Заметки после «ИНФОФОРУМА-12»

Александр Сапрыкин — член Оргкомитета «Инфофорума-Евразия», директор компании «С-Терра Бел»

В конце января этого года белорусская делегация, состоящая из представителей восьми министерств и ведомств, участвовала в работе 12-го российского форума информационной безопасности «Инфофорум», крупнейшем на пространстве СНГ. В данной публикации делается попытка взглянуть на белорусские проблемы в этой сфере через призму «Инфофорума», поскольку сравнительный анализ помогает сделать это предметнее.

Об электронном государстве и информационной безопасности

— Информационная безопасность (ИБ), или технологии безопасности, по убеждению участников форума, является ключевым фактором при создании электронного государства (ЭГ). Почему? То, что входит в понятие «электронное государство» можно кратко описать как информационное взаимодействие госорганов и граждан посредством ИТ-технологий. Понятно, что без развитой системы безопасности для всех этапов этого взаимодействия обойтись невозможно — от идентификации граждан (пользователей) для доступа к тем или иным государственным информационным ресурсам (базам данных), защиты самих баз данных и сетей госорганов от хищения, модификации, перехвата и, наконец, защиты используемых при взаимодействии открытых каналов связи.

Об удостоверяющих центрах

— В РФ создано главное идентификационное звено, с которого начинается ЭГ — общегосударственный удостоверяющий центр. И если раньше в российской ИТ-отрасли наблюдался почти что хаос примерно из трехсот местных удостоверяющих центров (УЦ), несовместимых между собой, то сейчас происходит формирование полноценной иерархичной структуры. Кроме того, созданы порталы государственных услуг, закупок и продаж. Через два года около 60 % государственных услуг будет оказываться населению в электронном виде.

В Беларуси внешне ситуация складывалась более благоприятно — на рынке представлено всего 4-5 местных УЦ. Однако они также несовместимы между собой, как и российские. Кроме того, распространение технологий УЦ-ЭЦП в республике незначительное — большинство министерств и ведомств их не имеют. И, наконец, сроки создания белорусского общереспубликанского УЦ (его официальное название — государственная система управления открытыми ключами — ГосСУОК) неизвестны, так как на это требуется немало времени.

О комплексном подходе к безопасности

— Что представилось наиболее значимым из российских реалий? Пожалуй, комплексный подход к проблемам ИБ: имеются методики сертификации, аттестации, значителен перечень норм, стандартов, инструкций и положений, описывающих весь процесс от проектирования защищенных ведомственных (корпоративных) сетей до практической реализации и проведения проверок.

В Беларуси нормативная база находится в начальном состоянии, а ее несовершенство, к примеру, приводит к тому, что сертифицировать средства защиты информации (СЗИ) у нас можно на что угодно. Можно произвольно взять из профиля защиты (стандарт безопасности) какие-либо функции безопасности и сертифицировать на их наличие, хотя сам профиль защиты делать подобное запрещает — только все или ничего. Можно сертифицировать многофункциональное устройство на какую-либо малозначительную функцию — и все, его можно поставлять как полноценное средство защиты. Законодательство обуславливает в качестве необходимого условия поставки средств защиты лишь наличие сертификата или положительного экспертного заключения, но вовсе не требует соответствия защитных функций поставляемого СЗИ реальным угрозам безопасности, как должно быть. В такой ситуации сложно спросить с тех, кто поставляет и покупает сертифицированные «дырки от бублика». Ведь, следуя теории комплексного подхода к ИБ, вначале формируется перечень угроз для защищаемого объекта информатизации, а затем подбираются сертифицированные средства защиты. Кроме того, на практике пока можно вовсе не защищаться — никто за это не накажет. И когда начнут спрашивать за исполнение законодательства по защите информации — тоже никто не берется сказать.

Об исполнении законодательства по защите информации

— С момента вступления в силу известных закона № 455 и постановления № 675 скоро исполнится год, а случаи приобретения сертифицированных средств защиты как были единичными в республике, такими и остались. Немногочисленные конкурсы, в которых где-то строкой присутствует упоминание о СЗИ (их всего-то было за этот период 4-5), на практике заканчиваются ничем — на средствах защиты экономят деньги, хотя факты закупок несертифицированных, либо формально сертифицированных, СЗИ имели и имеют место. Даже Национальный банк в конце прошлого года провел конкурс на приобретение сетевого оборудования с несертифицированными функциями защиты для межбанковской расчетной системы. Это оборудование для него затем сертифицировали по второстепенному функционалу. А на вопрос некоторых участников этого конкурса: «Как же это без белорусской криптографии?» — банк ответил, что «функции шифрования в данном случае не предусматриваются». То есть, следуя пояснению, электронные платежи в банковской системе страны будут проводиться в открытом виде и по открытым каналам связи?! Трудно в это поверить. Конечно же, средства криптографической защиты информации (шифро-

вания) будут задействоваться, только несертифицированные. К этому можно также добавить, что единственное банковское достижение в сфере средств шифрования — система «клиент—банк», не проходила никаких экспертиз! Другой, не менее характерный пример — Белтелеком. Предоставляя клиентам услуги защищенной связи (построения распределенной корпоративной сети — VPN), не пользуется сертифицированными средствами шифрования, хотя среди его клиентов немало госорганов, которым это необходимо по закону. И почему бы нашему оператору-монополисту не предоставлять подобные VPN-услуги, да еще за счет клиентов? Неразворотливость, безразличие? Возможно.

На фоне подобной практики белорусских лидеров возникли разговоры о том, что, мол, белорусская криптография слишком дорогая. Но это не белорусская криптография дорогая — она не дороже российской или испанской. Дешево бывает лишь тогда, когда не применяется ни та, ни другая, а что попадется под руку. Однако назвать это «лоскутное одеяло» технологиями ЭГ, где необходимы стандарты, унификация, совместимость, безусловно, нельзя.

В итоге, если в РФ эксплуатируются и создаются десятки и сотни защищенных ведомственных (корпоративных) IP-сетей на базе сертифицированных средств, то в Беларуси подобных сетей пока нет. В единичных случаях имеющихся защищенных ведомственных сетей используются не сетевые, а персональные СКЗИ. Такие специализированные АИС не вписываются в архитектуру ЭГ — они несовместимы, их трудно и затратно развивать, не говоря уже об организации межведомственного взаимодействия.

О защите персональных данных

— В РФ всерьез взялись за защиту персональных данных, что предписывают Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» от 1981 года и принятый в РФ в ее развитие закон № 455 ФЗ. Уже четвертый год продолжается подобная работа в финансово-кредитной сфере, медицине, отраслях связи — повсюду, где есть персональные данные (ПД). В острой дискуссии на форуме со стороны операторов ПД основные упреки к представителям госорганов заключались в несовершенстве законодательства, а также в сжатых сроках реализации в сравнении с Европой, которая занимается этим уже почти 30 лет. А ведь Беларусь к указанной Конвенции еще даже не присоединилась, что с позиций имиджа республики выглядит не лучшим образом, поскольку ПД — одна из незыблемых ценностей развитых стран (почти сорок европейских стран выполняют Конвенцию). Если и в дальнейшем не присоединимся, это не пойдет нам на пользу, так как законодательство и Европы, и России содержит ограничения по трансграничному обмену данными со странами, не обеспечивающими защиту ПД. Так что начинать, вероятно, все же надо. Причем целесообразно учесть в этом вопросе российский опыт, в том числе негативный. В частности, постараться избежать практики расширительного применения Конвенции, опираться на отраслевые стандарты (рекомендации) по защите данных. Например, Центробанк РФ дает подобные рекомендации по применению сертифицированных СКЗИ для всех российских банков.

О белорусско-российском защищенном взаимодействии

— Нельзя не упомянуть о том, что, по мнению представителей российских банков, работающих на белорусском рынке, отсутствие норм безопасности в кредитно-финансовой сфере Беларуси неизбежно повышает риски, связанные с утечкой информации и данных, снижает инвестиционную привлекательность отрасли в целом. Так, по словам представителя Сбербанка, при покупке БПС предполагалось распространить на него тот же корпоративный стандарт безопасности, который используется в Сбербанке. Однако выяснилось, что российские средства защиты не признаются в Беларуси, а обеспечить соответствующий уровень безопасности через белорусские стандарты невозможно — в нашей банковской сфере не имеется подобной практики. Поэтому неудивительно, что некоторые российские банки предпринимают меры по ввозу в свои представительства и филиалы в Беларуси российских сетевых СКЗИ.

Аналогичная ситуация в других отраслях. К примеру, представитель российского Минсоцразвития посетовал, что они завалены делами пенсионеров — миграционный поток между странами значительный, а никакой автоматизации при взаимодействии с белорусским министерством нет. Они хотели бы предложить белорусским коллегам применить в этих целях российские сетевые СКЗИ и надеются на их положительную реакцию. Однако, на самом деле, выбора — ставить российские СКЗИ или продолжать бумажную работу — у нашего Минтруда нет: первое нельзя, своего решения нет, остается последнее…

С развитием и насыщением рынка ИБ в России сетевыми СКЗИ на форуме прекратились дискуссии о возможности введения третьих стандартов для межгосударственного взаимодействия (например, белорусско-российской и союзной собственности). Характерно, что казахские коллеги на «Инфофоруме-12» посоветовали нам, белорусам, поступать так же, как они — признать российские стандарты. Так что наше прогрессирующее отставание от россиян в сфере ИБ, скорее всего, приведет к ситуации, когда и в Таможенном союзе, и в ЕврАзЭС в качестве межгосударственных будут применяться российские средства защиты. Хотя вполне достойно могли выглядеть решения с созданием буферных зон, где осуществлялась бы полная перекодировка передаваемых данных (информации) с одних национальных стандартов на другие.

Некоторые выводы

— Можно констатировать некий парадокс — законодательство о защите информации не только не придало импульс развитию рынка ИБ, но и из-за своего несовершенства в чем-то даже ухудшило ситуацию. Например, в условиях отсутствия комплексного подхода национальная система сертификации вместо того, чтобы стимулировать, фактически губит отечественного производителя, выпуская на рынок с сертификатом СЗИ фактически все, что захочет приобрести заказчик.

Белорусский рынок ИБ небольшой, поэтому зависим от факторов регулирования. Тем более что на начальном этапе просто необходимо поддержать и стимулировать отечественных производителей, поставив заслон всяческим исключениям и лазейкам. На рынке немало платежеспособных субъектов хозяйствования, в том числе с иностранным капиталом, способных его оживить и способствовать динамичному развитию. Ведь у себя дома и европейские, и российские компании активно используют согласно законодательству национальные СЗИ, заботясь о безопасности европейских (российских) вкладчиков, клиентов и потребителей, и почему бы так же не относиться к безопасности белорусских граждан?!

Словом, для развития рынка ИБ в гораздо большей степени, чем государственные вливания, необходимо умелое точечное регулирование. Далеко не бедная Россия, переложив финансовое участие операторов персональных данных, в результате имеет развитый рынок национальных СЗИ, крупных отечественных производителей, современные технологии безопасности электронного государства. А что хотим иметь мы? ■