VI Уральский форум: «Информационная безопасность банков»

Association for Banking Information Security Standards

ABiSS

Вопросы регулирования рынка информационной безопасности. Опыт АБИСС и дальнейшие перспективы

Пярин Виктор Анатольевич
Председатель Правления НП «АБИСС»
Действительный член АИН
Член корреспондент РАЕН и Академии криптографии
Лауреат Государственной премии

Республика Башкортостан,
17-22 февраля 2014 г.

www.abiss.ru

Содержание

Календарь событий и этапы развития НП «АБИСС»

- 2004 год – утверждение СТО БР ИББС 1.0-2004
- 2006 год - подписание Меморандума о создании Сообщества пользователей стандартов Банка России (Сообщество ABISS)
- 2006 год - утверждение СТО БР ИББС 1.0-2006
- 2008 год - утверждение СТО БР ИББС 1.0-2008
- 2010 – выход Комплекса документов СТО БР ИББС с учетом требований Роскомнадзора, ФСБ России, ФСТЭК России
- 2011 год – реорганизация Сообщества ABISS в НП «Сообщество пользователей стандартов по информационной безопасности АБИСС»
- 2012 год – Вступление в силу положения ФЗ-161 и ПП РФ №584 «Об утверждении Положения о защите информации в платежной системе», появление 382-П и 2831-У
- 2012 год – расширение сферы деятельности НП «АБИСС». Формирование новых целей и задач
- 2013 год – Изменение Устава и формирование нового состава Правления НП «АБИСС»

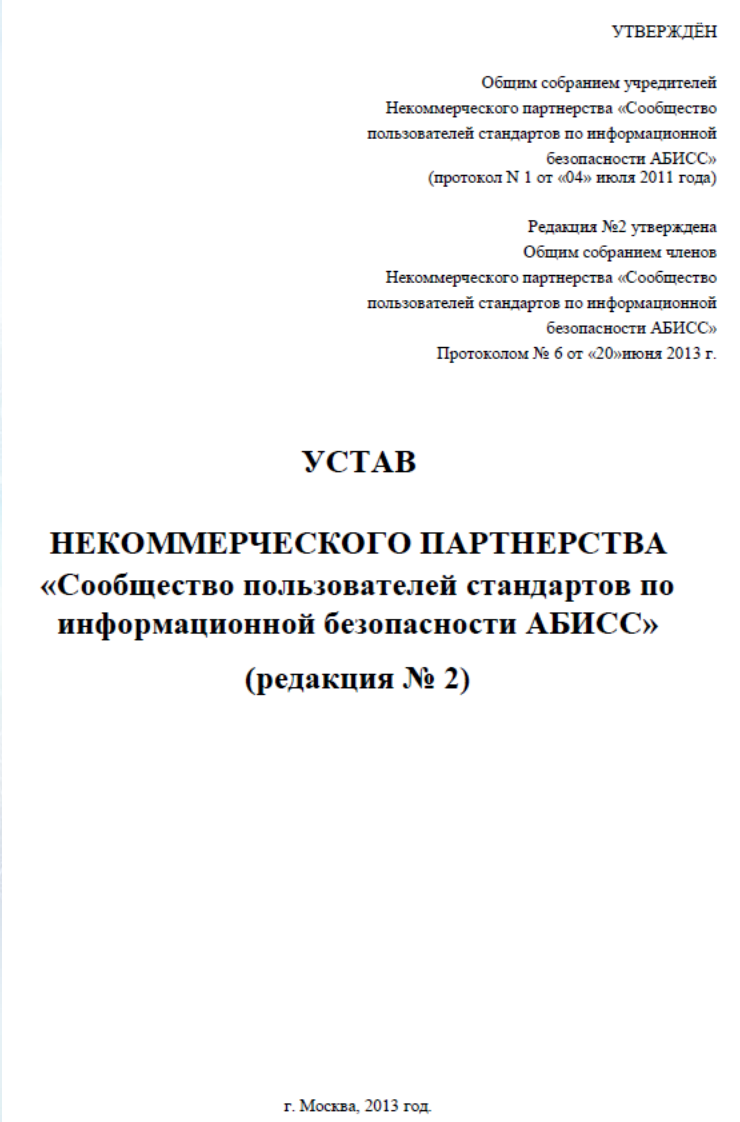
ABISS
НП «АБИСС»

Некоммерческое партнерство «Сообщество пользователей стандартов по информационной безопасности АБИСС»

Изменения Устава

12 августа 2013 года в Единый государственный реестр юридических лиц были внесены сведения о государственной регистрации изменений, вносимых в учредительные документы за номером 2137799125760

Согласно п. 6.1. 2) Правление Партнерства - постоянно действующий коллегиальный орган управления Партнерства, состоящий из 9 (девяти) человек. При этом 6 (шесть) членов Правления Партнерства являются представителями членов Партнерства, а 3 (три) члена Правления Партнерства - независимыми членами.



УТВЕРЖДЁН

Общим собранием учредителей
Некоммерческого партнерства «Сообщество
пользователей стандартов по информационной
безопасности АБИСС»
(протокол N 1 от «04» июля 2011 года)

Редакция №2 утверждена
Общим собранием членов
Некоммерческого партнерства «Сообщество
пользователей стандартов по информационной
безопасности АБИСС»
Протоколом № 6 от «20»июня 2013 г.

УСТАВ

НЕКОММЕРЧЕСКОГО ПАРТНЕРСТВА
«Сообщество пользователей стандартов по информационной безопасности АБИСС»

(редакция № 2)

г. Москва, 2013 год.

Новый состав Правления НП «АБИСС»

Председатель Правления - Пярин Виктор Анатольевич

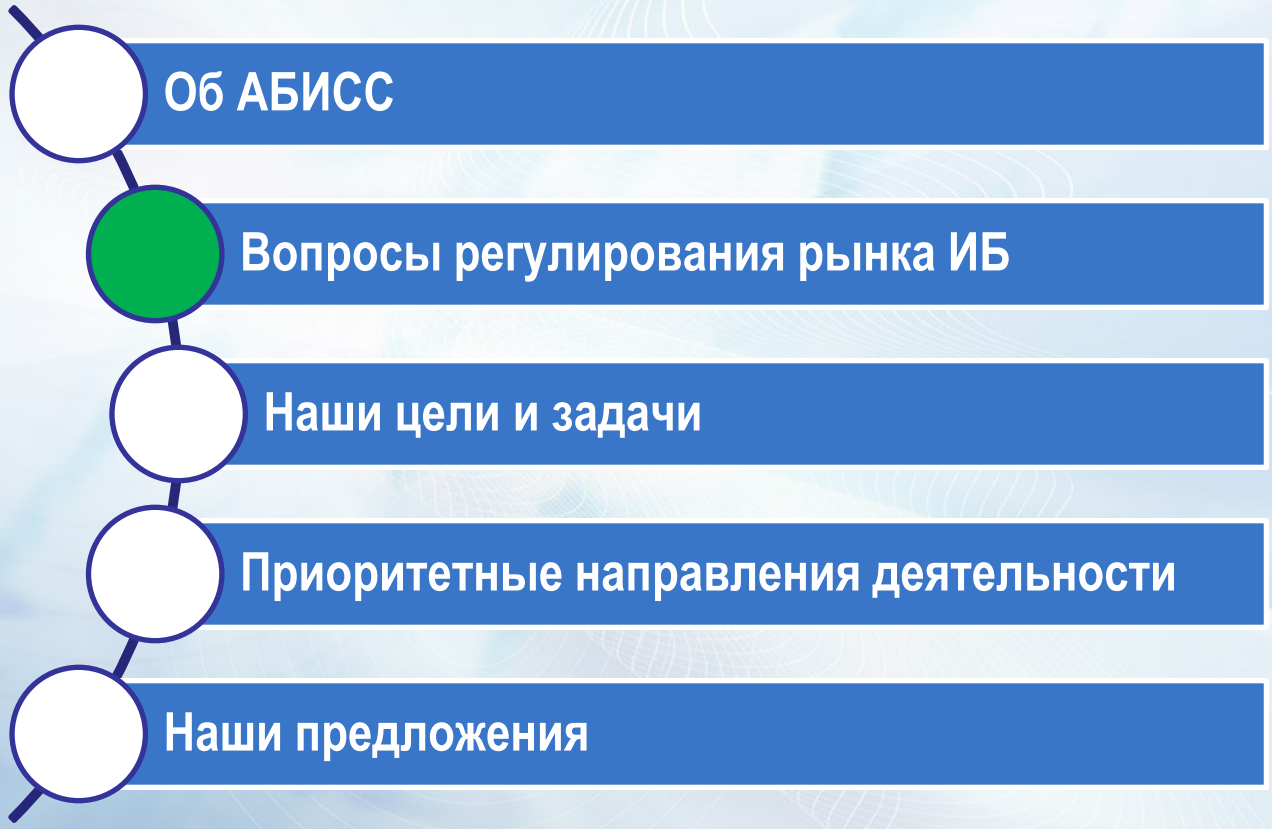
Члены Правления (6 человек):

1. Антимонов Сергей Григорьевич, ЗАО «ДиалогНаука»;
2. Вихорев Сергей Викторович, ОАО «Элвис Плюс»;
3. Гениевский Павел Владимирович, ООО «ПАЦИФИКА»;
4. Левашов Михаил Васильевич, ООО «Инфосекьюрити Сервис»;
5. Малинин Юрий Витальевич, Негосударственное образовательное учреждение дополнительного профессионального образования центр повышения квалификации «АИС»;
6. Решетов Андрей Борисович, ЗАО «РНТ».

Независимые члены Правления (3 человека):

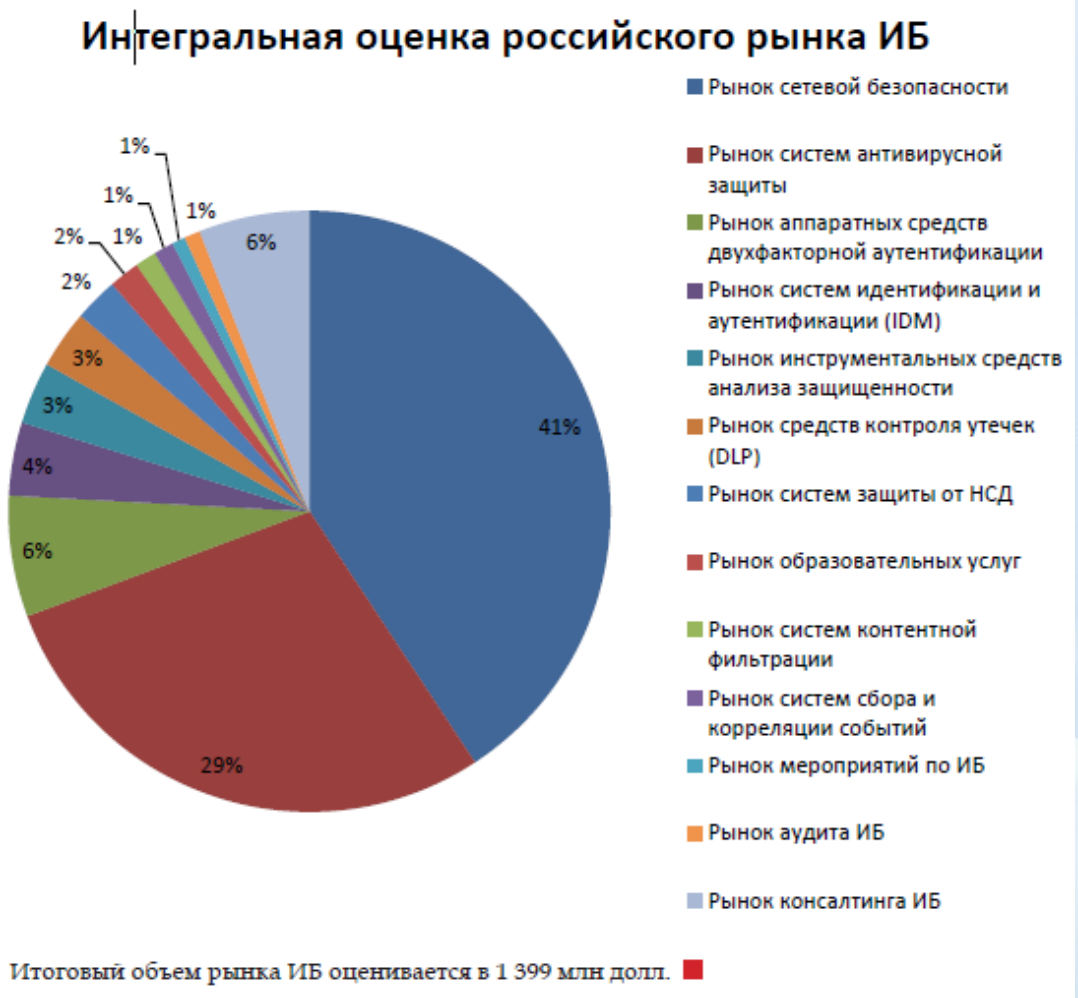
1. Пярин Виктор Анатольевич, Председатель Совета Директоров ЗАО «Орион»;
2. Федоров Борис Васильевич, начальник Управления информационной безопасности НКО ЗАО НРД;
3. Шипилов Валерий Витальевич, исполнительный директор Ассоциации российских банков.

Содержание


Об АБИСС
Вопросы регулирования рынка ИБ
Наши цели и задачи
Приоритетные направления деятельности
Наши предложения

Рынок ИБ в России сегодня

41% российского рынка ИБ представлено решениями отечественного происхождения
29% российского рынка ИБ представлено решениями по антивирусной защите
70% российского рынка ИБ представлено решениями по антивирусной защите и сетевой безопасности
Рынок аудита ИБ в России весьма незначителен (около 1%)
Рынок консалтинга не превышает 5–10% от всего рынка ИБ
Рынок ИБ имеет очевидную тенденцию к росту
Рынок ИБ находится под серьезным регулятивным влиянием, в первую очередь через инструмент сертификации и законодательство
Рынок консервативен, некоторые международные тенденции вроде активного развития облачных сервисов безопасности пока неактуальны для России



Источник: Рынок ИБ в Российской Федерации. Е.Царев и др.

Контроль и регулирование

Государственные органы РФ, контролирующие деятельность в области информационной безопасности:

- Комитет государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба безопасности России (ФСБ России);
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба надзора в сфере информационных технологий и массовых коммуникаций (Роскомнадзор);
- Министерство связи и массовых коммуникаций Российской Федерации (Минкомсвязь России)
- Центральный банк Российской Федерации (Банк России).

Контроль и регулирование

В России отсутствуют СРО в области информационной безопасности (по аналогии СРО в областях финансового аудита, строительства и др.). В мировой практике аналоги СРО в области информационной безопасности существуют, например, PCI Council – Совет в области стандартов безопасности индустрии платежных карт.

Название СРО полное
Некоммерческое партнерство «Аудиторская палата России», НП АПР
Некоммерческое партнерство "Институт Профессиональных Аудиторов", НП ИПАР
Некоммерческое партнерство "Московская аудиторская палата", "МоАП"
Некоммерческое партнерство «Гильдия аудиторов Региональных Институтов Профессиональных бухгалтеров», НП «Гильдия аудиторов ИПБР»
Некоммерческое партнерство «Российская Коллегия аудиторов», НП «РКА»
Некоммерческое партнерство «Аудиторская Ассоциация Содружество», НП ААС

Проблемы

Проблемы заказчиков:

- Система конкурсов и аукционов по 94-ФЗ породила систему срыва поставок продуктов и услуг мошенниками и ОПГ, избавит ли от этого система контрактов?
- Система услуг ИБ, навязанная поставщиками, не развивается
- Отсутствие независимой экспертизы и консалтинга;

Проблемы разработчиков:

- Система сертификации нуждается в реформировании (сроки)
- Недобросовестная конкуренция (обман заказчиков, отсутствие антимонопольности)
- Нет органа, выражающего интересы разработчиков

Проблемы интеграторов

- Обесценивание накопленных компетенций в виду недобросовестной конкуренции;
- Финансовые потери из-за системы конкурсов и аукционов;

Проблемы регуляторов

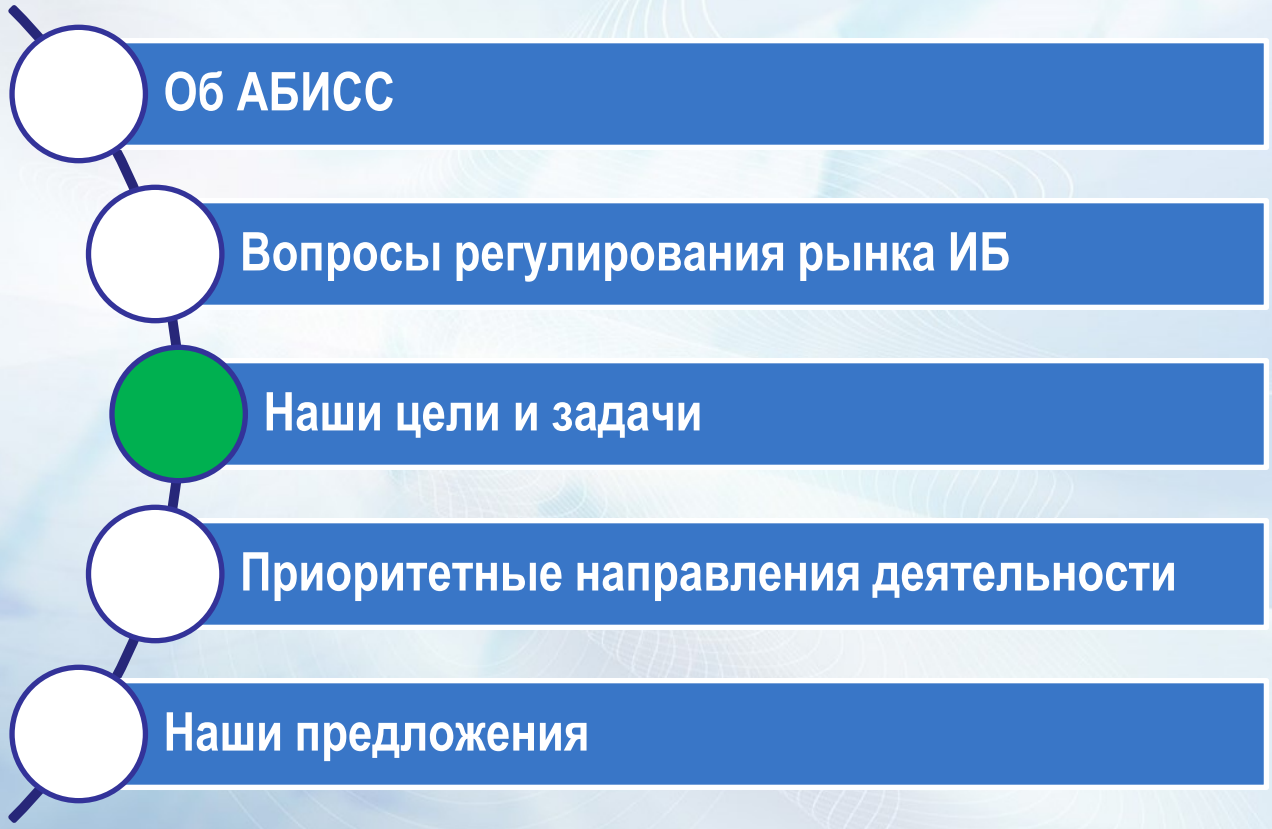
- Невозможность выхода за рамки документа, регулирующего деятельность (пример: ФЗ «О ФСБ»)
- Отсутствие адекватной обратной связи с участниками рынка

Стратегические направления деятельности по решению указанных проблем

- Создание единого центра формирования государственной политики в области информационной безопасности.
- Внедрение механизмов саморегулирования на рынке ИБ.
- Стимулирование на создание **саморегулируемых организаций СРО в области информационной безопасности**
- Внесение изменений в законодательство РФ, позволяющих делегировать определенную часть полномочий по определению механизмов обеспечения информационной безопасности СРО.

Основная идея СРО – возложить часть контрольных и надзорных функций за деятельностью субъектов в определённой сфере на самих участников рынка. При этом собственно государственный надзор в большей степени сосредотачивался бы не на надзоре за деятельностью, а на надзоре за её результатами.

Содержание


Об АБИСС
Вопросы регулирования рынка ИБ
Наши цели и задачи
Приоритетные направления деятельности
Наши предложения

Наши цели и задачи

- Организация системы оценки и контроля качества работы членов НП «АБИСС», включая проведение проверок, соблюдение ими законодательства, регулирующего деятельность по предоставлению услуг в области ИБ;
- Создание инфраструктуры, обеспечивающей выполнение членами НП «АБИСС» на высоком профессиональном уровне услуг ИБ на основе организации их методической поддержки;
- Разработка и внедрение для членов НП «АБИСС» системы профессиональных правил (стандартов), норм профессиональной этики, направленных на повышение их профессионального уровня, престижа и конкурентоспособности аудиторов и консультантов по информационной безопасности;
- Расширение рынка услуг ИБ для членов НП «АБИСС» путем развития сотрудничества с отраслевыми профессиональными объединениями, органами государственной власти, влияющими на развитие рынка услуг ИБ в России и другими общественными институтами;

Наши цели и задачи

- Установление правил этики конкуренции на рынке обеспечения безопасности ИТУ, противодействие монополизации рынка защиты информации, содействие интеграции России в мировое информационное пространство;
- Разработка и согласование с участниками рынка рекомендаций по обеспечению безопасности информационных систем, в том числе информационных систем персональных данных (за исключением ИС критически важных объектов), информационно-телекоммуникационных сетей и других сетей связи. В т.ч. разработка стандартов ИБ для новых информационных технологий. Согласование стандартов с Минкомсвязи России, ФСТЭК России и ФСБ России;
- **Организация системы добровольной сертификации** организаций, продуктов и услуг, в том числе, новых информационных технологий, на соответствие требованиям (рекомендациям) по ИБ, установленным стандартами СРО (цель этого пункта - ускорение внедрения новых ИТ за счет сокращения времени сертификации новых технологий, продуктов и услуг);

Наши цели и задачи

- сертификация (аудит) организаций, продуктов и услуг в области обеспечения ИБ информационных систем, в т.ч. ИСПДн (за исключением ИС КВО), ИТС и других СС;
- защита интересов членов организации при разработке и изменении российского и международного законодательства и стандартов в области ИБ, применении норм права в области ИБ, в том числе законодательства по ПДн;
- взаимодействие с уполномоченным органом по защите прав субъектов ПДн (Роскмонадзор) при регулировании отношений между субъектами ПДн и участниками рынка ИТУ;
- содействие Минкомсвязи России, ФСТЭК России и ФСБ России при разработке требований (рекомендаций) по обеспечению ИБ и безопасности ПДн для рынка ИТУ (т.е. отраслевых НПА по обеспечению ИБ и безопасности ПДн);
- Внесение предложений от участников Партнерства в регулирующие органы по изменению законодательства по вопросам защиты банковской и др. тайн, а также защиты персональных данных

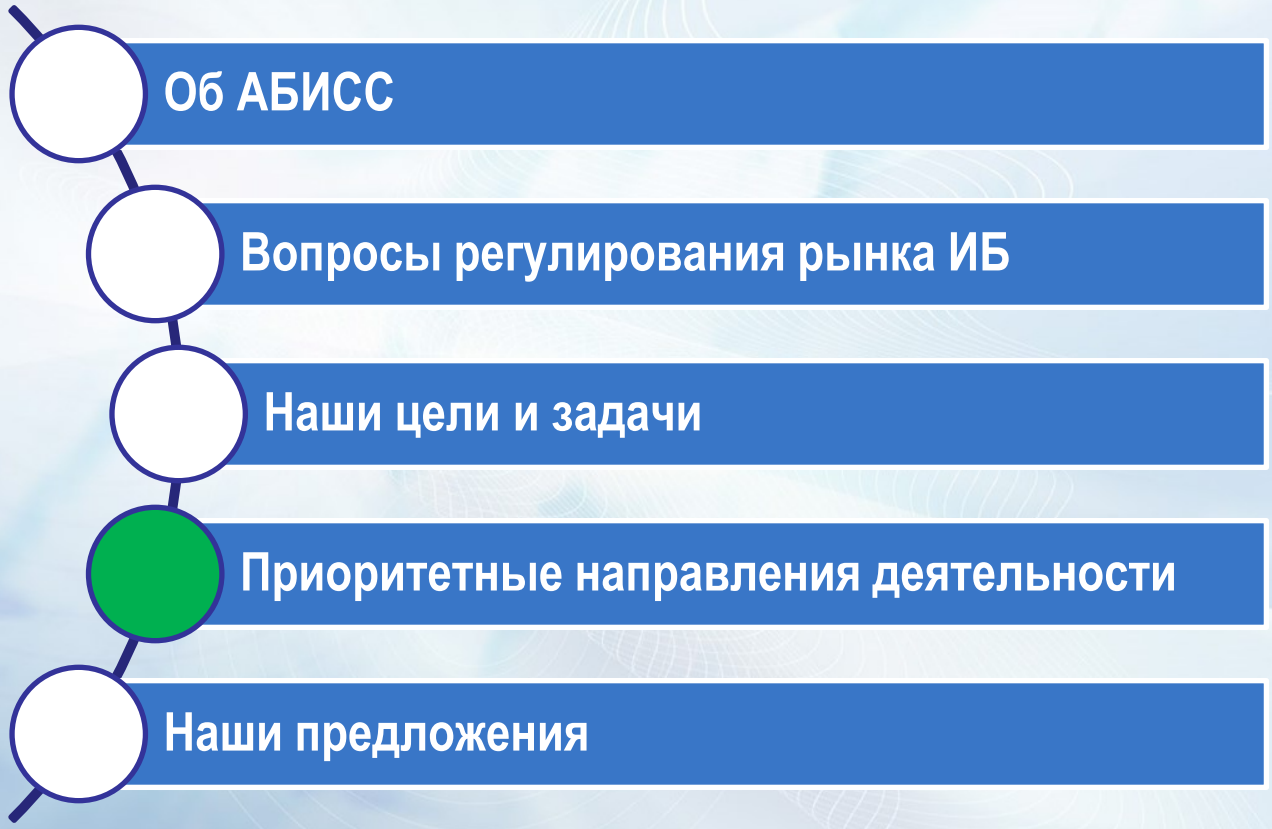
Наши цели и задачи

- индивидуальное позиционирование членов НП «АБИСС» в профессиональной и клиентской среде, в отраслевых профессиональных объединениях и общественных институтах;
- популяризация членов НП «АБИСС» путем организации и проведения специализированных мероприятий:
  - рекламно-имиджевых (форумы, конференции, круглые столы, выставки);
  - учебно-консультационных (семинары, круглые столы, дискуссионные клубы, тренинги).
- аккредитация учебных центров и ведение их реестра;
- организация и осуществление издательской и полиграфической деятельности, выпуск и распространение печатной продукции и других средств массовой информации (в том числе электронных), отвечающих профессиональным запросам членов НП «АБИСС»;
- проведение мероприятий совместно с представителями средств массовой информации и общественности, направленных на повышение престижа и деловой репутации членов НП «АБИСС»;

Наши цели и задачи

- содействие развитию международного сотрудничества в сфере предоставления услуг по информационной безопасности, установление деловых связей с национальными и зарубежными профессиональными объединениями в этой сфере, участие в организации и проведении национальных и международных конгрессов, симпозиумов, конференций, семинаров, презентаций, специализированных выставок и иных мероприятий;
- развитие региональной сети НП «АБИСС» во всех субъектах Российской Федерации, создание единого пространства в сфере услуг ИБ, обеспечивающего доступность и возможность свободного выбора исполнителя услуг ИБ на всей территории Российской Федерации;
- формирование системы поощрения наиболее активных членов НП «АБИСС», руководителей и специалистов;
- организация работы горячей линии по актуальным вопросам, связанным с предоставлением услуг ИБ;

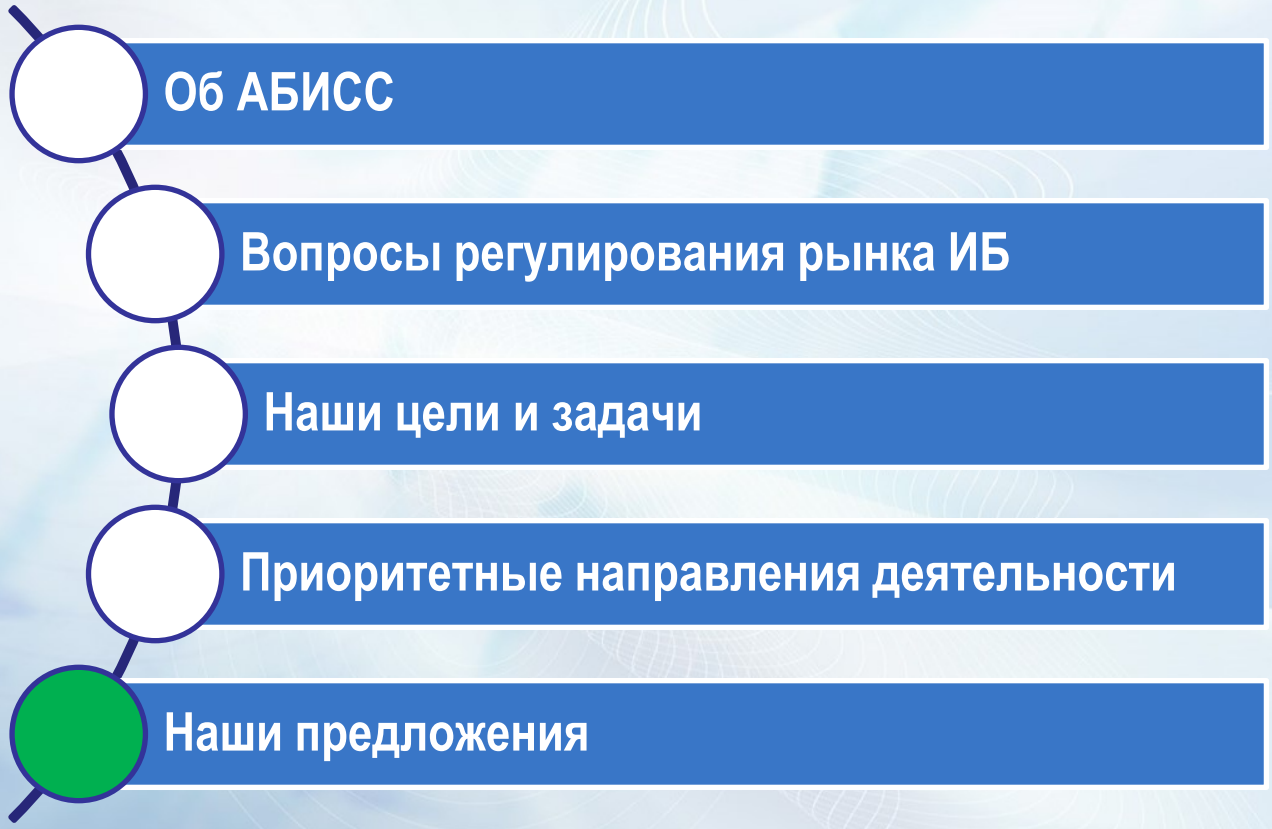
Содержание


Об АБИСС
Вопросы регулирования рынка ИБ
Наши цели и задачи
Приоритетные направления деятельности
Наши предложения

Приоритетные направления на 2014 год

- Завершение создания системы контроля качества, формирование Комитета по контролю качества
- выполнение необходимых условий для регистрации НП «АБИСС» как СРО, в частности:
  - ✓ обеспечение наличия минимального количества ее членов – не менее 25 субъектов предпринимательской деятельности или не менее 100 субъектов профессиональной деятельности.
  - ✓ принятие в строго легитимном порядке и в установленной федеральным законодательством и внутренними нормативными актами СРО форме обязательных стандартов и правил предпринимательской и профессиональной деятельности, под которыми понимаются требования к осуществлению предпринимательской или профессиональной деятельности, обязательные для выполнения всеми членами будущего СРО.
  - ✓ обеспечение дополнительной имущественной ответственности СРО, что обеспечивается наличием компенсационного фонда СРО и коллективного либо индивидуального страхования ответственности членов СРО.
- Получение статуса СРО.

Содержание


Об АБИСС
Вопросы регулирования рынка ИБ
Наши цели и задачи
Приоритетные направления деятельности
Наши предложения

Организация системы добровольной сертификации

Жизненный цикл АБС разделяется на следующие стадии:

- 1) разработка технического задания (ТЗ);
- 2) проектирование;
- 3) создание и тестирование;
- 4) приемка и ввод в действие;
- 5) эксплуатация;
- 6) сопровождение и модернизация;
- 7) снятие с эксплуатации.

И практически на всех перечисленных стадиях в проведении работ участвуют компании- интеграторы, обеспечивающие информационную безопасность .

Организация системы добровольной сертификации

В соответствии с проектом РС БР ИББС-х.х-201х:

Доверие к реализации обеспечения ИБ в АБС возможно только **при наличии определенных свидетельств полноты и корректности проведения мероприятий по обеспечению ИБ на стадиях жизненного цикла компонент АБС**, как минимум специализированных банковских приложений. В качестве свидетельств доверия рекомендуется рассматривать:

- регламенты, используемые для организации деятельности по обеспечению ИБ на этапах жизненного цикла АБС;
- документированные результаты выполнения деятельности по обеспечению ИБ на этапах жизненного цикла АБС.

Таким образом, организация работ на этапах жизненного цикла АБС, которая в полной мере бы обеспечивала возможность контроля с целью установления доверия к проведению всех указанных работ и, соответственно, доверия к реализации обеспечения ИБ в АБС, возможна только при наличии у предприятия (организации) разработчика или соразработчика в части ИБ формализованных регламентов, строго регламентированных процедур, отвечающих всем показателям качества.

Наше предложение

Использовать существующие в АБИСС механизмы саморегулирования (в частности систему контроля качества), для организации системы добровольной сертификации АБС и используемой в их составе совокупности программно-технических средств: телекоммуникационного оборудования, средств вычислительной техники, системного программного обеспечения, прикладного программного обеспечения, а также средств защиты информации, в части обеспечения ИБ, соответствия эксплуатационным и потребительским характеристикам, корректности встраивания и функционирования, оценки негативного влияния СЗИ или СКЗИ на аппаратно- программные телекоммуникационные средства, что будет способствовать:

- обеспечению реализации в АБС необходимых требований к обеспечению ИБ, установленных законодательством РФ, нормативными актами Банка России, СТО БР ИББС-1.0, внутренними документами организации БС РФ;
- снижению рисков нарушения ИБ, связанных с наличием уязвимостей в АБС;
- снижение рисков нарушения ИБ, в том числе рисков утечки информации, на этапе сопровождения, модернизации АБС и вывода из эксплуатации АБС;

Законодательство о подтверждении 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 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

Объекты добровольного подтверждения соответствия			
Продукция	Процессы	Работы и услуги	Иные объекты

Регистрация систем добровольной сертификации проводится Росстандартом

ABISS
НП «АБИСС»

СПАСИБО ЗА ВНИМАНИЕ!

Некоммерческое партнерство
«Сообщество пользователей стандартов
по информационной безопасности АБИСС»

www.abiss.ru