SCS SBERBANK CYBER SECURITY

Обеспечение кибербезопасности банка.
Первый опыт оценки соответствия новому национальному стандарту

Мартыненко Кирилл Владимирович
Исполнительный директор – начальник отдела киберкультуры
Департамента безопасности ПАО Сбербанк

Вихорев Сергей Викторович
Заместитель руководителя направления
информационной безопасности НТЦ «Вулкан»

НТЦ ВУЛКАН

Стандарты по кибербезопасности

ISO 27001

PCI Security Standards Council
PARTICIPATING ORGANIZATION™

Банк России

ГОСТ Р 57580.1 ?

Для кого?

Для кредитных, финансовых организаций и субъектов НПС

Когда вступает в силу?

Дата введения – 01.01.2018

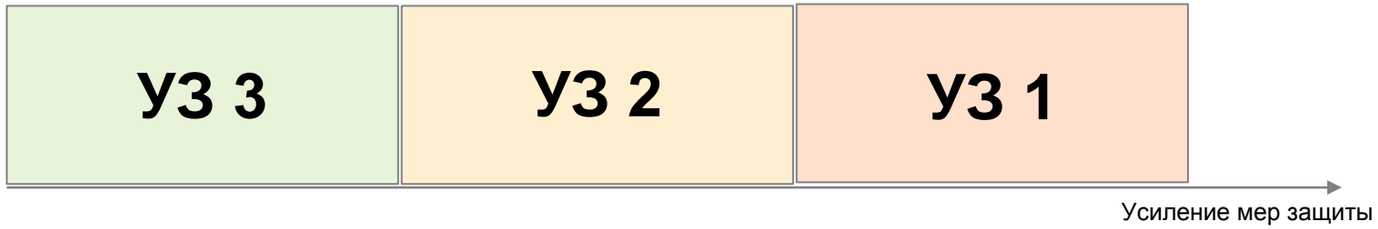
О чем он?

Определяет уровни защиты информации (УЗ) и требования к мерам защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.1	Идентификация и однофакторная аутентификация пользователей	Т	Т	Н

«У человека должен быть здравый смысл. Для всего остального есть ГОСТ»
(М.С. Кейно)

Требования ГОСТ Р 57580.1



Процесс 1 «Обеспечение защиты информации при управлении доступом»

Процесс 2 «Обеспечение защиты вычислительных сетей»

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

Процесс 4 «Защита от вредоносного кода»

Процесс 5 «Предотвращение утечек информации»

Процесс 6 «Управление инцидентами защиты информации»

Процесс 7 «Защита среды виртуализации»

Процесс 8 «Защита информации при осуществлении логического доступа с использованием мобильных (переносных) устройств»

Раздел 7

P D C A

Раздел 8

Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений

Раздел 9

Оценка соответствия ГОСТ Р 57580.1 (1/2)

ГОСТ Р 57580.2 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

Процесс 1	P	D	C	A

Оценка по процессу 1 (разделы 7 и 8)

. . .

Процесс 8	P	D	C	A

Оценка по процессу 8 (разделы 7 и 8)

Оценка по разделу 9

Методика качественной оценки процесса **(1..5)**

$$- 0{,}01Z = R$$

Оценка соответствия ГОСТ Р 57580.1 (2/2)

ГОСТ Р 57580.2 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

0,85 » R » 0,85

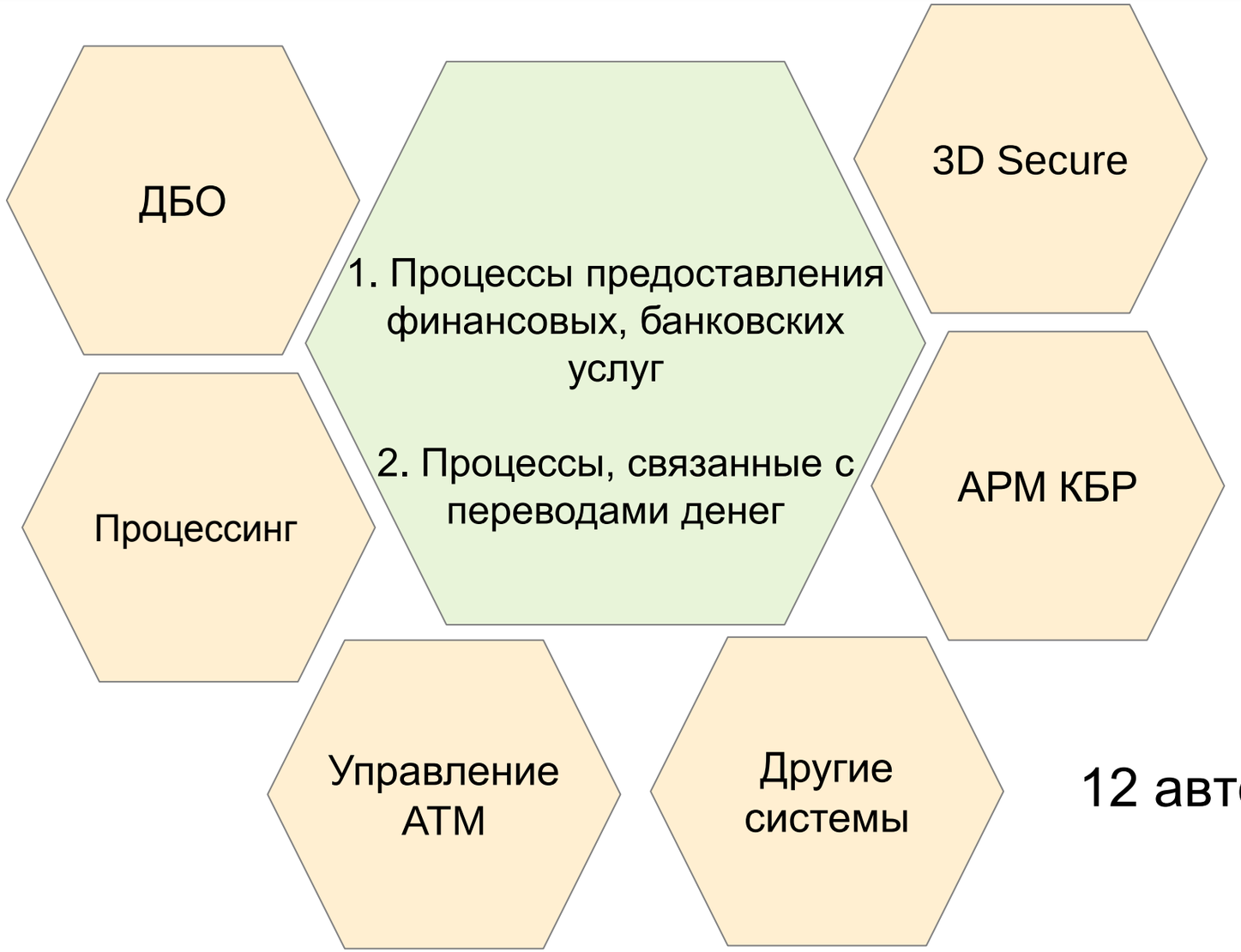
Процесс оценки соответствия ГОСТ Р 57580.1

Определение:
- области оценки
- уровней защиты (УЗ)

Изучение мер защиты информации на выбранной области оценки

Подсчет «математики», сравнение с эталонными 0,85

Шаг 1: Определение области оценки



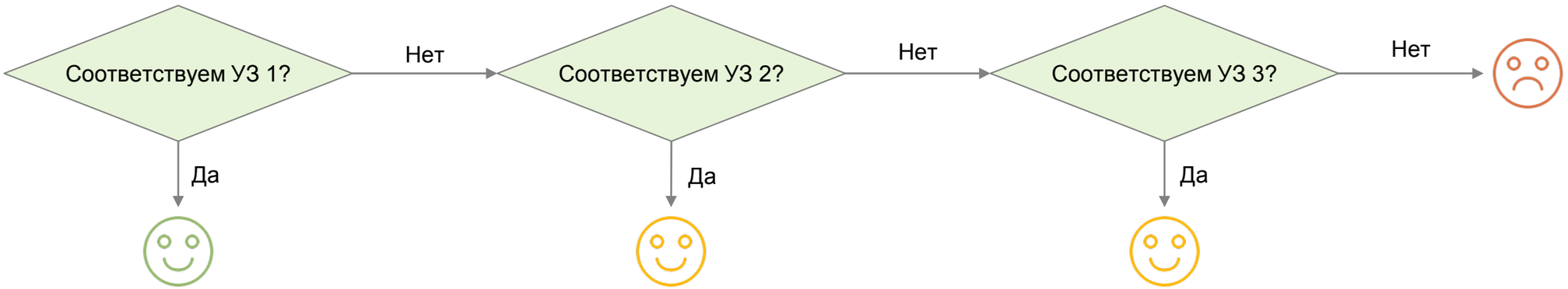
12 автоматизированных систем

«Уровни защиты информации финансовой организации для конкретного контура безопасности устанавливаются нормативными актами Банка России…»

ГОСТ Р 57580.1

Проблема: Нормативных актов Банка России пока нет…

Решение: Определим уровень защиты информации как 1-й, «усиленный»



1 Проведение интервью с сотрудниками Банка

Проблема: Язык ГОСТа. Специалисты не понимают, о чем речь.
Решение: «Перевод» с языка ГОСТа на используемые внутри компании понятия

2 Изучение нормативных документов Банка

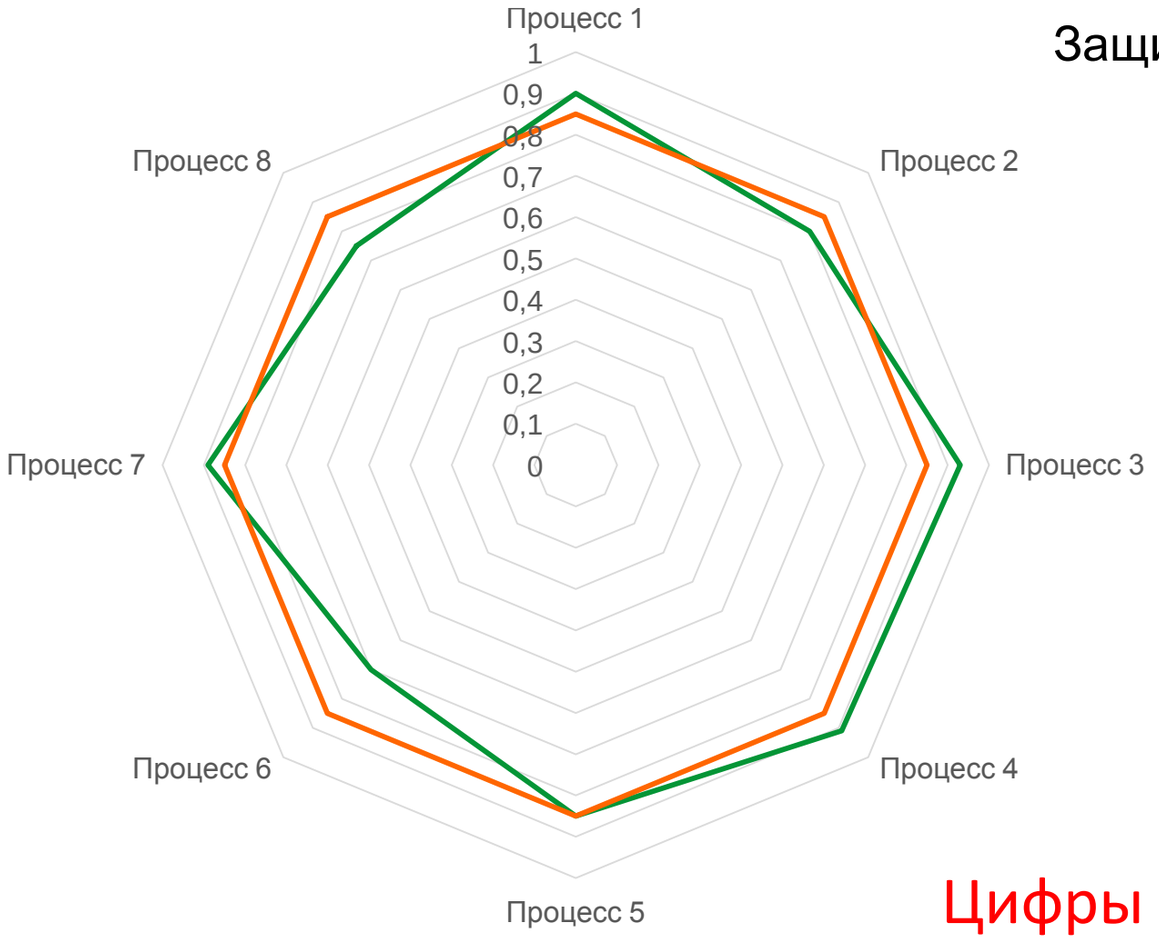
Проблема: ГОСТ новый. Некоторые документы в Банке отсутствуют.
Пример: ПЗИ.2. Документарное определение состава (с указанием соответствия стандарту) и содержания организационных мер защиты
Решение: Быстрая разработка и утверждение этих документов

3 Изучение конфигураций АС и СЗИ

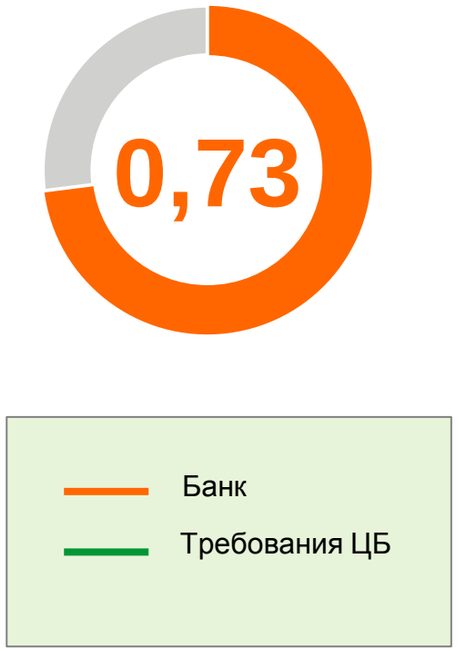
Проблема: требований много, объем работы большой
Решение: больше времени на аудит

ПРИМЕР

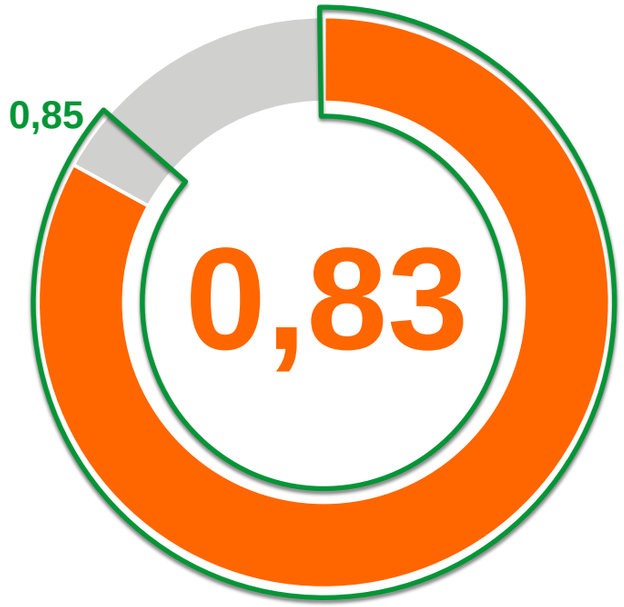
8 процессов защиты информации + PDCA



Защита информации на этапах ЖЦ АС и приложений



Итоговая оценка



Цифры на этом слайде приведены для примера
и не отражают реальной ситуации в ПАО Сбербанк!

Проблемы ГОСТ Р 57580.1 в настоящее время

На ГОСТ нет ссылок в документах ЦБ => «можно пока не выполнять»

Не утверждены «сопутствующие» документы

Оценка требует большого количества внутренних ресурсов

Не формализована требуемая «глубина» оценки:
ГОСТ содержит требования не только к автоматизированным системам, но и к организации в целом

Критерий оценки – качество процесса, а не реализация мер ЗИ

Процесс

- спланирован
- реализован
- проконтролирован
- оценивается
- совершенствуется

Реализация мер

?

Нужна утвержденная методика оценки реализации мер ЗИ

Как подготовиться к аудиту

1. Разработка модели угроз

   без этого выбрать меры весьма проблематично…

2. Работа по выбору мер защиты

   обосновать что мер достаточно, обосновать компенсирующие меры

3. Пред-оценка выбранных мер защиты

   GAP-анализ соответствия выбранного рекомендованному

4. Разработка необходимых ОРД

   стандарт требует документирования многих процессов

5. Техническая оценка настроек СЗИ

   проще заранее иметь протоколы, чем проводить работы в ходе оценки

6. Дополнительные методики

   определение актуальных угроз, оценка выполнения мер

SCS SBERBANK CYBER SECURITY

СПАСИБО ЗА ВНИМАНИЕ!

НТЦ ВУЛКАН

www.ntc-vulkan.ru