Виктор СЕРДЮК: «Реальная защищенность ИСПДн возможна только при комплексном подходе»

Интервью с генеральным директором ЗАО «ДиалогНаука», к. т. н., CISSP

– Об актуальности такой темы, как защита персональных данных, говорить излишне. Что может предложить компания «ДиалогНаука» в плане организации системы защиты ПДн и выбора оптимальных для этого решений?

– «ДиалогНаука» оказывает максимально широкий спектр услуг в области защиты персональных данных, позволяющих реализовать полный цикл создания системы защиты ПДн – от обследования до аттестации. Каждый этап работ имеет свои особенности. На этапе обследования необходимо правильно определить и классифицировать информационные системы персональных данных, составить корректную модель угроз и модель нарушителя. На стадии проектирования основная задача заключается в правильном выборе средств защиты информации с учетом испытаний. Необходимо также разработать комплексный пакет документов, соответствующий требованиям российского законодательства.

При техническом проектировании наша компания предлагает заказчику несколько вариантов реализации подсистемы защиты. Кроме того, мы рекомендуем провести макетирование и стендовые испытания различных продуктов, чтобы проверить их совместимость с существующим программно-аппаратным окружением, а также оценить их потребительские характеристики. По результатам испытаний заказчик самостоятельно принимает решение по выбору продукта исходя из его цены, удобства эксплуатации, известности бренда и других показателей.

– Различается ли задача защиты ПДн в организациях различных сфер бизнеса?

– Наша компания работает с клиентами практически из всех отраслей экономики, включая государственные предприятия, страховые компании и банки, компании нефтегазового сектора, негосударственные пенсионные фонды, операторов связи, промышленные предприятия. Каждый проект по защите ПДн является уникальным, поскольку всегда учитывает особенности бизнес-процессов организаций и информационных систем, при помощи которых они реализованы. Своя специфика есть у банков и операторов связи, поскольку для защиты персональных данных в этих организациях можно применять соответствующие отраслевые стандарты.

– Случалось ли вам исправлять, «доводить до ума» не завершенные кем-то другим проекты?

– Спрос всегда рождает предложение. На фоне высокого спроса на услуги по защите ПДн на российском рынке ИБ стали появляться новые игроки. Подавляющее большинство таких компаний не имеют опыта реализации подобных проектов и не могут выполнить их качественно. Основная проблема для клиентов подобных компаний – это иллюзия, что они получают систему защиты, полностью соответствующую требованиям ФЗ «О персональных данных». Однако при проверке Роскомнадзора, ФСТЭК или ФСБ выясняется, что это не так.

Мы уже сталкивались с ситуацией, при которой на втором этапе реализации проекта заказчик отказывался от услуг первоначального исполнителя и приглашал ЗАО «ДиалогНаука». В таком случае приходится проводить повторное обследование и уточнять данные, не отраженные в исходных документах, что, естественно, увеличивает сроки реализации проекта.

– Делает ли различия среднестатистический заказчик между выполнением требований регулятора и реальным уровнем защищенности данных на предприятии?

– Соблюдение требований российского законодательства по защите персональных данных является необходимым, но недостаточным условием для обеспечения высокого уровня защищенности информационной системы. Необходимо понимать, что даже аттестованная информационная система может быть взломана, если в рамках проекта был использован формальный подход, предусматривающий выполнение требований, изложенных в нормативных документах. Реальная защищенность ИСПДн возможна только при комплексном подходе, который учитывает и требования российского законодательства, и рекомендации международных стандартов.

Задача по защите ПДн не должна рассматриваться как разовый проект. Система защиты ПДн должна постоянно сопровождаться и совершенствоваться в рамках процессной модели управления ИБ. Это подразумевает администрирование средств защиты информации, актуализацию документов, регламентирующих вопросы защиты ПДн, проведение периодического аудита защищенности ПДн и т. д. ■

Компания «ДиалогНаука»
Тел.: (495) 980-67-76
E-mail: info@dialognauka.ru