



Сергей Химаныч, ведущий специалист отдела информационной безопасности ОАО «МегаФон»:

«Одной из таких сложностей вполне можно считать затягивание сроков работы над проектом. Причины могут быть самыми различными, не всегда зависящими от заказчика или исполнителя. В нашем случае причиной затягивания сроков могла послужить разветвленная и географически распределенная структура ОАО „МегаФон“. По совету специалистов со стороны исполнителя проекта — компании ReignVox — было принято решение по формированию рабочей группы, в которую вошли представители разных подразделений компании, в том числе бизнес-, ИТ- и ИБ-подразделений. Это позволяет оперативно проводить сбор исходной информации и согласование результатов работ».

ях. Выход возможен только один: вся работа должна быть построена с учетом планового развития событий.

Принципиально и экономно

— **Вопрос минимизации расходов — наверное, самый популярный во всех ипостасях жизнедеятельности компании. Можно ли сократить возможные расходы не в ущерб информационной безопасности?**

— **«Типовой проект — он есть, и в то же время его нет» — ваши слова. Каким же образом это происходит?**

— На каждом из описанных этапов перед нами, как перед интегратором, встают различные дополнительные задачи, обусловленные спецификой того бизнеса, который ведет компания-заказчик, ее размерами, инфраструктурой, активностью бизнес-процессов и многими другими пунктами. И из множества таких «пазлов» каждый раз складывается новая, индивидуальная конфигурация проекта по защите персональных данных для каждой конкретной организации.

В поисках ложки дегтя

— **Не могу не задать вопрос, касающийся проблем, с которыми приходится сталкиваться на различных стадиях работы. Можно ли выделить наиболее частые?**

— Использование самого слова «проблема» мне кажется чрезмерным: в процессе работы над проектами наших клиентов возникают не проблемы, а скорее нюансы, тонкости и — иногда — сложности. Но они решаются в рабочем порядке.

Например, на этапе обследования часто приходится сталкиваться с тем, что в компаниях существует масса недокументированных процессов или систем. В структурных подразделениях не всегда находятся сотрудники, обладающие полной информацией даже о собственных бизнес-процессах. Решением в данном случае становится комплексный анализ с учетом специфики организации, выявление всех возможных точек получения, накопления, хранения и передачи персональных данных.

Отдельного внимания заслуживает процесс изменения ИТ-инфраструктуры организации. Если вы помните, я уже обозначал средние сроки проведения комплексного проекта — около шести месяцев. За этот период иногда инфраструктура компании-заказчика претерпевает значительные изменения. И это нормально: современные ИТ-технологии более чем нестатичны: сегодня изменения и обновления в системах происходят в буквальном смысле слова ежедневно. Зачастую получается, что проект по защите персональных данных стартует, опираясь на одни «выходные данные», а завершить приходится в несколько иных услови-

— Существует ряд принципов, следование которым позволит существенно минимизировать бюджет на создание системы защиты персональных данных.

В основе первого принципа лежит *максимальное использование существующих средств защиты информации* при проектировании соответствующих систем. Средства защиты в любой компании применяются независимо от необходимости защиты персональных данных: это и системы антивирусной защиты, и встроенные средства контроля доступа операционной системы, и межсетевые экраны, и многие другие. Поэтому необходимо закрыть максимальное количество требований существующими средствами защиты. И только в том случае, если текущими средствами какие-то требования не выполняются, необходимо закупить и внедрить дополнительные.

Второй принцип — *экономичное логическое структурирование информационных систем персональных данных*. Если системы собраны в едином центре обработки данных, то целесообразно



Иван Гузев, начальник отдела информационной безопасности ООО «Таможенная платежная система»:

«В ходе выполнения проекта по построению системы защиты персональных данных мы столкнулись с необходимостью пересмотра части уже подготовленной документации по защите ПДн, возникшей по причине изменений требований нормативно-методических документов ФСТЭК России (Приказ ФСТЭК России №58 от 5 марта 2010 года). Изменения повлекли за собой коррекцию плана согласованных ранее мероприятий. Компания ReignVox, выполняющая работы, внесла изменения в модели угроз и часть других документов, разработанных и согласованных с нами ранее. Конечно же, в результате увеличились и сроки работ по проекту, но дополнительные задачи, выходящие за рамки заключенного ранее договора, были выполнены специалистами компании ReignVox в максимально сжатые сроки и без выдвижения дополнительных компенсационных условий. Несмотря на смягчение требований ФСТЭК России, мы решили не вносить изменения в договор с компанией ReignVox и аттестовать свои ИСПДн на соответствие требованиям по безопасности информации».

их логически структурировать в одну и защитить по периметру. В том же случае, если одна из систем имеет класс выше, чем другие, то ее экономически целесообразно выделить в отдельный сетевой сегмент — посредством использования межсетевого экранирования.

Принцип третий — *защищаться только от актуальных угроз*. При этом актуализация угроз описывается в обязательном для специальных систем документе, называемом «Модель угроз». При актуализации угроз отбрасываются те из них, чья вероятность низка, а ущерб при реализации невелик. <