



**ВОЗРОЖДЕНИЕ
БАНК**

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

**Практика проведения аудита
по Положению Банка России № 382-П.
Спорные вопросы и способы их решения.
Взгляд Банка**



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

Положение Центрального банка Российской Федерации от 9 июня 2012 г. № 382-П

Глава 2. Требования к обеспечению защиты информации при осуществлении переводов денежных средств

- ОПДС обеспечивает **проведение оценки выполнения требований** к обеспечению защиты информации при осуществлении переводов денежных средств
- ОПДС обеспечивает проведение оценки соответствия **не реже одного раза в два года**, а также по требованию Банка России
- **Организация**, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, **должна провести первую оценку соответствия в течение шести месяцев** после получения соответствующего статуса (Указание Банка России от 5 июня 2013 г. № 3007-У)

СРОКИ ВЫШЛИ !!!



ЧТО ДЕЛАТЬ ?



Зарегистрировано в Минюсте России 14 июня 2012 г. N 24575

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

9 июня 2012 г. N 382-П

**ПОЛОЖЕНИЕ
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**

(в ред. [Указания](#) Банка России от 05.06.2013 N 3007-У)

Оценка соответствия осуществляется оператором

самостоятельно

или

**с привлечением
сторонних организаций**



Самооценка

- ✓ «Бесплатное» проведение
- ✓ Возможность выдать желаемое за действительное
- ✓ Возможность провести оценку за 1 день

Оценка сторонней организацией

- ✓ Объективная оценка текущего уровня информационной безопасности Банка
- ✓ Объективная трактовка требований Положения 382-П
- ✓ Корректно выбранная область оценки (платежные системы, проверяемые подразделения, объекты информационной инфраструктуры и т.д.)
- ✓ Обоснованность выставленной оценки с учетом множества факторов
- ✓ Исключение субъективного завышения (занижения) оценок показателей
- ✓ Обоснованный подбор свидетельств аудита и беспрепятственное их получение в подразделениях Банка
- ✓ Ответственность за обоснованность оценки (качество выполненных работ) ложится на стороннюю организацию

Самооценка

- ✓ Сложность работ
- ✓ Отвлечение персонала от своих основных обязанностей
- ✓ Нужны специалисты соответствующей квалификации
- ✓ **Сомнения в объективности**
- ✓ **Отчет подписывается руководством организации – ответственность на нем**

Оценка сторонней организацией

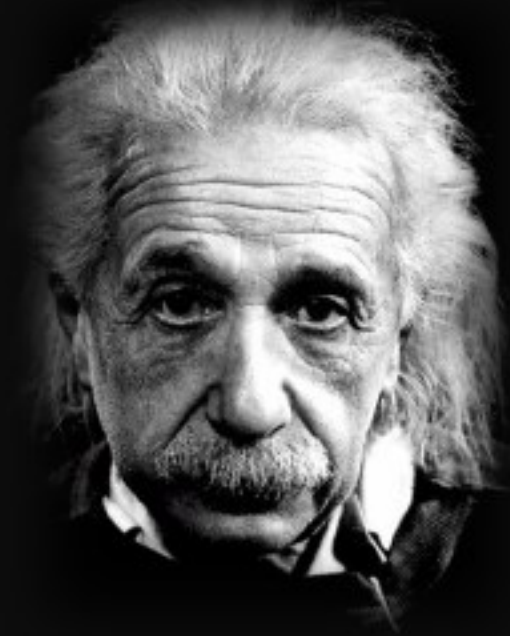
- ✓ Высокая стоимость проведения
- ✓ Профессиональные требования к аудиторам

Выбирать вам!



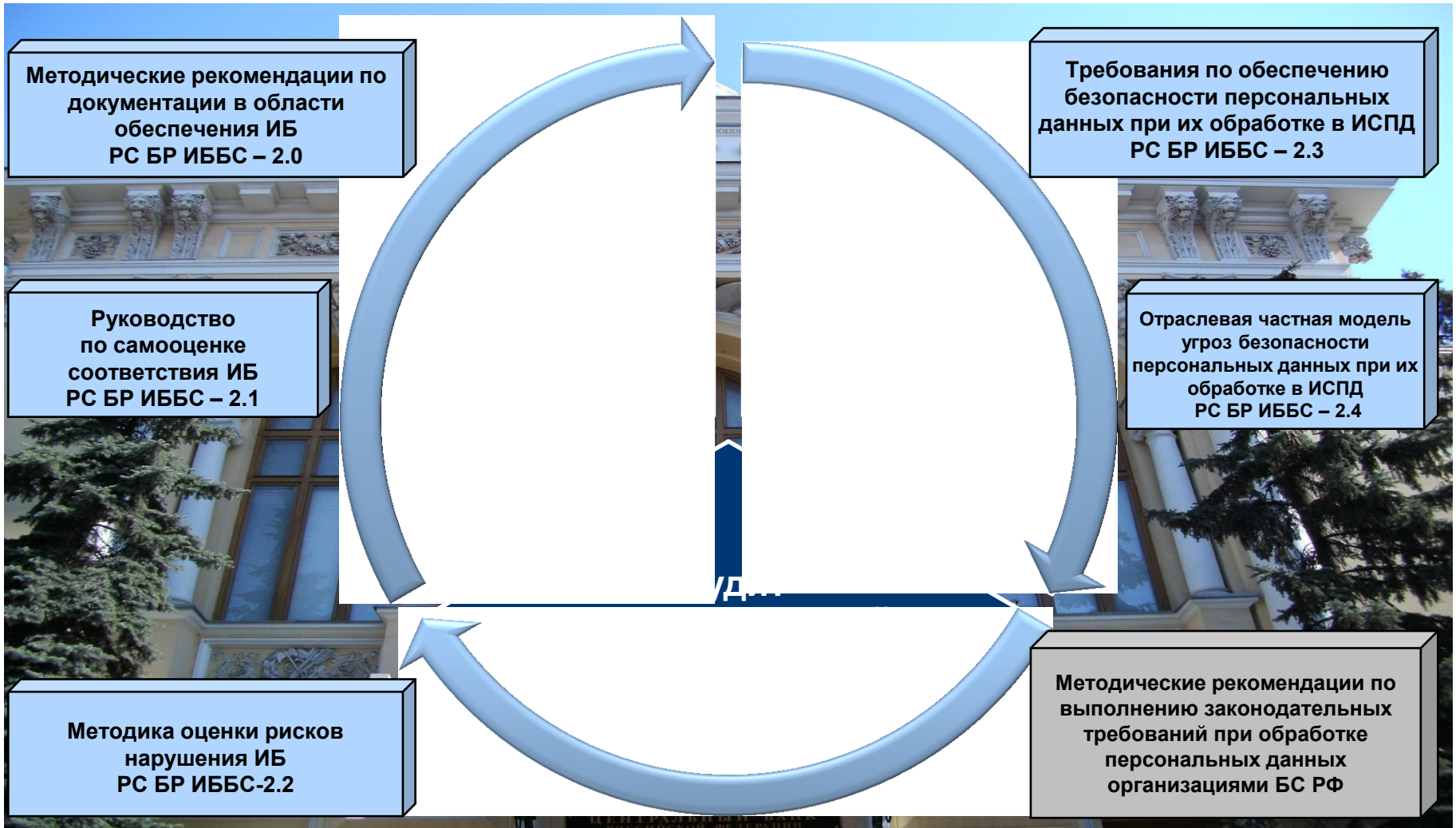
Система не может понять сама себя

*“Мы не сможем
решить наши
проблемы
на том же уровне
мышления,
на котором они
были созданы”.*



*Альберт Эйнштейн
(1879-1955)*

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



Оценка соответствия информационной безопасности банка требованиям стандарта СТО БР ИББС-1.0-2010 в 2010 году

- Оценка соответствия в банке проводилась аудиторской группой ЗАО НИП «Информзащита» в составе **6 человек с 7 октября по 10 декабря 2010 года**
- Оценке были подвергнуты **Центральный аппарат банка** и **филиалы** в Московском регионе и в других субъектах РФ с выездом группы на места
- По различным областям стандарта аудиторской группой было **опрошено 116** сотрудников банка с оформлением конспектов опроса
- В ходе проведения оценки соответствия аудиторской группой было собрано и проанализировано **более 800** документов-свидетельств выполнения процессов обеспечения ИБ



Информзащита
Системный интегратор



Система оценки соответствия по Стандарту ЦБ

Групповые показатели ИБ (М1 - М34)

М1	М2	М3	М4	М5	М6 (СКЗИ)	М7	М8	М9 (ПД)	М10	М11 - М27	М28 - М34
----	----	----	----	----	-----------	----	----	---------	-----	-----------	-----------

Приложение В

Защита ПД без учета СКЗИ
$EV^1_{\text{озпд}}$
М1 - М5, М8, М10

Обработка ПД
$EV_{\text{оопд}}$
М9 (min)

Защита платежных процессов
$EV_{\text{блпп}}$
М1 - М7

Защита информацион. процессов
$EV_{\text{битп}}$
М1 - М6, М8

Защита ПД с учетом СКЗИ
$EV^2_{\text{озпд}}$
М1 - М6, М8

min

Текущий уровень ИБ
EV1

Менеджмент ИБ
EV2

Осознание ИБ
EV3

min

Итоговый уровень соответствия ИБ
R

Подтверждение соответствия Банка Стандарту

ЦБ РФ

ФСТЭК

Роскомнадзор

ФСБ



Система оценки выполнения требований к обеспечению защиты информации по 382-П

**Требования к обеспечению защиты информации
при осуществлении переводов денежных средств, 133 требования в 129 пунктах**

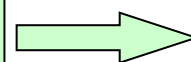
1-я группа требований		2-я группа требований
1 категория проверки Оценка 0, 0.25, 0.5, 0.75 или 1	2 категория проверки Оценка 0 или 1	3 категория проверки Оценка 0, 0.5 или 1

$$EV1_{пс} = \frac{1}{n} \sum_{i=1}^n x_i \times K1$$

$$EV2_{пс} = \frac{1}{n} \sum_{i=1}^n x_i \times K2$$

min

**Итоговый уровень
соответствия $R_{пс}$**



Отчет

утверждается исполнительными
органами управления и хранится в
организации

Значения показателя $R_{пс}$	$R_{пс} < 0,5$	$0,5 \leq R_{пс} < 0,7$	$0,7 \leq R_{пс} < 0,85$	$R_{пс} \geq 0,85$
Значение оценки	«неудовлетво- рительная»	«сомнительная»	«удовлетво- рительная»	«хорошая»
Выполнение установ- ленных требований	Не обеспечивается	Обеспечивается не в полной мере	В целом обеспечивается	Обеспечивается на необходимом уровне



Система оценки выполнения требований к обеспечению защиты информации по 382-П

Требования к обеспечению защиты информации при осуществлении переводов денежных средств, 133 требования в 129 пунктах		
1-я группа требований		2-я группа требований
1 категория проверки Оценка 0, 0.25, 0.5, 0.75 или 1	2 категория проверки Оценка 0 или 1	3 категория проверки Оценка 0, 0.5 или 1



- Методика оценки соответствия требований похожа на методику оценки СТО БР ИББС-1.2-2010, но значительно проще – всего 2 групповых показателя
- Обобщающие показатели $EV1_{пс}$ и $EV2_{пс}$ не обозначают какие-либо направления в ИБ
- Все требования считаются обязательными

Система оценки выполнения требований к обеспечению защиты информации по 382-П

Требования к обеспечению защиты информации при осуществлении переводов денежных средств, 133 требования в 129 пунктах		
1-я группа требований		2-я группа требований
1 категория проверки Оценка 0, 0.25, 0.5, 0.75 или 1	2 категория проверки Оценка 0 или 1	3 категория проверки Оценка 0, 0.5 или 1



- Также введены корректирующие коэффициенты $k1$ и $k2$, понижающие итоговую оценку соответствия в случае полного невыполнения ряда требований
- Требования по документационному обеспечению должны быть выполнены в полном объеме, иначе итоговая оценка будет занижена до 0,85 или 0,7 (**максимум оценка «удовлетворительно»**)



Общие сведения о проведении оценки

Сроки проведения	25 ноября – 23 декабря 2013 г.
Группа оценки	9 человек
Область оценки:	
• платежные системы	4 из 8 (включая ПС Банка России)
• подразделения Центрального аппарата Банка	11
• филиалы	3
• автоматизированные системы	7
Исключено из оценки	14 показателей (оценка – «н/о»)
Представлено свидетельств аудита	457 (политики, руководства, положения, описания тех. процессов, приказы, распоряжения, инструкции, служебные записки и т.д.)
Опрошено сотрудников Банка	54

Отчет по результатам оценки утвержден Правлением Банка 25 декабря 2013 г.

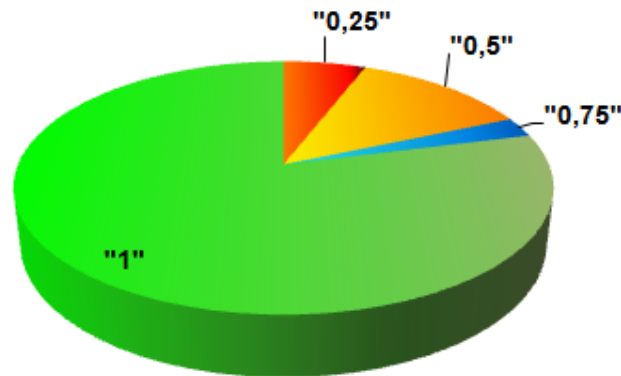
Отчет по форме 0403202 отправлен в Банк России 21 января 2014 г.



Полученные оценки

Оценки	Количество оценок	%%
«0»	0	0
«0,25»	7	6
«0,5»	15	13
«0,75»	3	2
«1»	94	79

Распределение значений оценок выполнения требований



Оценено – 119 показателей.

Исключено из области оценки – 14 показателей (оценка «н/о»).



Сведения о выполнении операторами требований к обеспечению защиты информации при осуществлении переводов денежных средств

Код формы по ОКУД 0403202
На нерегулярной основе

I	Вид деятельности	ОПДС, РЦ
II	Регистрационный номер оператора платежной системы	
III	Предоставление услуг платежной инфраструктуры	0022
IV	Участие в платежных системах	0001, 0004, 0011, 0014, 0018, 0022, 0025

Номер строки	Вид сведений	Содержание
Сведения о выполнении требований к обеспечению защиты информации при осуществлении переводов денежных средств		
1	Показатель EV1 _{пс}	0,87
2	Показатель EV2 _{пс}	0,92
3	Итоговый показатель R _{пс}	0,87
Сведения об оценке выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств		
4	Проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств	Закрытое акционерное общество НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ «ИНФОРМЗАЩИТА», 40308570



Вопросы

1. Трудности при реализации Положения: ревизия объектов информационной инфраструктуры (ОИИ), сложно «уложить» внутренние ОИИ (АС, коммуникации, техпроцессы и т.д.) в конкретную ПС.

Предложения: включить в Положение 382-П (а возможно и в Стандарт ИБ) требования о наличии у участников ПС: Перечня ОИИ (информационных ресурсов), участвующих в переводах денежных средств, Реестра программного обеспечения и т.д.

2. **Получение хотя бы по одному из требований оценки «0»** не позволяет получить общую оценку «хорошая», даже при условии всех остальных оценок «1», так как значение корректирующего коэффициента снижает максимальную оценку до 0,85.

Предложение: При присвоении корректирующему коэффициенту значения «1» допустить наличие оценок «0» по 2-3 требованиям, «привязать» коэффициент к среднему арифметическому оценок всех показателей.



Вопросы

3. Подход к оценке требований категории 1:

- порядок защиты определен в документах, но ничего не делается - оценка «0,25»;
- документ отсутствует, но защита выполнена на отлично - оценка – «0»;
- все требования выполнены на отлично, но меры не документированы – общий вывод аудита «работа по обеспечению ЗИ не обеспечивает выполнение установленных требований»;
- документированные и выполняемые меры не учитывают конкретных угроз и не обеспечивают защиту от них, но оценка должна быть «1».

Предложения:

- выставлять оценку не менее «0,25», если меры не документированы, но обеспечивают необходимый уровень безопасности;
- оценивать обеспечение «необходимого» уровня безопасности (снижение рисков реализации угроз до установленного значения), т.е. проверять адекватность установленных мер защиты существующим угрозам.



Вопросы

4. **Требуется разъяснение**, как проводить самооценку при условии охвата 100% филиалов. Достаточно автономное подразделение должно постоянно совершенствовать защиту. Как выставить в конце отчетного периода (1 раз в 2 года) оценку всему Банку с учетом результатов филиалов, проверявшихся регулярно головным офисом в течение 2-х лет: результаты ведь устаревают.

Предложение: документировать порядок самооценки многофилиальных (многоофисных) участников ПС, или предоставить им право самим устанавливать такой порядок, не противоречащий Положению 382-П.

5. Неоднозначность трактовок формулировок аудиторами и проверяемой организацией.

Предложение : Разработать методические рекомендации по проведению оценки согласно Положению 382-П с однозначными трактовками терминов, понятий и примерами реализации требований. Кто возьмется? ТК122, Партнерства, ABISS?



Вопросы

6. Неоднозначность в оценке требований категории 2
(0 - документ отсутствует, 1 – документ в наличии):

- В требовании № 69 сказано, что операторы «определяют» и «выполняют» порядок применения СКЗИ. А оценивать нужно 0 или 1 по наличию документа. А как же «выполнение»?
- Если документ в наличии, но в нем отсутствуют некоторые позиции? Ставить оценку «0»?

Предложения: 1) Установить критерии оценки «полноты» проверяемых документов. Например, по соответствию установленным угрозам.

Несмотря на имеющиеся вопросы к методике оценки, следует отметить, что расчет стал намного проще и понятней по сравнению с использованной ранее Методикой оценки по СТО БР ИББС



Требования

Оптимизация

Может подумать об
оптимизации?

М

М

нные

Минко

Требования кредитованным УЦ

Проверки аккредитованного УЦ

Аудит PCI DSS

Аудит по PCI DSS



Благодарю за внимание!

ВОПРОСЫ?



Над презентацией работали:

Начальник Службы ИБ Грициенко Андрей Александрович

Заместитель начальника Службы ИБ Широков Александр Григорьевич

Начальник отдела оценки соответствия и аттестации Службы ИБ Кисиленко Геннадий Анатольевич

