсов по СУИБ, 2006 год ознаменовался рядом успешно завершенных сертификационных проектов.

BG: А ваши планы?

Е. Ш.: С целью повышения качества внедряемых Систем BSI разработал Партнерскую Программу, которая позволила объединить в своих рядах около 20 ведущих системных интеграторов России, Украины и Молдавии. В рамках партнерской программы проводятся совместные мероприятия, направленные на продвижение Стандарта на рынках России и стран СНГ.

На данный момент осведомленность Российского бизнеса о международных подходах обеспечения информационной безопасности и, в частности, о международном стандарте ISO27001 остается недостаточной. С момента опубликования международного стандарта ISO27001 в октябре 2005 года в России сертифицировано 5 компаний. Однако, к концу текущего года партнеры BSI закончат проекты внедрения СУИБ в более чем 15 крупных компаниях. По нашим прогнозам эта цифра будет ежегодно расти высокими темпами.

Особенно актуальным внедрение и сертификация Систем Менеджмента в соответствии с международными стандартами видится на фоне предстоящего вступления России во Всемирную Торговую Организацию и постоянно растущего количества Российских компаний, выходящих на IPO.