

Как до конца года обеспечить защиту персональных данных?

Ф 3-152, подписанный 27 июля 2006 года, не оставил равнодушными операторов персональных данных. Закон был прилежно изучен, статьи «на злобу дня» средствами массовой информации написаны, исследования на предмет готовности обеспечить требования закона проведены. Согласно одному из них (InfoWatch и SecurityLab, 2007), требования закона большинством компаний (79%), участвующих в опросе, были признаны вполне подъемными к реализации, а 71% организаций даже запланировал внедрение новых, соответствующих законодательству средств защиты информации. Закон вступил в силу 30 января 2007 года. На текущий период о готовности защитить обрабатываемые персональные данные уведомили лишь 5% операторов. У остальных участников рынка есть несколько недель на то, чтобы выполнить необходимые действия.

На вопрос «что делать?» есть один ответ — выполнять требования закона. На вопрос «каким образом?» мы сейчас попробуем ответить. Если компания обладает достаточными технологическими и, что самое важное, финансовыми ресурсами, реализовать защиту ИСПДн

к указанному сроку представляется возможным. В противном случае, на выполнение требований закона понадобится от года до нескольких лет. Оптимальным вариантом в такой ситуации станет составление концептуального документа, согласно которому будет осуществляться поэтапная деятельность создания систем защиты персональных данных.

Услуги компании РАМЭК-Интеграция в области построения комплексных систем защиты персональных данных (СЗПДн) ориентированы на следующие основополагающие принципы:

- последовательность;
- экономическая эффективность;
- соответствие созданных решений нормативно-правовым документам.

Последовательность подразумевает под собой декомпозицию всего комплекса работ и выработку пошагового плана реализации проекта. Его формирование требует проведения аудита для определения текущего уровня состояния информационной безопасности в организации и класса системы, обрабатывающей персональные данные.



Оператор персональных данных по итогам аудита получит полное видение проблематики, что позволит ему подняться над ситуацией «зачем думать? трясти надо!» и действовать планомерно. Так, анализ бизнес-процессов, средств защиты информации (СрЗИ), используемых на текущий период, определение порядка доступа к ресурсам позволяют выявлять наиболее уязвимые места в существующей системе защиты персональных данных и оперативно решать наиболее актуальные задачи. К примеру, может быть, не нужно немедленно менять систему антивирусной защиты, которая успешно справляется со своим функционалом, но не соответствует требованиям ФСТЭК, а направить усилия на защиту серверов и рабочих станций от несанкционированного доступа, внедрение подсистемы межсетевого экранирования или обратить внимание на принятие организационных мер по предотвращению утечек.

Экономическая эффективность достигается за счет разумного выполнения требований закона и выработанных центром компетенции РАМЭК-Интеграция рекомендаций по итогам аудита.

Например, сократить издержки может позволить создание решения по защите ИСПДн с терминальным доступом. Терминальная архитектура предполагает наличие терминального сервера, на котором организованы все процессы обработки персональных данных (хранение, обработка и др.), а доступ пользователей к обработке осуществляется посредством бездисковых терминалов с минимальной функциональностью.

Преимуществами решения являются:

- сокращение стоимости за счет использования централизованной архитектуры защиты и создания рабочих мест сотрудников при помощи терминальных клиентских устройств;
- простота развертывания ИСПДн и средств защиты информации по сравнению с архитектурой «клиент-сервер»;
- масштабируемость архитектуры;
- простота подключения новых пользователей и их сопровождения;
- удобство администрирования и снижение операционных затрат за счет отсутствия необходимости локального развертывания ряда СрЗИ на терминалах ИСПДн.

Целесообразность использования терминального доступа рассматривается на этапе предпроектного обследования, после расчета TCO (Total cost of ownership, совокупная стоимость владения). В случае, если реализация такого решения оправдана, осуществляется построение соответствующей СЗПДн. Если у компании система обработки персональных данных изначально организована с терми-

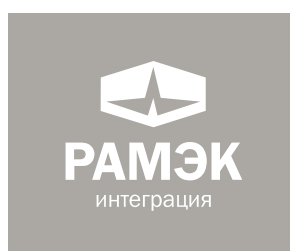
нальным доступом, вопрос решается только в части создания защиты.

На каком бы решении не остановился оператор, проектирование и реализация комплексных систем защиты информации всегда должны учитывать организационную структуру предприятия, уровень автоматизации, используемые технические средства и другие индивидуальные особенности компании.

Например, для небольших организаций характерны слабо развитая ИТ-инфраструктура и небольшое количество ИТ-специалистов, среди которых зачастую много «универсалов» — специалистов с сильно диверсифицированными навыками, которые должны заниматься поддержкой сразу нескольких информационных систем. На одного человека может возлагаться и поддержка ИТ-инфраструктуры, и решение вопросов обеспечения информационной безопасности, что чаще всего негативно сказывается на уровне защищенности. Крупные компании с территориально-распределенными офисами и развитой региональной сетью нередко сталкиваются с ситуацией, когда уровни зрелости в вопросах обеспечения информационной безопасности в одном офисе существенно отличаются от уровня в другом. Так же дела могут обстоять и с проработкой организационных мероприятий, использованием средств защиты информации. Таким образом, аттестат соответствия на созданную СЗПДн получают те организации, которые на этапе проектирования учтут всю специфику своей деятельности в проекте.

Соответствие созданных решений нормативно-правовым документам обеспечивается системным интегратором путем аттестации на соответствие требованиям безопасности информации (для 1 и 2 класса) и декларирования соответствия (для 3 класса). В информационных системах четвертого класса обрабатываются обезличенные персональные данные, требования к защите которых устанавливает сам оператор персональных данных.

С помощью последовательных и разумных шагов можно выстроить СЗПДн в оптимальные сроки и с последовательными финансовыми вложениями. Безусловно, к началу следующего года закончить проект удастся единицам, но начать его уже сегодня и реализовать в ближайшей перспективе под силу всем.



integration.ramec.ru
(495) 221 17 18