О НОВОЙ ВЕРСИИ СТАНДАРТА БАНКА РОССИИ СТО БР ИББС-1.0-2014 И ДРУГИХ ДОКУМЕНТАХ КОМПЛЕКСА БР ИББС

Антон Свинцицкий
Руководитель отдела консалтинга
ЗАО «ДиалогНаука»

ДиалогНаука

О компании «ДиалогНаука

«ДиалогНаука» является членом:

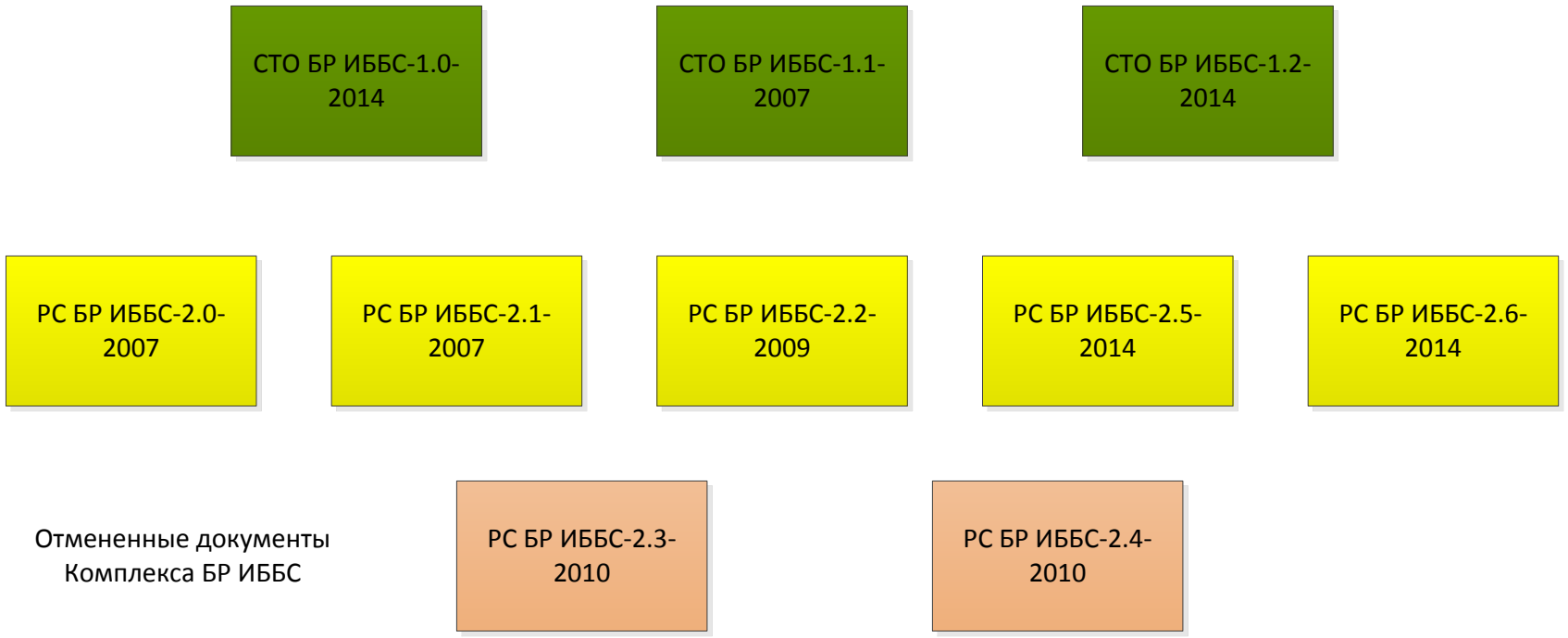
- Межрегиональной общественной организации «Ассоциация защиты информации» (АЗИ),
- Ассоциации документальной электросвязи (АДЭ),
- НП «АБИСС» (Некоммерческого партнерства «Сообщество пользователей стандартов по информационной безопасности АБИСС»)
- Ассоциации предприятий компьютерных и информационных технологий (АП КИТ)
- Консорциума «Инфорус»
- Британского Института Стандартов (British Standards Institution Management Systems)

План презентации

1. О новой версии стандарта Банка России СТО БР ИББС-1.0-2014 (Что изменилось с момента публикации первой версии СТО БР ИББС-1.0-2004).
2. Новые требования в части обеспечения ИБ, определенные в СТО БР ИББС-1.0-2014.
3. Применение стандарта в части обеспечения безопасности персональных данных.
4. Методика оценки соответствия требованиям СТО БР ИББС-1.0-2014 (сложности и плюсы).
5. Новые рекомендации Банка России.

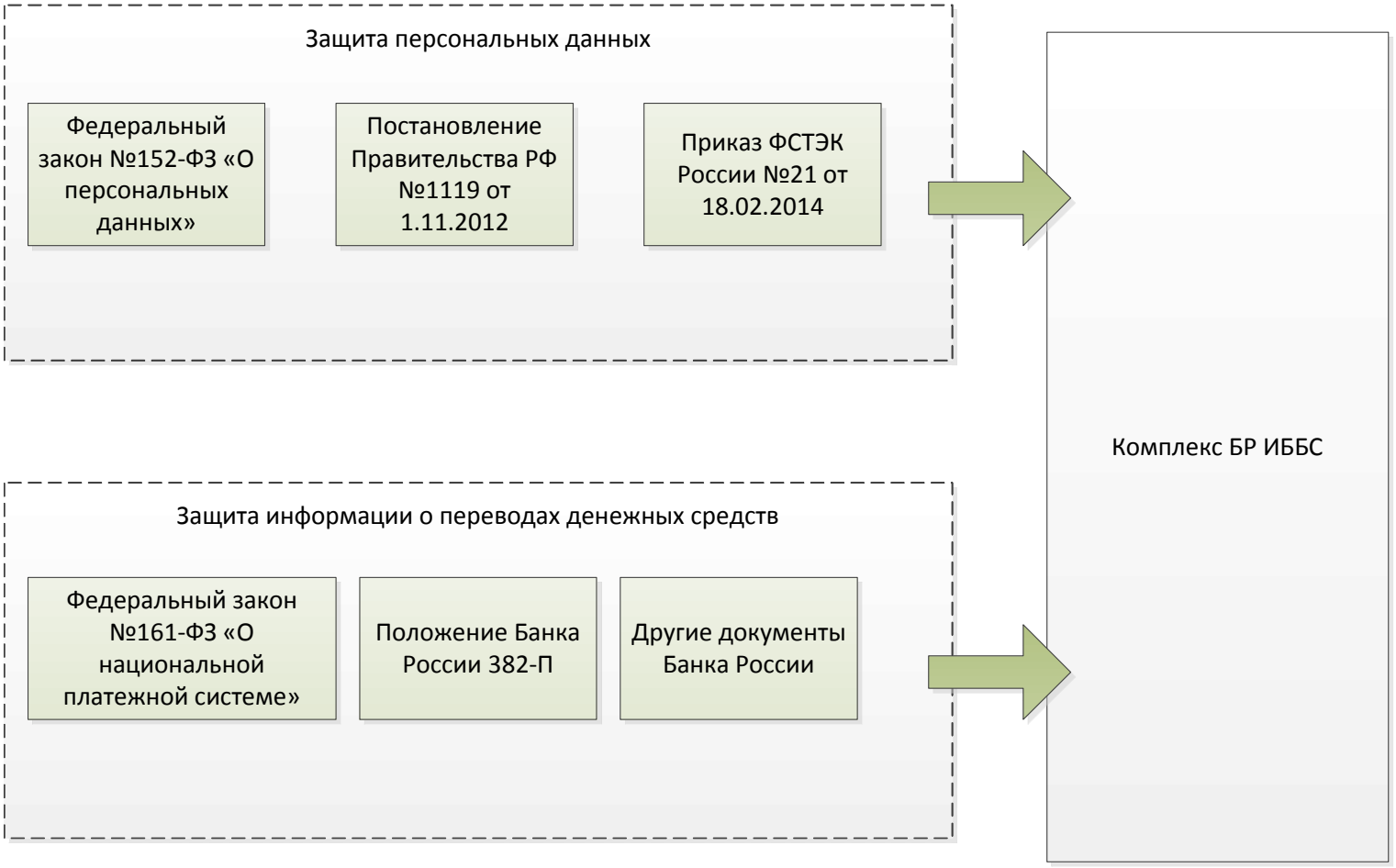
О новой версии стандарта СТО БР ИББС-1.0-2014

1. Новая версия Стандарта Банка России СТО БР ИББС-1.0 введена в действие распоряжениями Банка России от 17 мая 2014 года №Р-399 и №Р-400 и вступила в силу с 1 июня 2014 года.
2. Структура документов Комплекса БР ИББС



О новой версии стандарта СТО БР ИББС-1.0-2014

Внешние требования



О новой версии стандарта СТО БР ИББС-1.0-2014

Основные новые требования, описанные в СТО БР ИББС-1.0-2014:

1. В Стандарте появились детальные требования в части необходимости использования дополнительных мер по обеспечению информационной безопасности в рамках реализации системы информационной безопасности банковских технологических процессов:

- ✓ средств анализа защищенности, направленных на выявление различных классов уязвимостей (требования в разделе 7.3);
- ✓ необходимости регистрации событий и хранения указанных данных (требования в разделе 7.4);
- ✓ требования к сегментации сети и контроля информационных потоков (требования описаны в разделах 7.3, 7.4, 7.6 и 7.9);
- ✓ реализация контроля съемных носителей информации (требования описаны в разделах 7.4 и 7.5);
- ✓ необходимости протоколирования посещения ресурсов сети Интернет (требования в разделе 7.6);
- ✓ требования к банкоматам (требования в разделе 7.8).

О новой версии стандарта СТО БР ИББС-1.0-2014

Основные новые требования, описанные в СТО БР ИББС-1.0-2014:

2. Необходимость использования средства криптографической защиты информации определяется организацией банковской системы Российской Федерации самостоятельно, однако в Стандарте остались ограничения на использование средств криптографической защиты информации для защиты персональных данных – **сертифицированные, не ниже уровня КС2**.

Примечание: для практически любой организации Банковской системы РФ это требования выполнимо только частично…

О новой версии стандарта СТО БР ИББС-1.0-2014

Основные новые требования, описанные в СТО БР ИББС-1.0-2014:

3. Требования в части обеспечения защиты ПДн гармонизированы с требованиями действующего законодательства и подзаконных актов.

Примечание:

В Стандарте появился новый термин «***Ресурс ПДн***» (совокупность персональных данных, обрабатываемых в организации банковской системы Российской Федерации с использованием или без использования средств автоматизации и автоматизированных банковских систем, в том числе информационных систем персональных данных, объединенных общими целями обработки), для которого сформированы требования к документированности отдельных процедур, связанных с обработкой персональных данных (раздел 7.10). В качестве «Ресурсов ПДн» в организации могут быть выделены:

- ✓ персональные данные работников;
- ✓ персональные данные клиентов;
- ✓ персональные данные посетителей;

и т. п.

О новой версии стандарта СТО БР ИББС-1.0-2014

В соответствии с п.7.11.3 Стандарта т**ребования разделов 7 и 8 направлены на нейтрализацию актуальных угроз безопасности персональных данных**, однако в соответствии с п.13г Постановления Правительства Российской Федерации № 1119 от 1.11.2012 средства защиты информации, используемые для нейтрализации актуальных угроз безопасности персональных данных, должны пройти в установленном порядке процедуру оценки соответствия (читать «сертифицированные»).

То есть любое средство защиты, которое внедряется в организации в соответствии с требованиями Стандарта для защиты персональных данных должно пройти оценку соответствия (должно быть сертифицированным), т. е. нельзя использовать встроенные механизмы управления доступом операционной системы для реализации соответствующих мер обеспечения безопасности персональных данных.

А поскольку «требования, установленные в разделах 7 и 8 Стандарта, рекомендуются для выполнения требований к защите персональных данных для 3 и 4 уровней защищенности» и направлены на нейтрализацию актуальных угроз, организациям банковской системы Российской Федерации необходимо выполнять требования Приказа ФСТЭК России № 21 от 18.02.2013 в части реализации мер, описанных в Приложении к данному Приказу.

Остается надеяться на дополнительные разъяснения со стороны Банка России.

Методика оценки соответствия требованиям СТО БР ИББС-1.0-2014

Банком России также была актуализирована методика оценки соответствия информационной безопасности требованиям СТО БР ИББС-1.0-2014 (СТО БР ИББС-1.2-2014). Основные изменения коснулись подхода к оценке:

- ✓ методика приведена в соответствие с подходом, описанным в Положении Банка России № 382-П;
- ✓ все требования отнесены к одному из трех классов (документирование, выполнение, документирование и выполнение);
- ✓ оценка групповых показателей определяется как среднее арифметическое (отсутствуют весовые коэффициенты частных показателей);
- ✓ вводится понятие корректирующих коэффициентов, влияющих на оценки по направлениям и зависящих от количества полностью не реализованных требований Стандарта;
- ✓ значение показателя М9 (Общие требования по обработке персональных данных) рассчитывается по общей схеме (не как минимальное из значений входящих частных показателей в предыдущей версии Стандарта).

Методика оценки соответствия требованиям СТО БР ИББС-1.0-2014

Оценка выполнения требования СТО БР ИББС-1.0-2014 должна осуществляться с учетом результатов оценки выполнения требования Положения 382-П.

Частный показатель С ТО БР ИББС-1.2-2014	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П
М7.9	П.72
	П.73
	П.77

Например, оценка показателя **М7.9** не может быть выше минимальной из оценок по 382-П **П.72, П.73, П.77…**

Методика оценки соответствия требованиям СТО БР ИББС-1.0-2014

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ, отнесенного к Категории 1
0	Требования частного показателя ИБ не установлены (определены) во внутренних документах проверяемой организации
0,25	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации, но не выполняются
0,5	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации, но выполняются в неполном объеме
0,75	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации и выполняются почти в полном объеме
1	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации и выполняются в полном объеме

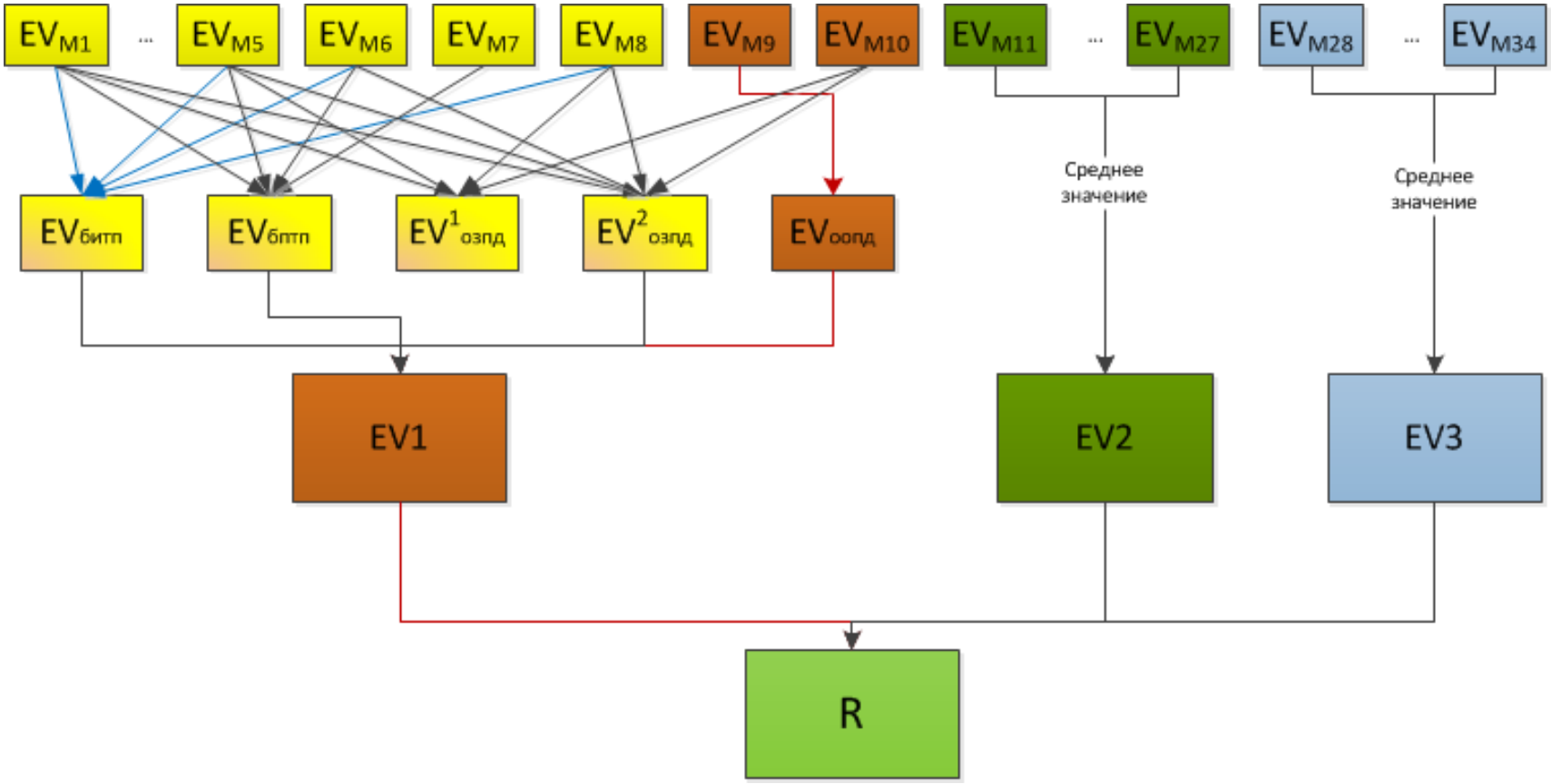
Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ, отнесенного к Категории 2
0	Требования частного показателя ИБ не установлены во внутренних документах проверяемой организации
1	Требования частного показателя ИБ полностью установлены во внутренних документах проверяемой организации

Методика оценки соответствия требованиям СТО БР ИББС-1.0-2014

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ, отнесенного к Категории 3
0	Требования частного показателя ИБ не выполняются
0,5	Требования частного показателя ИБ выполняются в неполном объеме
1	Требования частного показателя ИБ выполняются в полном объеме

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ, отнесенного к Рекомендуемым
н/о	Требования частного показателя ИБ не выполняются
1	Требования частного показателя ИБ полностью выполняются

Методика оценки соответствия требованиям СТО БР ИББС-1.0-2014



Примечание: появились корректирующие коэффициенты для итоговых значений по направлениям. В случае оценки хотя бы по одному из частных показателей равна 0, **итоговая оценка не может быть больше или равна 0,85.**

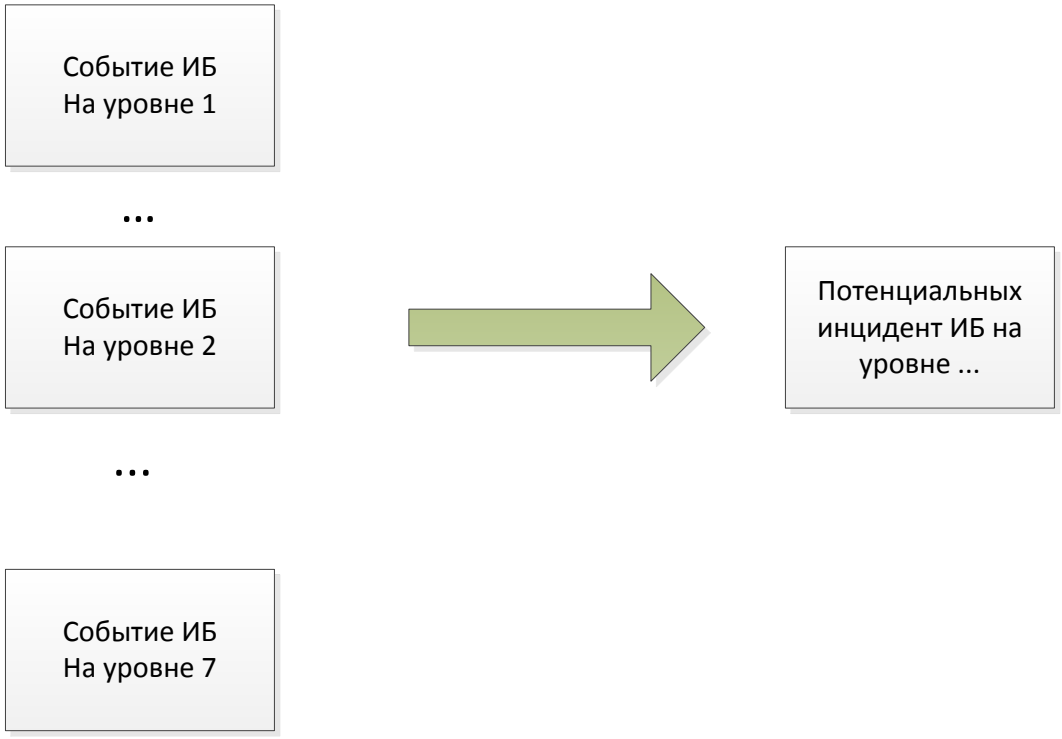
Рекомендации Банка России РС БР ИББС-2.5-2014

В дополнение Банком России были выпущены новые рекомендации в части управления инцидентами информационной безопасности РС БР ИББС-2.5-2014, основанные на рекомендациях ISO/IEC TR 18044:2004. Рекомендации РС БР ИББС-2.5-2014 содержат:

- ✓ описание подхода к построению процессов менеджмента инцидентов информационной безопасности на основе циклической модели Деминга;
- ✓ описание задач, решаемых на каждой стадии обработки инцидентами информационной безопасности;
- ✓ описание организационной структуры менеджмента инцидентов информационной безопасности;
- ✓ рекомендации по документированию процесса менеджмента инцидентов информационной безопасности;
- ✓ рекомендации по использованию специализированных средств при обработке (в том числе для обнаружения) инцидентов информационной безопасности;
- ✓ рекомендации по классификации инцидентов информационной безопасности.

Рекомендации Банка России РС БР ИББС-2.5-2014

Определены типы событий, которые могут использоваться для выявления потенциальных инцидентов ИБ на всех уровнях среды обработки информационных ресурсов.



Рекомендации Банка России РС БР ИББС-2.6-2014

Банком России также были выпущены новые рекомендации в части обеспечения ИБ на всех стадиях жизненного цикла РС БР ИББС-2.6-2014, содержащие:

- ✓ описание детальных требования по обеспечению ИБ на всех рассматриваемых СТО БР ИББС-1.0 стадиях жизненного цикла АБС:
  - ✓ Разработка ТЗ
  - ✓ Проектирования АБС
  - ✓ Создания и тестирования АБС
  - ✓ Приемки и ввода в действие
  - ✓ Эксплуатации
  - ✓ Сопровождение и модернизация АБС
  - ✓ Снятия с эксплуатации
- ✓ Типовые проблемы обеспечения ИБ в разных процессах;
- ✓ Рекомендации по оценке (проверке) исходного кода;
- ✓ Рекомендации по проведению анализа защищенности (в том числе тестов на проникновение);
- ✓ Рекомендации по соблюдению стандартов конфигурации.

Спасибо за внимание!

Вопросы?

ЗАО «ДиалогНаука»

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru

e-mail: svintsitskii@DialogNauka.ru