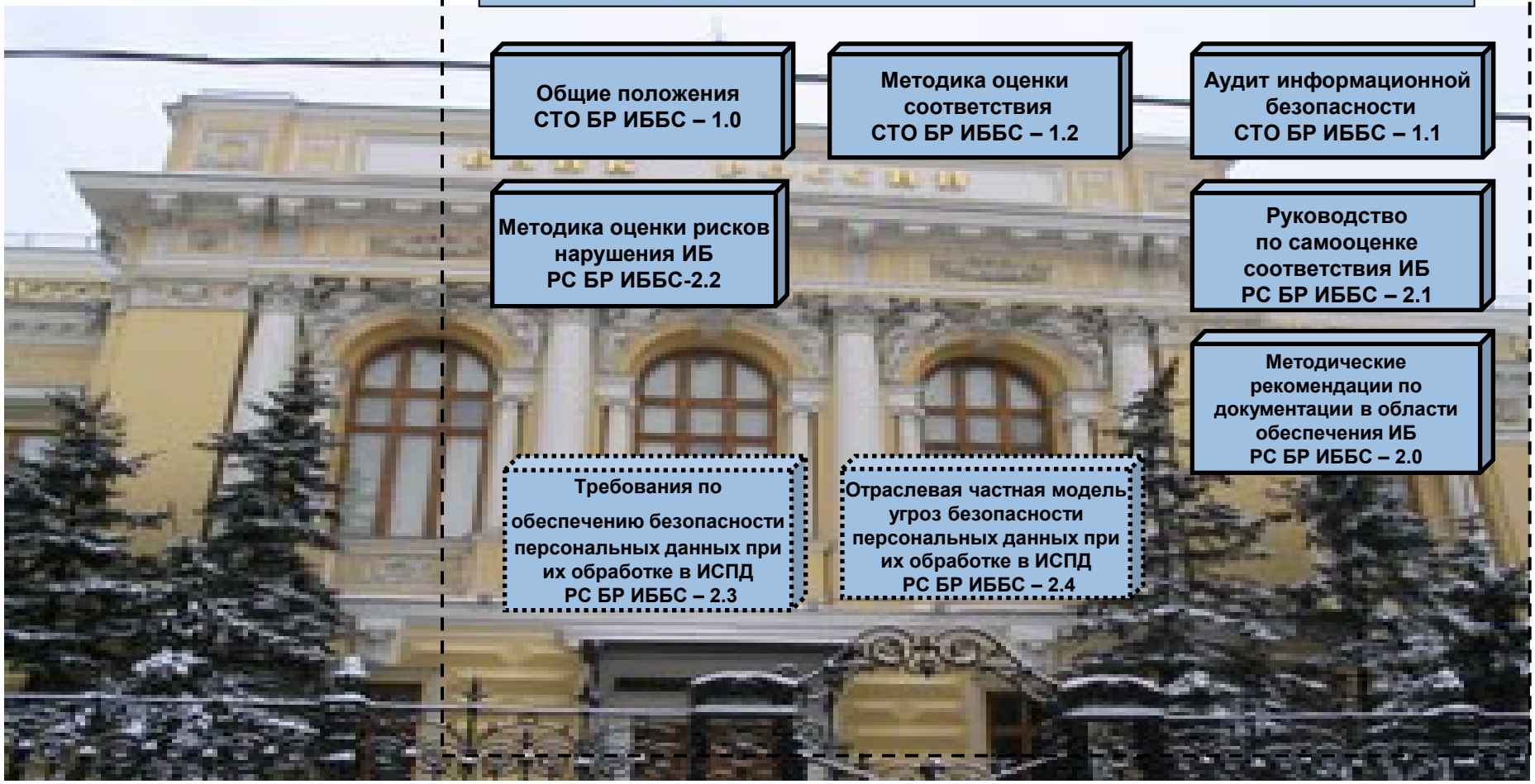
ВОЗРОЖДЕНИЕ БАНК

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

Соответствие программного обеспечения требованиям положения Банка России № 382-П и стандарта СТО БР ИББС-1.0

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

Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»



- Общие положения СТО БР ИББС – 1.0
- Методика оценки соответствия СТО БР ИББС – 1.2
- Аудит информационной безопасности СТО БР ИББС – 1.1
- Методика оценки рисков нарушения ИБ РС БР ИББС-2.2
- Руководство по самооценке соответствия ИБ РС БР ИББС – 2.1
- Методические рекомендации по документации в области обеспечения ИБ РС БР ИББС – 2.0
- Требования по обеспечению безопасности персональных данных при их обработке в ИСПД РС БР ИББС – 2.3
- Отраслевая частная модель угроз безопасности персональных данных при их обработке в ИСПД РС БР ИББС – 2.4

Список организаций БС РФ, информация о принятии решения о введении в действие Комплекса БР ИББС в которых получена Банком России по состоянию на 1 декабря 2012 года

Национальный Банк (НБ) республики Адыгея Банка России (БР)

1. ЗАО АКБ «МайкопБанк»
2. ОАО АКБ «Новация»
3. ООО КБ «ГазтрансБанк»

Главное управление (ГУ) БР по Алтайскому краю

4. ООО КБ «АлтайКапиталБанк»
5. ООО КБ «Тальменка-банк»

……

ГУ БР по Ярославской области

528. ОАО КБ «Верхневолжский»
529. ООО КБ «РБА»
530. ЗАО АКБ «Ярзембанк»
531. ОАО «КредитПромБанк»

= 531 КО

Стандарт СТО БР ИББС-1.0-2010

7.1.3. Требования к СИБ должны быть сформированы в том числе для следующих областей:

- назначения и распределения ролей и обеспечения доверия к персоналу;

- обеспечения ИБ на стадиях ЖЦ АБС;

- защиты от НСД и НРД, управления доступом и регистрацией всех действий в АБС, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.;

- антивирусной защиты;

- использования ресурсов сети Интернет;

- использования СКЗИ;

- защиты банковских платежных и информационных технологических процессов, в том числе банковских технологических процессов, в рамках которых обрабатываются персональные данные

ТАНДЕМ

Положение Банка России № 382-П от 9.06.2012г. «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Указание Банка России № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»

Положение Банка России № 382-П от 9.06.2012г.

2.2. Требования к обеспечению защиты информации при осуществлении переводов денежных средств включают в себя:

- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при назначении и распределении функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании информационно-телекоммуникационной сети Интернет при осуществлении переводов денежных средств;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании СКЗИ;
- требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств;
- требования к организации и функционированию подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации;
- требования к повышению осведомленности работников оператора по переводу денежных средств, банковского платежного агента (субагента), являющегося юридическим лицом, оператора услуг платежной инфраструктуры и клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;
- требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них;
- требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- требования к оценке выполнения оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- требования к доведению оператором по переводу денежных средств, оператором услуг платежной инфраструктуры до оператора платежной системы информации об обеспечении в платежной системе защиты информации при осуществлении переводов денежных средств;
- требования к совершенствованию оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств.

Примеры некоторых условно «проблемных» для банков требований к ПО АБС из СТО БР ИББС-1.0-2010

7.3.5. ….. Также документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты должна содержать описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки.

7.8.9. ….. При проектировании, разработке и эксплуатации систем дистанционного банковского обслуживания должны быть документально определены и выполняться процедуры, реализую щие в том числе механизмы:

- снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;

Примеры некоторых условно «проблемных» для банков требований к ПО АБС из федеральных законов

Федеральный закон от 6.04.2011 г. N 63-ФЗ «Об электронной подписи»

Статья 12. Средства электронной подписи

…….

2. При создании электронной подписи средства электронной подписи должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана.

Федеральный закон от 6.04.2011 г. N 161-ФЗ «О национальной платежной системе»

Статья 9. Порядок использования электронных средств платежа

…….

4. Оператор по переводу денежных средств обязан информировать клиента о совершении каждой операции с использованием электронного средства платежа путем направления клиенту соответствующего уведомления в порядке, установленном договором с клиентом.

6. Оператор по переводу денежных средств обязан фиксировать направленные клиенту и полученные от клиента уведомления, а также хранить соответствующую информацию не менее трех лет.

Промежуточные выводы

1. Несмотря на наличие требований регуляторов по обеспечению ИБ для АБС (в т.ч. для ПО), решить в полной мере вопросы соответствия ПО АБС этим требованиям в рамках индивидуальных договорных отношений заказчиков (банков) и 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.

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.

Как у них?

Организации, попадающие под действие стандарта PCI DSS, получают такие преимущества использования сертифицированных по PA-DSS приложений, как:

- использование более безопасного приложения, чем существенно уменьшает операционный риск;

- возможность оставаться на рынке после начала даты действия стандарта PA-DSS;

- уменьшение количества необходимых мер для выполнения требований PCI DSS, перенося их на разработчика ПО, сокращая тем самым общие расходы на приведение организации в соответствие стандарту PCI DSS;

- использование руководства по безопасному внедрению (Implementation Guide), которое способствует приведению системы организации в соответствие стандарту PCI DSS.

Как у них?

Аудит на наличие программных уязвимостей в рамках сертификации по стандарту PA-DSS предполагает не только статический анализ ПО с использованием типовых специальных программных средств, но и глубокий анализ бизнес-логики приложения и поиск соответствующих уязвимостей в процессе реальной работы приложения, которые позволяют выявить ошибки, относящиеся к классу логических ошибок, которые не обнаруживаются стандартными утилитами.

Примеры у нас

4.2. Члены Партнерства обязаны:

……

- один раз в 2 (два) года подтверждать количество и квалификацию сотрудников на соответствие требованиям, предусмотренным пунктами 3.2, 3.3, 3.4 настоящего Положения;

……

Примеры у нас

ABISS

Association for Banking Information Security Standards
Сообщество пользователей стандартов по информационной безопасности

Некоторые аналогии с системой добровольной сертификации:

- орган по сертификации - АБИСС;
- аккредитованная испытательная лаборатория - член Партнерства;
- правила функционирования системы - Положение о членах Некоммерческого партнерства «Сообщество пользователей стандартов по информационной безопасности АБИСС».

Законодательство по поводу подтверждению 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.

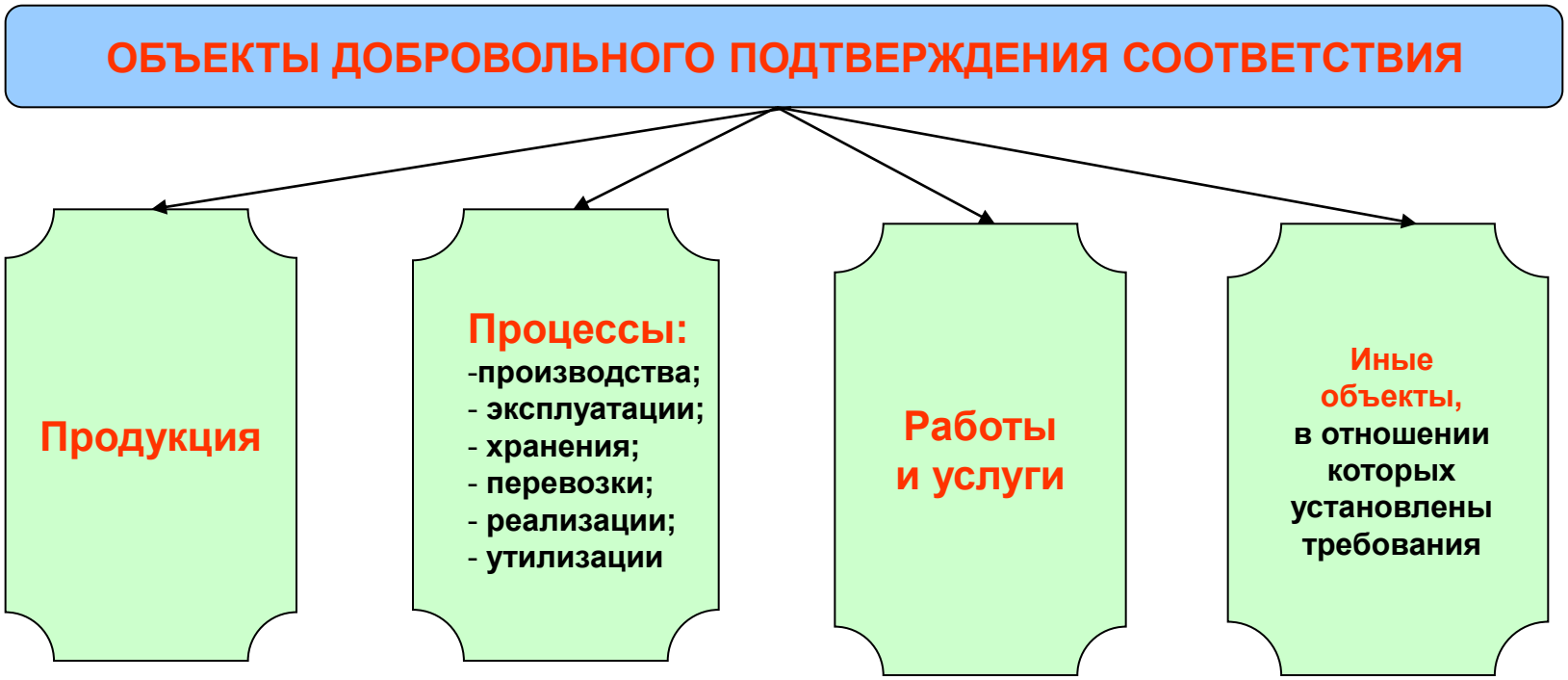
2. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

3. Обязательное подтверждение соответствия осуществляется в формах:

- принятия декларации о соответствии (декларирование соответствия);

- обязательной сертификации

Законодательство по поводу подтверждению соответствия



Законодательство по поводу подтверждению соответствия

В настоящее время Росстандартом в соответствии с Федеральным законом от 27.12.2002 г. № 184-ФЗ «О техническом регулировании» зарегистрированы сотни систем добровольной сертификации

Системы добровольной сертификации

Рег. номер	**РОСС RU.3596.04РГ01**
Дата регистрации	14.10.2009
Наименование системы сертификации	**Система добровольной сертификации информационных технологий для формирования государственных информационных ресурсов "РОСИНТЕХСЕРТ"**
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
ООО **ЦРИОИТ** (ОГРН 106900553932)	170023 г. Тверь, ул. Ржевская, 10, (4822) 44-3173, 44-4044/(4822) 44-4044, gic@tvcom.ru
Область распространения системы (объекты сертификации)	Сети, системы, комплексы и машины вычислительные, устройства центральные вычислительных сетей, систем, комплексов и машин электронных цифровых, устройства периферийные вычислительных комплексов и машин электронных цифровых, устройства межсистемной связи сетей, систем, комплексов и машин вычислительных электронных, устройства вычислительных комплексов и машин аналоговых и аналогово-цифровых, устройства программного управления, устройства сервисные и вспомогательные ЭВМ, носители информации, программно-технические комплексы для автоматизированных систем, системные программные средства, программные средства общего назначения, прикладные программные средства для научных исследований, прикладные программные средства для проектирования, **прикладные программные средства для управления техническими средствами и технологическими процессами, прикладные программные средства для решения организационно-экономических задач**, прикладные программные средства учебного назначения, программно-информационные продукты, программные средства прочие, цифровые карты, планы, услуги сетей передачи данных, услуги телематических служб, услуги по программному обеспечению, консультативные услуги по вопросам систем и программного обеспечения, услуги по системному анализу, по проектированию системы, по программированию задач на ЭВМ, по техническому уходу за системами, по обработке данных и составлению таблиц, по вводу данных, по совместному использованию машинного времени, по созданию банка данных, консультативные услуги, связанные с установкой вычислительной техники, услуги по ремонту вычислительной техники, услуги в научной области, информационное обеспечение ме а качества, системы менеджмента качества и оценка интеллектуальной собственности.
Изображение знака	

Системы добровольной сертификации

Рег. номер	**РОСС RU.И921.04ФДЦ0**
Дата регистрации	02.05.2012
Наименование системы сертификации	**Система добровольной сертификации программного обеспечения и аппаратно-программных комплексов**
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
АНО "Межрегиональный испытательный центр" (ОГРН 1047796578609)	124489 Москва, г. Зеленоград, корп. 601-А, 2 этаж, (499) 976-1428 / (499) 976-1428, info@gametest.ru
Область распространения системы (объекты сертификации)	Операционные системы и языки программирования, системы управления базами данных, программные средства для методоориентированных запросов, для моделирования технологических процессов, математического и иного моделирования, а также исследований, для технико-экономических расчетов, для автоматизированного проектирования, для автоматизированных систем управления технологическими процессами, приборами, оборудованием, установками, станками и промышленными роботами, программные средства диагностические, для автоматизированных рабочих мест, для решения организационно-экономических задач, для автоматизированных систем контроля и учета энергоресурсов, учебного назначения, демонстрационные, досуговые, для тренажеров и иных имитационных систем, защиты и восстановления информации, программное обеспечение средств измерений, систем управления, информационно-измерительных систем, контроллеров и вычислительных блоков, устройств с измерительными фукнциями, для передачи, хранения, актуализации, защиты, обеспечения доступа и использования измерительной, вычислительной и иной информации, развлекательных игровых автоматов, аттракционов, тотализаторов, букмекерских контор, лотерейного оборудования, виртуальных игр, платежных терминалов, торгового оборудования, баз данных, информационных и информационно-справочных систем, электронных архивов, для мультимедиа, аттестованное обеспечение программных средств и информационных продуктов вычислительной техники, аттестованно-программные комплексы.
Изображение знака	ПО

Системы добровольной сертификации

Рег. номер	**РОСС RU.М089.04ИТ00**
Дата регистрации	30.06.2003
Наименование системы сертификации	**Система добровольной сертификации средств информационных технологий по требованиям информационной безопасности (Система "АйТиСертифика")**
Область распространения системы (объекты сертификации)	Технические средства защиты информации от утечки по техническим каналам, включая средства контроля эффективности принятых мер защиты информации, основные и вспомогательные технические средства и системы в защищенном исполнении, средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности, средства контроля эффективности применения средств защиты информации, системы управления и контроля опасными производственными объектами, защищенные программные средства обработки информации, программные средства общего назначения, контрольно-кассовые машины, средства защиты информации, передаваемой по сетям электросвязи, системы и средства
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
Евро-Азиатская Ассоциация производителей товаров и услуг в области безопасности (Ассоциаиця "ЕВРААС")	115280, Москва, ул. Автозаводская, 19, корп. 2, (495) тел.: 748-09-44, факс: 674-60-18, evraas@evraas.ru

Системы добровольной сертификации

Рег. номер	**РОСС RU.В244.04ИН01**
Дата регистрации	29.07.2005
Наименование системы сертификации	**Система добровольной сертификации средств и систем в сфере информатизации "Росинфосерт"**
Организация, представившая систему на регистрацию	Адрес, телефон, e-mail
ФГУП "Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации"	115114, г. Москва, 2-й Кожевнический пер., 4/6, (095) 2355809/2355267, vniipvti@pvti.ru
Область распространения системы (объекты сертификации)	Вычислительные средства, программные средства, программно-информационные продукты, системы менеджмента качества.

Системы добровольной сертификации

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

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

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
ПРИКАЗ
от 30 ноября 2010 г. № 631-ст

ОБ УТВЕРЖДЕНИИ НАЦИОНАЛЬНОГО СТАНДАРТА

В соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании"

приказываю:

1. Утвердить для добровольного применения национальный стандарт Российской Федерации **ГОСТ Р ИСО/МЭК 12207-2010 "Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств",** идентичный международному стандарту ИСО/МЭК 12207:2008 "Системная и программная инженерия. Процессы жизненного цикла программных средств", **с датой введения в действие 1 марта 2012 г.** взамен ГОСТ Р ИСО/МЭК 12207-99.

Отменить ГОСТ Р ИСО/МЭК 12207-99 с 1 марта 2012 г.

2. Закрепить утвержденный стандарт за Управлением технического регулирования и стандартизации.

Руководитель Федерального агентства
Г.И.ЭЛЬКИН

ГОСТ Р ИСО\МЭК 12207-2010. ИТ. Системная и программная инженерия. Процессы жизненного цикла программных средств

Стандарт предназначен для представления определенной совокупности процессов, облегчающих связи между приобретающими сторонами, поставщиками и другими правообладателями в течение жизненного цикла программных продуктов.

Настоящий стандарт разработан для сторон, приобретающих системы, программные продукты и услуги, а также для поставщиков, разработчиков, операторов, сопровожденцев, менеджеров (в том числе, менеджеров по качеству) и пользователей программных продуктов

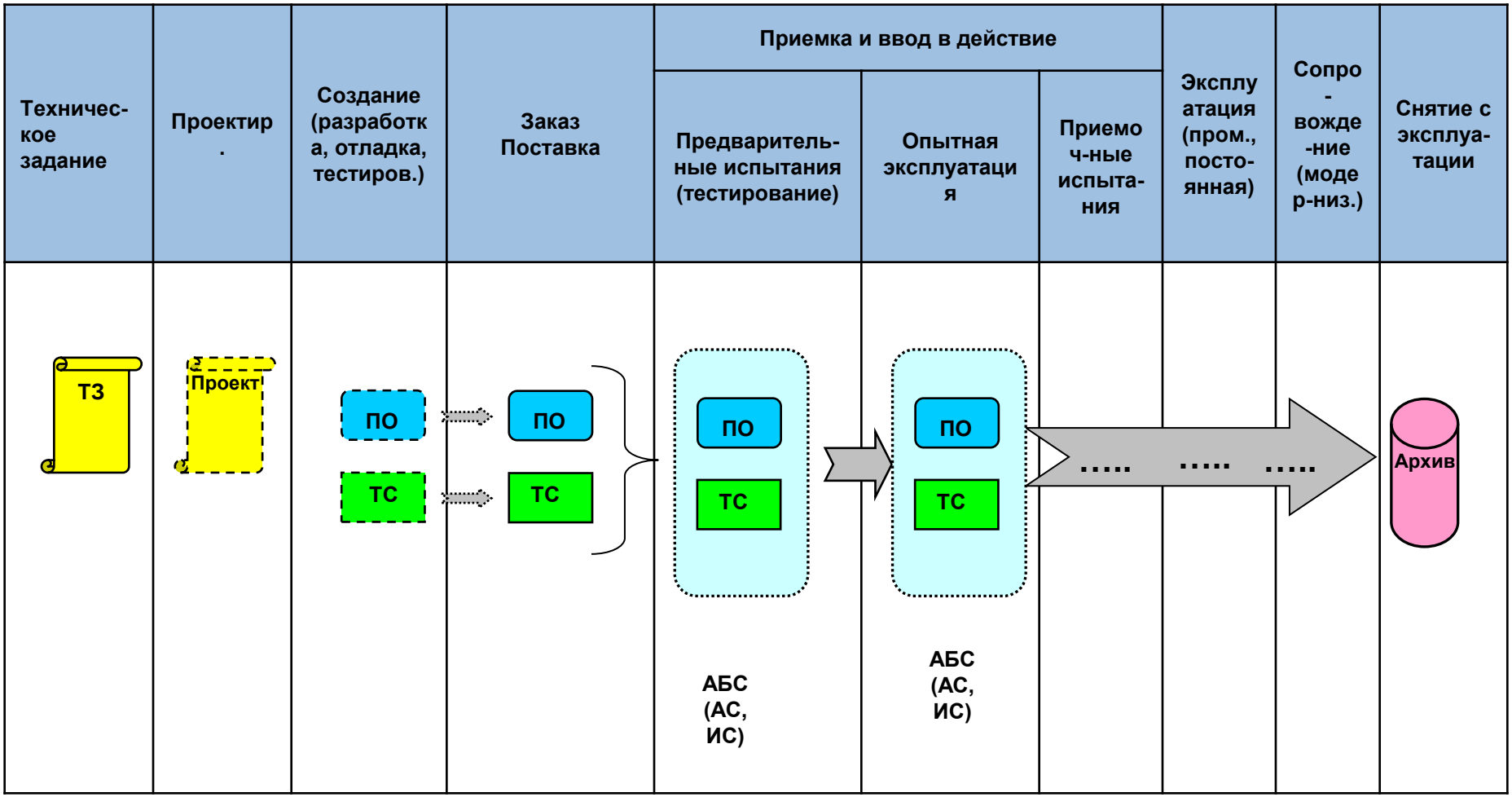
ГОСТ Р ИСО\МЭК 12207-2010. ИТ. Системная и программная инженерия. Процессы жизненного цикла программных средств

Стандарт не устанавливает конкретной модели жизненного цикла системы или программных средств, разработки методологии, методов, моделей или технических приемов.

Стороны, применяющие настоящий стандарт, отвечают за выбор модели жизненного цикла для программных проектов и отображение процессов, действий и задач, представленных в настоящем стандарте, на эту модель.

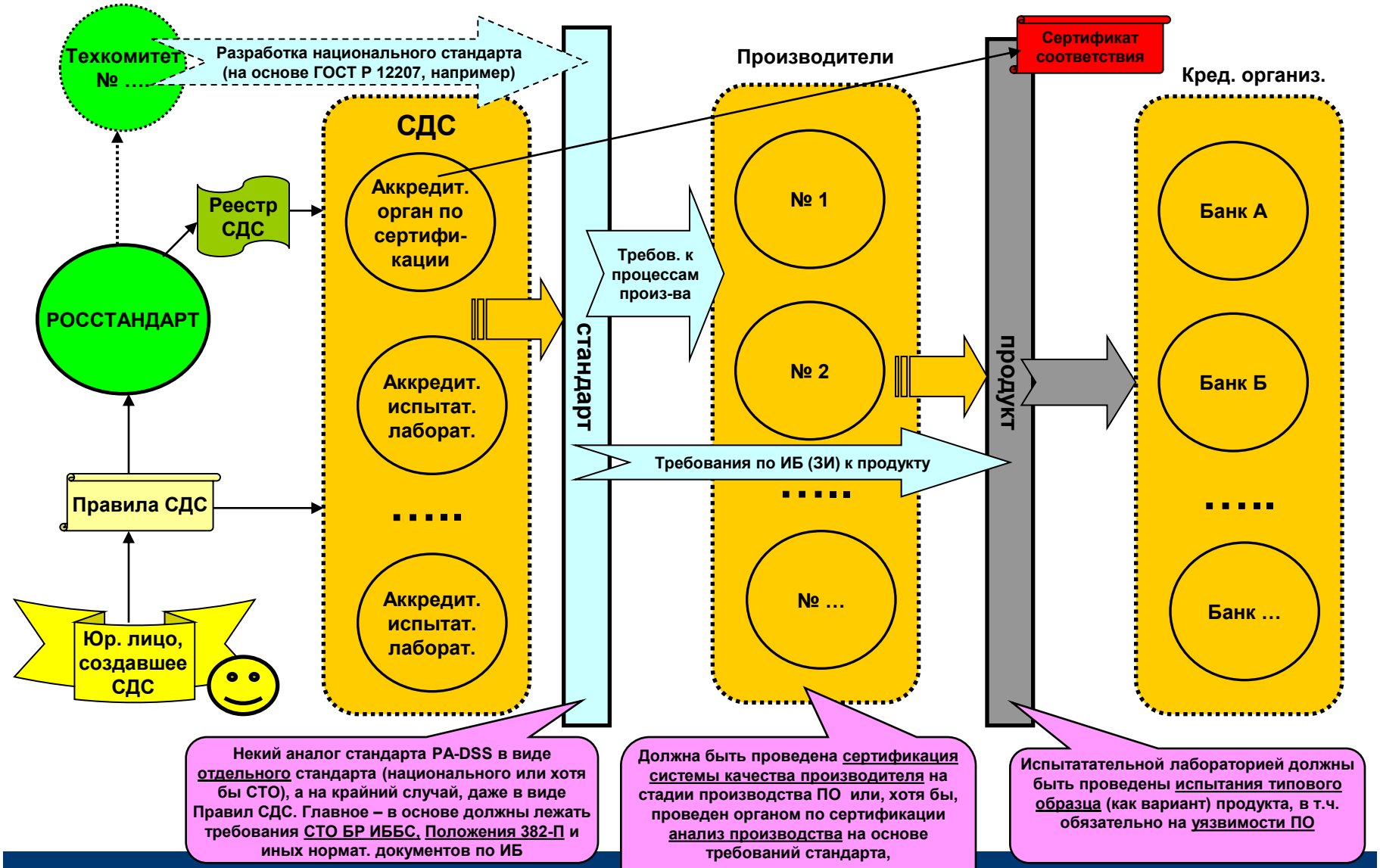
Стороны также ответственны за выбор и применение методов разработки программных средств и за выполнение действий и задач, подходящих для программного проекта.

УПРОЩЕННАЯ СХЕМА
стадий модели жизненного цикла автоматизированных банковских систем



ТЗ – техническое задание, ПО – программное обеспечение; ТС – технические средства, АБС – автоматизированная банковская система; АС – автоматизированная система; ИС – информационная система

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)?

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)