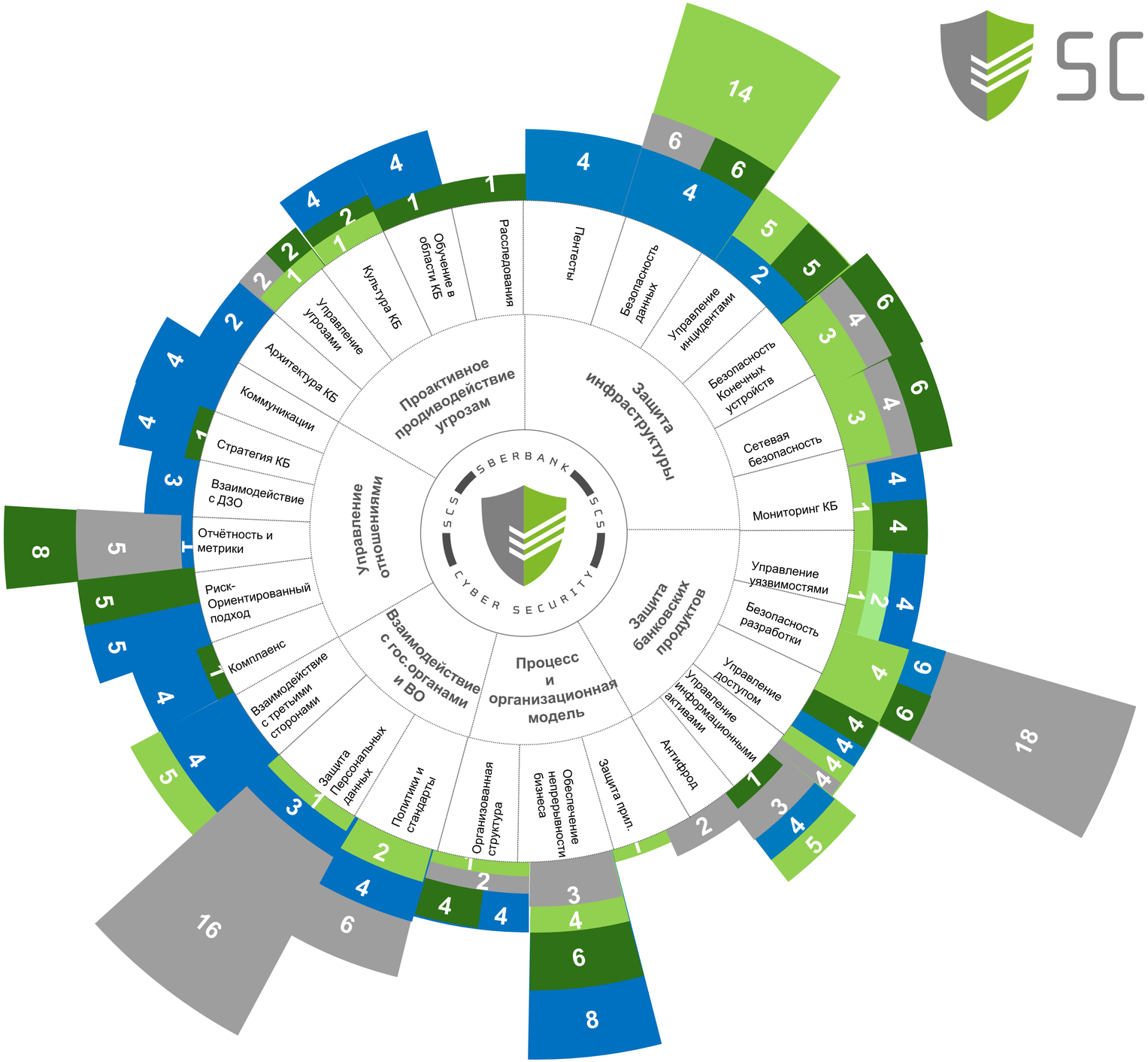
SCS SBERBANK CYBER SECURITY

Стандартизация кибербезопасности

Волков Алексей Николаевич

Управляющий директор -
начальник Управления методологии
кибербезопасности
Департамента безопасности
ПАО Сбербанк

Области регулирования



- Федеральные законы
- Документы ФОИВов
- Государственные стандарты
- Международные стандарты

Полнота регулирования: топ 5 областей

Слабо регулируемые области

- Защита банковских программных приложений в процессе эксплуатации
- Взаимодействие с третьими сторонами
- Обеспечение безопасности инструментов цифровой экономики
- Расследования инцидентов кибербезопасности
- Риски кибербезопасности

Наиболее зарегулированные области

- Безопасность разработки программного обеспечения
- Обеспечение непрерывности бизнеса
- Защита персональных данных
- Управление доступом
- Защита коммерческой тайны

Уровни соответствия

SCS SBERBANK CYBER SECURITY

I **Обязательные**

Федеральные законы

ФСБ

ФСТЭК

БАНК РОССИИ

Минкомсвязи

РОСКОМНАДЗОР

PCI DSS COMPLIANT

II **Добровольные**

ISO

NIST

SANS

Росстандарт

III **Лучшие практики**

Gartner

COBIT 5 AN ISACA® FRAMEWORK

OICU-IOSCO

ITIL®

Формирование периодической отчётности

AS IS Банк на регулярной основе:

- Формирует порядка 400 отчётных материалов по требованиям госорганов и регуляторов (Банк России, ФСБ, МВД, Минкомсвязи, Росатом)
- Принимает до 10 аудитов со стороны регулятора и внешние аудиты на соответствие требованиям международных и отраслевых стандартов,
- том числе PCI DSS, ISO 27001, ISO 20000 и т.д.

TO BE Ужесточение требований по КИИ и фрод-мониторингу (ГосСОПКА) и Банка России (ФинЦЕРТ) - рост проверок и запросов до 50% в горизонте 3 лет (более 20 проверок и 600 запросов)

Среднее время на обработку одного запроса со стороны внешних источников к 2020 возрастёт с 3 до 8 чел/день – рост издержек на сопровождение проверок составит до 20%

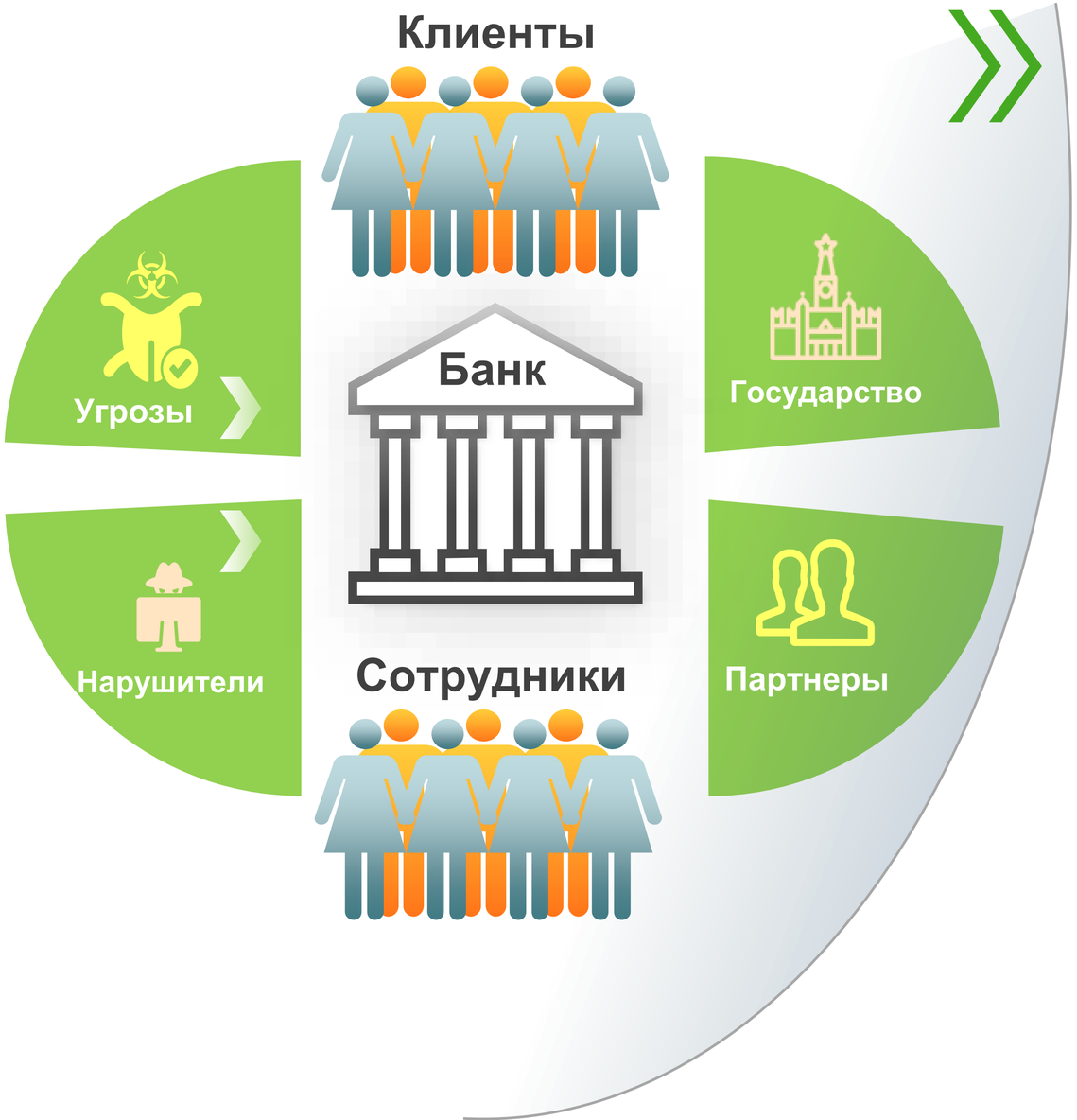
По состоянию на 2018 год ежегодно

10 проверок

400 запросов

250 внутренних отчётов

Управление рисками и управление требованиями



Риск-ориентированный подход

Сильные стороны

- Оперативное реагирование на меняющийся мир, применение необходимых защитных мер там, где это необходимо
- в конкретный момент

Слабые стороны

- Отсутствие объективной оценки используемых защитных мер
- Отсутствие нормативной и законодательной базы принятия решений

Регуляторный подход

Сильные стороны

- Исключает ошибки при принятии решений об использовании защитных мер
- Включает законодательные инструменты и нормативную базу принятия решений

Слабые стороны

- Нормативная база меняется гораздо медленнее и реже, чем ландшафт угроз и методы злоумышленников

- Оптимален сбалансированный подход к управлению рисками кибербезопасности

- Управление киберрисками должно быть интегрировано в общую систему риск-менеджмента компании, руководство должно быть вовлечено в принятие решений

Новые инициативы регуляторов

ФСБ

Порядок информирования ФСБ об инцидентах КИИ
Порядок обмена данными с ГосСОПКОЙ в рамках обеспечения безопасности КИИ
Состав сведений об инцидентах для передачи в ГосСОПКУ в рамках обеспечения безопасности КИИ

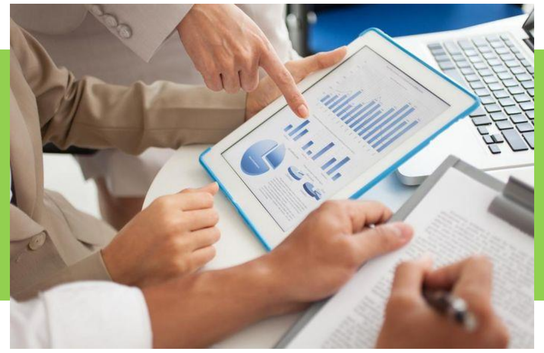
ФСТЭК

Требования к созданию системы безопасности значимых объектов КИИ (общие требования для субъектов КИИ)
Требования по безопасности значимых объектов КИИ (по аналогии с 17-м и 31-м приказами ФСТЭК)

Порядок организации и координации обмена информацией между ФинЦЕРТ, правоохранительными органами и финансовыми организациями
Новые рекомендации ТК 26 для ФО

Качественные требования к ВПОДК в соответствии с Указанием Банка России №3624-У, отраслевыми стандартами ИБ (например, ГОСТР 57580.1-2017) с учётом качественных требований Базеля II к ВПОДК

Выводы



- Необходимо использовать сбалансированный подход к управлению рисками кибербезопасности

- Необходима унификация и гармонизация требований регуляторов
  - ✓ сокращение объёма запрашиваемой информации
  - ✓ сокращение количества проверок
  - ✓ автоматизация отчётности

- Требуется внимание областям стандартизации, призванных совершенствовать механизмы получения добавленной стоимости Банку
  - ✓ управление киберрисками,
  - ✓ расследование компьютерных преступлений
  - ✓ защита банковских приложений
  - ✓ безопасность цифровых технологий, облачных вычислений и обработки больших массивов данных

- Необходим практический опыт обеспечения безопасности новейших технологий

SCS SBERBANK CYBER SECURITY

Спасибо за внимание!