Крепость для персональных данных

Краткое пособие-самоучитель по построению систем защиты персональных данных для начинающих

Часть 1

Дом для поросенка должен быть крепостью…

Умный Наф-Наф из сказки "Три поросенка"

Сергей Вихорев, *заместитель генерального директора по развитию ОАО "ЭЛВИС-ПЛЮС"*

По оценкам, средняя стоимость 1 дня работы специалиста по информационной безопасности с учетом накладных расходов и прочих налогов на сегодня составляет 28–33 тыс. рублей. Следовательно, даже простой экспресс-аудит, который длится не более 3 дней, не может стоить меньше 100 тыс. рублей, не говоря уже о более сложных работах.

В самом конце прошлого года, идя навстречу пожеланиям трудящихся, законодатель дал передышку на год для приведения информационных систем, которые обрабатывают персональные данные, в соответствие требованиям закона[1]. Ура! Но не стоит опять ждать русского "жареного петуха", времени осталось не так уж и много, и его надо эффективно использовать для решения проблем обеспечения безопасности персональных данных. Надеюсь, что все уже осознали значимость этой проблемы и к настоящему времени озаботились тем, как построить защиту для персональных данных. Вот и поговорим о том, как построить эдакую крепость для этих данных.

Как строить мост: вдоль или поперек?

Но прежде чем решать, как строить, необходимо определиться, какую защиту мы хотим построить: защиту от регуляторов при обработке персональных данных или защиту персональных данных при их обработке. А прежде чем решать эту дилемму, хочу обратить внимание на то, что все мы не только бизнесмены или чиновники, но еще и люди, которые имеют свои персональные данные, то есть все мы являемся носителями этих данных и, следовательно, в терминах закона сами являемся субъектами персональных данных, на защите интересов которых, собственно, закон и стоит. И для нас наши персональные данные ценны настолько, насколько мы сами их ценим. Поэтому, приступая к обработке чужих персональных данных, надо всегда помнить, что кто-то еще в этот момент приступает к обработке ваших персональных данных. Как говорится, будьте взаимно вежливы – и вы получите моральное право требовать от других должного отношения к вашим персональным данным.

Итак, решаем: что строим? Защита от регуляторов проще и, естественно, дешевле. Достаточно где-нибудь в Интернете найти образцы необходимых документов, немного их подправить, распечатать, составить план реализации мер по защите персональных данных, выполнить для приличия какой-нибудь пункт этого плана и на этом успокоиться. Придут регуляторы, а у нас что-то делается, ну не успели, но ведь стараемся! Может, и проскочит! Правда, остаются еще и сами субъекты этих данных, и они могут быть недовольны порядком их обработки. Они могут жаловаться, и вот тогда уж такая защита не поможет, это будет не крепость, а так, редутик. А на каждый роток не накинешь платок. И потом переделывать все заново – дороже. Так что этот путь – тупиковый. Поэтому я рекомендую сделать выбор в сторону строительства защиты именно персональных данных при их обработке в информационных системах. Об этом и пойдет дальше речь.

Можно ли построить защиту самому?

А можно построить самому загородный дом? Можно, но это будет не дом, а скорее эдакий "киль-дим" на фазенде, если, конечно, ты не архитектор и строитель в одном лице. Так и здесь, когда говорим о защите, – можно. Но для этого надо хорошенько разобраться в законах, правильно выбрать и применить требования регуляторов на практике, грамотно спроектировать защиту, да так, чтобы то, что уже есть, не пропало. Для этого нужны специальные знания, то есть нужен спец, да не один: нужен и юрист по компьютерному праву, и технический специалист по защите, и еще, может быть, криптограф. А это стоит дорого, да и штат такой держать не всегда выгодно. Опыт тоже немаловажен, а на защите одной информационной системы такого опыта не получишь. Опять же время. У профессионала на что-то уйдет час, у дилетанта – день, а то и два. Если кто-то уверен в своих силах и готов к таким издержкам, то, наверное, лучше строить защиту самому. Но получается, что проще и, может быть, даже дешевле отдать создание такой защиты на подряд (аутсорсинг) специалистам, которые сталкивались с этой проблемой и имеют большой опыт в ее решении. Главное – найти того, кому доверяешь, кто имеет авторитет в этой сфере.

Кто умеет строить защиту?

Естественно, сапоги должен тачать сапожник, а пироги печь – пирожник. Так и здесь: только профессионал, имеющий значительный опыт работы по внедрению систем защиты, способен грамотно и в сжатые сроки построить защиту персональных данных. Конеч-

[1] *Федеральный закон № 152-ФЗ, "О персональных данных".*

но, это должен быть интегратор. Но не просто интегратор информационных технологий, а именно интегратор в области информационной безопасности. Такой интегратор должен хорошо знать требования и законы, уметь использовать средства защиты разных производителей, иметь хороших аналитиков, необходимые квалифицированные кадры и производственную базу для реализации задуманного проекта. Бесспорно, он должен обладать всеми необходимыми лицензиями от регуляторов на выполнение таких работ и поддерживать с ними деловые контакты, чтобы при необходимости получить дополнительную консультацию. Пул контрагентов, которых привлекает интегратор для реализации проекта, должен быть проверен временем и иметь достаточную квалификацию.

Лирическое отступление о водке, конкуренции и "шабашниках от защиты"

Последние несколько лет ощущается сильная озабоченность правительства продажей и потреблением "паленой" и контрафактной водки. Водку вообще пить вредно, а "паленую" – вдвойне! И помереть можно. Но избавиться сразу от этой пагубной привычки не получается – все-таки русская особенность. А "паленая" или контрафактная водка в два, а то и в три раза дешевле легальной. Вот ее, родимую, и сметают с прилавков в первую очередь. А это не только вредит здоровью, но и бьет по легальному производителю. Сложно конкурировать с "серой" дешевой водкой, ведь за легальную продукцию надо платить налоги, акцизы и прочее. Поэтому года два назад в целях борьбы с недобросовестными производителями легальные производители выступили с инициативой установить минимальную розничную цену на водку. Инициатива реализовалась в приказ Федеральной службы по регулированию алкогольного рынка, и с 1 января этого года в России запретили продавать водку дешевле 89 рублей за пол-литра. А определять минимальные цены на алкоголь велено путем сложения себестоимости продукции при минимальном уровне рентабельности, акциза, НДС, оптовой (10%) и розничной (15%) надбавок. Не знаю, насколько эта мера поможет убрать "паленую" водку из продажи, но сама по себе идея интересная. "Ну и что? – скажет читатель. – А причем здесь защита персональных данных?"

А при том, что, по некоторым оценкам, в России от 4 до 7 млн операторов персональных данных, и всем им надо защищать свои информационные системы. Представляете, какое это поле для деятельности компаний, занимающихся защитой! Многие, почуяв возможность заработать, ринулись в этот сектор. Конкуренция выросла. Это, конечно, хорошо, но, к сожалению, наряду с профессионалами высокого класса появились недобросовестные производители, или, вернее, "шабашники от защиты". У кого-то спецов не хватает, а кто-то просто хочет подзаработать на этом буме. А для этого надо потеснить конкурентов, и желательно самым простым способом. Первое, что приходит на ум в этой ситуации, – снизить цены в ущерб качеству (по-другому не получается!). Вот и складывается ситуация, почти полностью аналогичная водочной. Сами по себе конкуренция и снижение цены – это благо. Но снижать можно только до определенного минимума, который определяется "себестоимостью продукции при минимальной рентабельности" и налогами. По оценкам, средняя стоимость 1 дня работы специалиста по информационной безопасности с учетом накладных расходов и прочих налогов на сегодня составляет 28–33 тыс. рублей. Следовательно, даже простой экспресс-аудит, который длится не более 3 дней, не может стоить меньше 100 тыс. рублей, не говоря уже о более сложных работах (об этом чуть позже). Поэтому и цена работ по защите персональных данных не может быть бесконечно малой величиной. Если же посмотреть некоторые итоги конкурсов на создание систем защиты персональных данных, которые прошли в 2009 г., то предложения по цене некоторых претендентов в два-три раза ниже среднерыночных! Это наводит на мысль, что они явно демпингуют. Причем и состав, и сроки работ совпадают, разница только в цене. И естественно, тот, кто предлагает более низкую цену, в силу требований Закона о конкурсных торгах[2] и выигрывает. Но защиту информации просто так руками не пощупаешь, и этим кто-то из "шабашников от защиты" пользуется. И малые цены в этом случае сильно отражаются на качестве работ. Вот и получается, как по поговорке: дешево, да гнило. Деньги потрачены, а толку мало.

Получается, что самая низкая цена на работы по защите – не всегда основной критерий в выборе подрядчика. При выборе работ по защите персональных данных надо обращать внимание и на наличие сильного коллектива разноплановых специалистов-профессионалов, и на опыт работы, и на состав партнеров подрядчика, и на возможность выполнения полного цикла всех работ, и на успешный опыт работы по аналогичным проектам. Ну а у вас всегда остается право выбора: делать нормальную систему или "паленую". ●

Ваше мнение и вопросы присылайте по адресу infosec@groteck.ru

2 Федеральный закон № 94-ФЗ "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".