Визитка

АЛЕКСАНДР ЛЫСЕНКО, ведущий эксперт по вопросам защиты информации компании «Код Безопасности»

Защита персональных данных

Год 2011-й. Отсчет продолжается

Хроника ФЗ 152

2006-2007: ФЗ 152 принят 27 июля 2006 года, вступил в законную силу 26 января 2007 года.

2008: Издан приказ «Об утверждении порядка проведения классификации информационных систем персональных данных», а также разработаны методические документы ФСТЭК и ФСБ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Глава 6 п. 3: информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны были приведены в соответствие с его требованиями не позднее 1 января 2010 года.

2009: 29 декабря – информационные системы персональных данных, созданные до 1 января 2010 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2011 года.

2010: 10 декабря – информационные системы персональных данных, созданные до 1 января 2011 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 июля 2011 года.

Суть ФЗ 152

Федеральным законом №152 «О персональных данных» (совместно с главой 14 Трудового кодекса Российской Федерации и Постановлением Правительства Российской Федерации от 17 ноября 2007 году №781) установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных данных собственных работников и сторонних физических лиц, персональные данные которых обрабатываются в организации.

В результате указанных государственных инициатив персональные данные стали информацией ограниченного доступа, вследствие чего физические лица в России получили право на юридическую защиту своих персональных данных со стороны государства. А компании, ведущие в своих ИС обработку ПДн, получили обязанности защищать персональные данные субъектов.

Таблица 1. Средства используемые в ИС, в которых производятся обработка и хранение персональных данных в соответствии с требованиями ФЗ-152

Классы СЗИ	Класс ИСПДн		
	К3	К2	К1
Средства защиты информации от несанкционированного доступа	◔	●	●
Межсетевые экраны	●	●	●
Средства доверенной загрузки	◔	●	●
Защита от вторжений (в т.ч. на основе имитации данных) и антивирусы	●	●	●

● – требуется, ◔ – рекомендуется

Все эти тонкости и неясности…

Закон о защите персональных данных сам по себе не вызывает ни у кого никаких нареканий – идея здравая и необходимая. Если уж компания получает от субъекта его ПД, то обязана их защищать от утечек, хищений, НСД и других опасностей. Но сколько несоответствий между реальной жизнью, бизнесом и текстом закона выявилось на практике!

Вот только несколько вопросов, которые обсуждались, в частности, на прошедшем в Москве в феврале Инфофоруме, на заседании секции, которая была посвящена защите персональных данных:

- Как поступать, если ПДн субъекта должны быть предоставлены в налоговую инспекцию, а субъект не подписал разрешение на предоставление данных третьим лицам?
- Как поступать с ПДн субъекта, который является недобросовестным плательщиком и не подписал разрешение на предоставление данных третьим лицам?
- Нужно ли отказываться от средств защиты информации, которые использовались ранее, и закупать новые средства защиты, специально сертифицированные для использования в ИСПДн?

Компании: что делать и сколько стоит?

Перед компаниями стоят сакраментальные вопросы: «Что делать?» и «Сколько стоит?». Второй вопрос также связан с еще одним, третьим: «Где брать финансирование?».

Один из самых простых ответов на вопрос «Что делать?», предлагаемый некоторыми компаниями на российском рынке, сегодня такой: решить вопрос выполнения требований ФЗ 152 выпуском невероятного количества внутренних документов и регламентов, которые будут определять порядок обработки и защиты ПДн в организации. Немало компаний предлагало и, вероятно, предлагает услуги такого плана несчастным операторам ПДн. Единственное, о чем умалчива-

ют поставщики услуг, – это риски, которые берет на себя компания в случае решения вопроса с помощью подобных «бумажных оргмер». Однако, отказавшись от реальной защиты данных в ИС, компания может не только не пройти плановую проверку со стороны контролирующих органов, но и столкнуться с реальной утечкой информации или жалобой со стороны субъекта ПД в контролирующие органы.

Российские компании-интеграторы предостерегают своих клиентов от выбора подобного пути и рекомендуют использовать сертифицированные средства защиты информации для ИСПДн.

Выбираем средства защиты. Перед операторами встает проблема выбора средств защиты, имеющих подтверждение соответствия для использования в системах ИСПДн. Выбрать решение для защиты информации всегда сложно, компаниям приходится учитывать и функциональные возможности приобретаемых решений, и их соответствие потребностям компании, и финансовые аспекты.

Определяем класс ИСПДн. Самая сложная задача, а для некоторых компаний и самая дорогая – определить класс своей ИСПДн. Некоторые фирмы стремятся занизить класс ИСПДн, что ведет к повышению рисков при осуществлении проверок регулирующими органами. Некоторые выбирают варианты построения ИСПДн, позволяющие сэкономить. Одним из таких способов выполнения требований ФЗ 152 с достижением реальной экономии является сегментирование ИСПДн.

Сегментируем ИСПДн с помощью межсетевого экрана. Приведем пример, при котором использование продукта разработки компании «Код Безопасности» Trust Access – МЭ высокого класса защиты, позволяет сегментировать ИСПДн и тем самым снизить затраты на построение ИСПДн.

Из документов ФСТЭК России (СТР-К, приказ №58 и т.п.) следует, что АС/ИСПДн можно разделить с помощью сертифицированных межсетевых экранов на части, при этом каждая из частей будет сохранять свой класс (см. рис. 1).

Защита ПДн, обрабатываемых на конечных станциях. В соответствии с базовой моделью угроз, утвержденной ФСТЭК («Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России 15.02.2008), для защиты ПДн на конечных станциях нужно использовать антивирусное средство, межсетевой экран (МЭ), средство обнаружения вторжений, а для ИСПДн высокого класса также необходимо средство защиты от несанкционированного доступа. «Код Безопасности» разработал решение, представляющее комплекс Антивирус + МЭ + HIPS , – это Security Studio Endpoint Protection (SSEP). В SSEP сертифицированы для использования в системах до К1 все компоненты, которые лицензируются для удобства как совместно с входящим в состав SSEP антивирусом, так и отдельно – для случаев, когда в организации уже приобретен и используется сертифицированный антивирус.

Защита ИСПДн в виртуальной среде

Безопасность информации – один из ключевых вопросов при развертывании ИСПДн в виртуальной среде. Нужно учитывать, что, во-первых, виртуальным машинам присущи ровно те же уязвимости, что и физическим, а во-вторых, как и любая новая технология, виртуализация несет новые угрозы безопасности. Проблема усугубляется тем, что, с одной стороны, традиционные средства защиты информации не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. С другой стороны, они не защищают от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры.

Специалисты «Кода Безопасности» выполнили анализ угроз, характерных для виртуализации. В результате было принято решение о разработке специализированного средства защиты информации в виртуальной среде, которое обеспечит сертифицированную защиту в виртуальной среде и в результате поможет операторам ПДн пройти аттестацию «виртуальных» ИСПДн.

Сегодня на рынке доступна версия продукта vGate, предназначенная для защиты виртуальных инфраструктур на платформе VMware Infrastructure 3 и vSphere 4. Продукт имеет сертификат ФСТЭК, позволяющий применять его для защиты ИСПДн до К1 включительно. BOF

Рисунок 1. Снижение класса ИСПДн с помощью TrustAccess