ВОЗРОЖДЕНИЕ БАНК

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

БЕЗОПАСНОСТЬ БАНКОВСКИХ ПРИЛОЖЕНИЙ – ВЗГЛЯД СО СТОРОНЫ БАНКА

Грициенко Андрей Александрович
Начальник Службы информационной безопасности Банка «Возрождение» (ОАО)

Вопрос

Зачем нужна банку какая-то особенная безопасность для банковских приложений?

Зачем нужна безопасность пешеходу при его перемещении в мегаполисе?

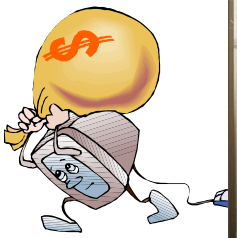
Приоритеты и пути их достижения

Приоритетом для бизнеса в банковской сфере является получение прибыли от операций с денежными средствами

Операции с денежными средствами обеспечиваются, в том числе путем обработки в корпоративной информационной системе банка информации, составляющей банковскую тайну

Банковская тайна и интерес к ней

Обработка информации, составляющей банковскую тайну, производится с помощью различных банковских приложений



«Нездоровый» интерес к банковской тайне и к соответствующим эксплуатируемым банковским приложениям проявляется со стороны злоумышленников

Требования и их применение

В целях противодействия «нездоровому» интересу злоумышленников, государство на законодательном и ведомственном уровнях определяет требования по защите информации, составляющей банковскую и иные виды тайн

Требования по защите информации «применяются» к исполнителям (банкам), которые обязаны обеспечить их выполнение «любой ценой»

Некоторые выводы

1. Несмотря на наличие требований регуляторов по обеспечению ИБ для АБС (в т.ч. для банковских приложений), решить в полной мере вопросы соответствия ПО АБС этим требованиям в рамках индивидуальных договорных отношений заказчиков (банков) и разработчиков (производителей) ПО достаточно затруднительно, так как корень проблемы лежит в необходимости построения системы безопасного программирования у производителя и наличия его заинтересованности в приведении своего продукта в полное соответствие требованиям по ИБ регуляторов и законодательства.

2. В построении эффективной полномасштабной системы безопасного программирования крупный производитель зачастую просто не заинтересован (пока он будет «строить», увеличивая тем самым стоимость продукта, менее разборчивые конкуренты уже продадут свой продукт «is as» по меньшей цене). А менее крупные производители зачастую просто не в силах внедрить такую систему.

Некоторые выводы

3. Пока ситуация в вопросе обеспечения регуляторных требований для банков такова, что готовность разработчика (производителя) банковских приложений к исполнению любых требований весьма высока, правда с одной существенной оговоркой, вроде такой как "любой каприз - за ваши деньги»

Вопрос

Не пришла ли пора банкам "поделиться" в плане ответственности за выполнение этих требований во всем их многообразии с разработчиками (производителями) тех самых банковских приложений, которые должны отвечать регуляторным требованиям по безопасности, будучи установленными в корпоративной информационной системе банка?

Как у них?

Вопрос насчет прихода "поры" возможно и риторический, но он назрел, да и тот самый западный рынок, в который мы так стремимся влиться, в рассматриваемом контексте дает нам соответствующие примеры решения подобных вопросов

Например, это введение обязательной сертификации системы обеспечения информационной безопасности (СОИБ) банков по стандарту обеспечения информационной безопасности ISO/IEC 27001 в ряде государств, которые играют значимую роль в мировой экономике.

Но, видимо, это не наш путь, т.к. Федеральный закон №184-ФЗ "О техническом регулировании" не позволяет без соответствующего технического регламента делать требования стандарта обязательными для выполнения, а наличие в России технического регламента именно в области информационной безопасности в ближайшее время практически недостижимая цель

Как у них?

Стандарт Payment Card Industry Data Security Standard (PCI DSS) с 2006 года был предназначен для сертификации организаций, осуществляющих обработку данных о держателях карт (ДДК). При этом на практике возникло множество проблем, мешающих организациям достичь соответствия PCI DSS из-за приложений, которые поддерживали не все требования стандарта.

Для решения этих проблем Совет по безопасности индустрии платежных карт PCI SSC (учредители American Express, Discover Financial Services, JCB International, MasterCard Worldwide и Visa Inc.) запустил в 2008 году программу повышения безопасности платежных приложений, в основу которой был положен производственный стандарт PA-DSS для разработки платежных приложений, которые продаются, распространяются или передаются по лицензии третьим лицам производителями программного обеспечения:

- ПО процессинга (front-office, back-office, middleware/switching);

- ПО для банкоматов и POS-терминалов;

- ПО для поддержки электронной (мобильной) коммерции (если идет обработка данных платежных карт).

Как у них?

Стандарт PA-DSS призван обеспечить безопасность платежных приложений при условии соответствия их требованиям стандарта PCI-DSS, в значительной мере перенося ответственность за наличие такого соответствия на производителей программного обеспечения.

Все платежные приложения, выпускающиеся на рынок для применения в международных платежных системах, должны проходить сертификацию по стандарту PA-DSS, которую могут выполнить только компании, обладающие статусом PA-QSA.

При этом международные платежные системы предписывают торгово-сервисным предприятиям и поставщикам услуг использовать с 1 июля 2012 года только сертифицированные по стандарту PA-DSS приложения, перечень которых опубликован и регулярно обновляется Советом PCI SSC

Законодательство по поводу подтверждения соответствия

Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регулировании»

Статья 20. Формы подтверждения соответствия

1. Подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер.

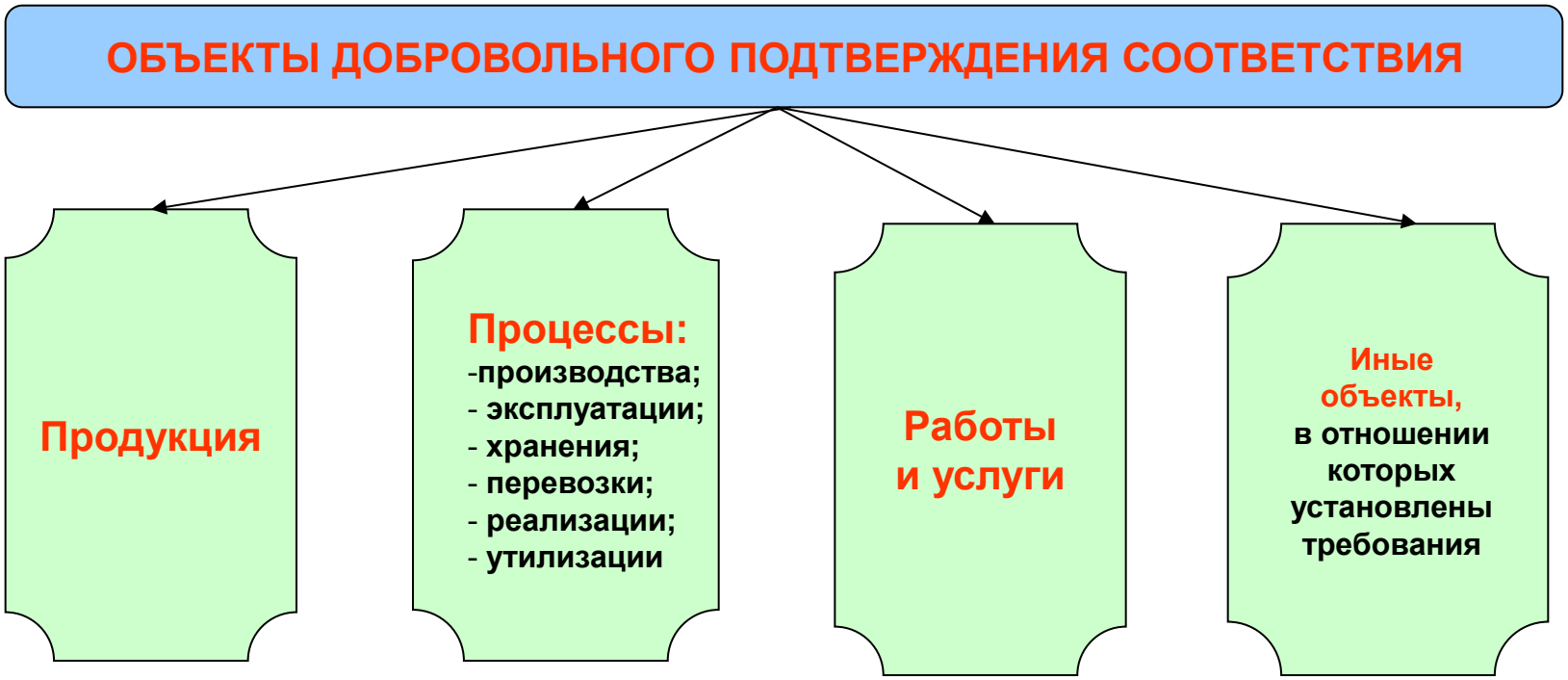
2. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

3. Обязательное подтверждение соответствия осуществляется в формах:

- принятия декларации о соответствии (декларирование соответствия);

- обязательной сертификации

Законодательство по поводу подтверждению соответствия



Системы добровольной сертификации
(пример)

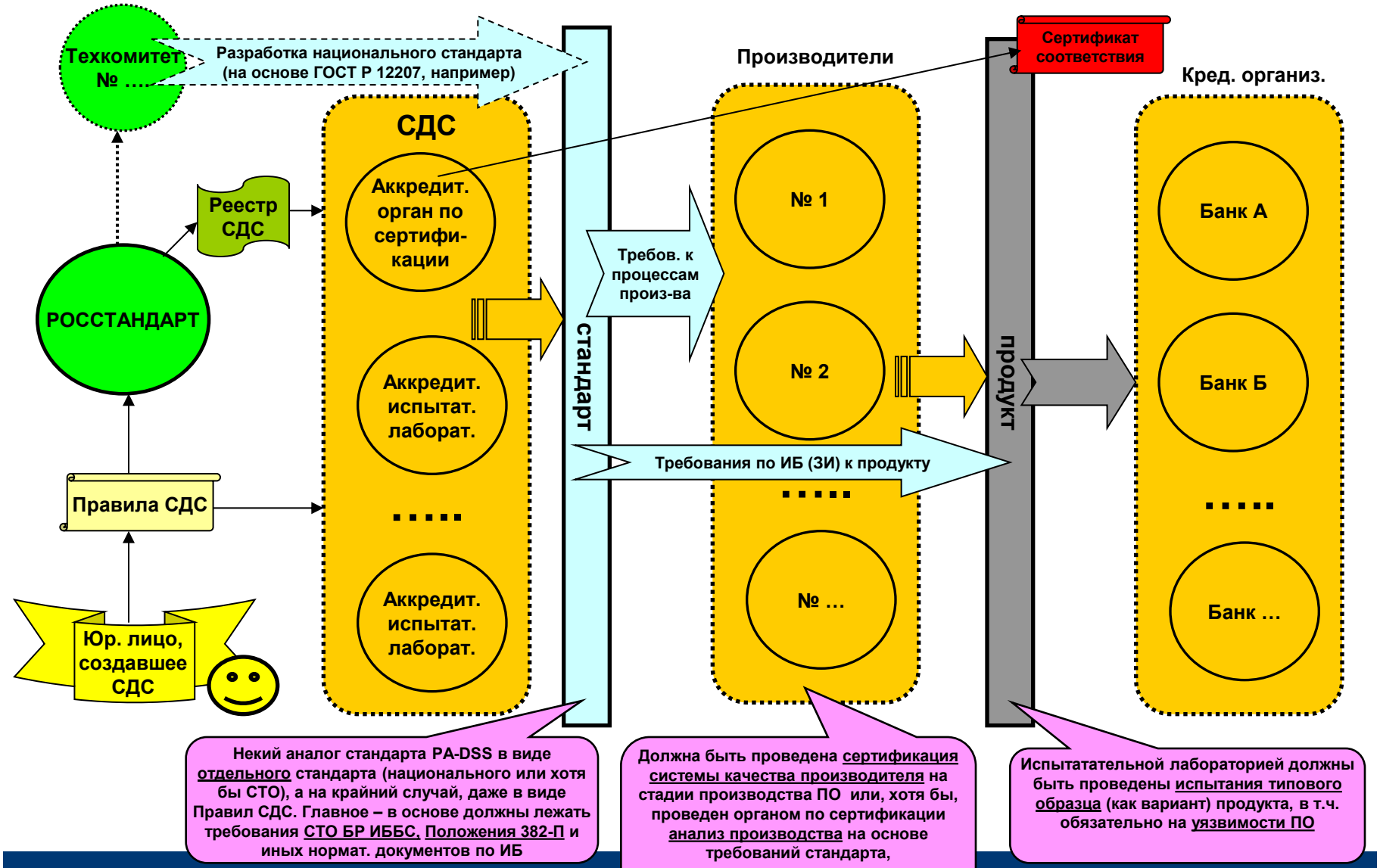
Рег. номер	**РОСС RU.0001.030001**
Дата регистрации	15.11.1993
Наименование системы сертификации	**Система сертификации средств криптографической защиты информации**
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
Федеральное агентство правительственной связи и информации при Президенте Российской Федерации	нет информации
Область распространения системы (объекты сертификации)	Шифровальные средства, системы и комплексы телекоммуникаций высших органов государственной власти Российской Федерации, закрытые системы и комплексы телекоммуникаций органов государственной власти субъектов Российской Федерации, центральных органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности и форм собственности, информационно-телекоммуникационнных систем и баз данных государственных органов, Центрального банка Российской Федерации, Внешэкономбанка и их учреждений, иных государственных учреждений Российской Федерации

Системы добровольной сертификации
(примеры)

Рег. номер	РОСС RU.3103.04ТР00
Дата регистрации	04.10.2004
Наименование системы сертификации	Система добровольной сертификации автомототехники "За рулем"
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
ЗАО "Книжно-журнальное издательство "За рулем"	107045, г. Москва, Селиверстов пер., д. 10, стр. 1, (095) 7374243/7374307
Область распространения системы (объекты сертификации)	Транспортные средства, прицепы к транспортным средствам, запасные части, принадлежности к транспортным средствам, расходные материалы для эксплуатации транспортных средств, средства для ремонта и технического обслуживания транспортных средств.

Рег. номер	РОСС RU.0116.04БМ00
Дата регистрации	21.10.2004
Наименование системы сертификации	Региональная система добровольной сертификации бытовых услуг и систем качества в сфере оказания бытовых услуг в г. Москве
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
Департамент потребительского рынка и услуг города Москвы	125009, г. Москва, ул. Тверская, 19, стр. 2, 2004641, 2005893, 2003433/2003573, dprtms@post.mos.ru
Область распространения системы (объекты сертификации)	Бытовые услуги и системы качества в сфере бытовых услуг

ПРИМЕР ОРГАНИЗАЦИИ СИСТЕМЫ ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ (СДС)



ВОПРОСЫ как ВЫВОД

Кто возьмет на себя функции этих органов и лиц при решении проблемы соответствия прикладного программного обеспечения АБС требованиям по обеспечению информационной безопасности?

Будет ли на все это «действо» воля РЕГУЛЯТОРА (a`la PCI SSC)?

Вопрос в завершении

Зачем же все-таки эта система именно для банков необходима и что она может им дать в итоге хорошего, кроме увеличения стоимости тех самых условно более безопасных банковских приложений?

Ответ
(не бесспорный)

- при применении банком сертифицированных по требованиям безопасности банковских приложений будет иметь место общее снижение операционного риска банка, вопрос может быть лишь о величине этого снижения;
- при организации работы на всех этапах жизненного цикла банковских приложений в соответствии с моделью Деминга (PDCA), возможно достаточно оперативное реагирование на вновь появляющиеся угрозы информационной безопасности банковским приложениям (при условии "обязательности добровольности"!!!, установленной регулятором);
- возможное уменьшение финансовых издержек "законопослушных" банков на приведение банковских приложений в соответствие требованиям по безопасности от регуляторов;
- возможное уменьшение величины репутационного, правового и операционного риска, связанного с регулирующим воздействием регуляторов при проверках (так называемая "защита от регулятора", в России живем);
- некоторое конкурентное преимущество банков, использующих сертифицированные по требованиям безопасности банковские приложения

В заключении

Таков, возможно неоднозначный в чем-то, взгляд со стороны некоторых банков на общую проблему обеспечения безопасности банковских приложений.

При взгляде, условно "за скобками", оставлены не менее проблемные вопросы, тесно связанные с обеспечением безопасности банковских приложений, такие как обеспечение безопасной среды функционирования банковских приложений, создание системы безопасного программирования у разработчика (производителя), сертификация средств защиты информации и другие.

Значимого же реального эффекта при решении вопроса обеспечения безопасности банковских приложений возможно достичь только при комплексном подходе к решению всех вопросов по защите информации в АБС, в т.ч. вопросов, оставленных "за скобками"

Благодарю за внимание!

ВОПРОСЫ?

Презентацию готовили:
Грициенко Андрей Александрович
Начальник Службы информационной безопасности Банка «Возрождение» (ОАО)
Шубин Александр Сергеевич
Главный специалист Службы информационной безопасности Банка «Возрождение» (ОАО)