Построение системы управления рисками ИБ в рамках корпоративного риск-менеджмента

Юрий Шелихов
Отдел безопасности банковских систем

Информзащита
Системный интегратор

Типовое положение дел

Причины:

- СУОР рассматривает риски ИБ поверхностно
- Риски ИБ логически не связаны с ОР
- Разные методики
- Разные и не интегрированные инструменты
- Отсутствие планов коммуникации между СУОР и СУРИБ
- Разная система отчетности

Следствия:

- Низкая эффективность (ресурсы)
- Конфликты интересов

Информзащита
Системный интегратор

Курьезные ответы респондентов

«Каким образом Вы управляете рисками ИБ?»

- «Не смешите меня…»
- «Мы не занимаемся этой ***профанацией***»
- «Если риски нельзя посчитать ***количественно***, то зачем из считать?»
- «У нас этим заведует ***управление операционными рисками***»
- «У нас разработаны ***модели угроз*** *ИБ*, этого достаточно»
- «***Процесс*** управления рисками у нас есть, мы его ***запускаем*** раз в 2 -3 года»

Информзащита
Системный интегратор

Задачи и инструменты СУОР и СУРИБ

	СУОР	СУРИБ
Идентификация и оценка рисков	+	+
Сценарный анализ рисков	+	+
Ведение реестра рисков	+	+
Учет рисковых событий (инцидентов) в БД	+	+
Отчетность	+	+
Сбор данных о потерях	+	-
Определение критичности процессов	+	+/-
Контроль полноты БД со стороны СВК	+/-	-
Мониторинг КИР (раннее предупреждение о риске)	+	-
Автоматизированный мониторинг инцидентов	-	+
Автоматизированный мониторинг уязвимостей	-	+
Автоматизированный контроль настроек (требований)	-	+

Какая польза СИБ от СОР?

Знания

- О риск-аппетите
- Критичность бизнес-процессов
- Стоимость инцидентов ($ потерь)

Владение

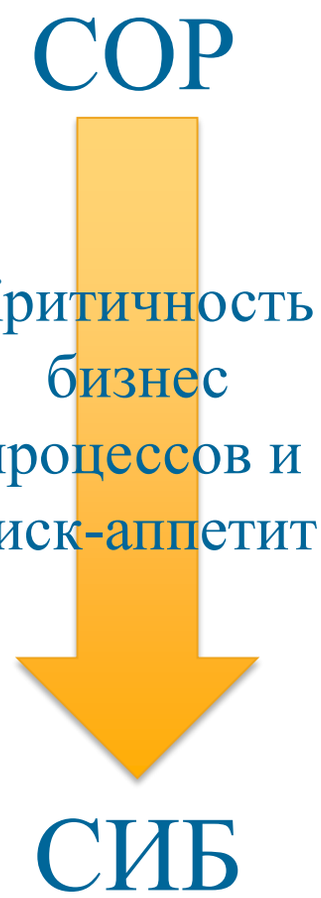
- Методологией
- Базой данных инцидентов
- Весомая позиция для руководства

Возможность

- Активного вовлечения бизнес-подразделений

Автоматизация

- БД регистрации и учета инцидентов
- GRC (у некоторых)



Информзащита
Системный интегратор

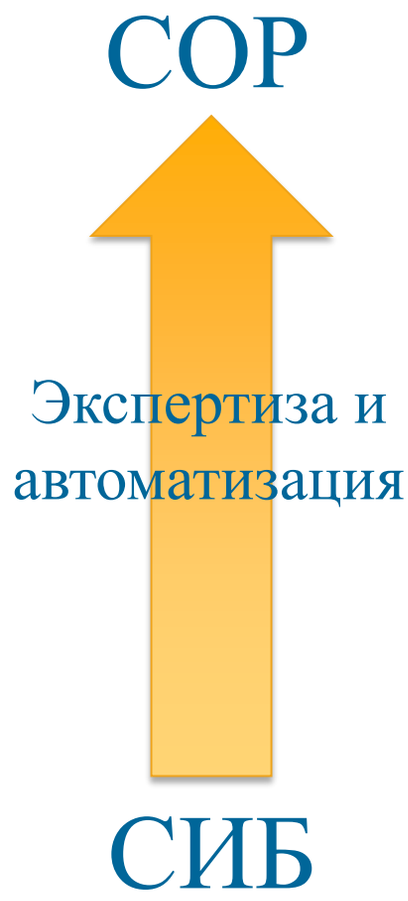
Какая польза СОР от СИБ?

Экспертиза о

- ИТ инфраструктуре
- Технологиях и тенденциях
- Актуальных угрозах
- Защитных мерах
- Требованиях регуляторов
- Уязвимостях

Автоматизация

- Выявления инцидентов
- Идентификации уязвимостей
- Контроля настроек (выполнения требований)
- Выявления рисков



Информзащита
Системный интегратор

Инструменты СИБ

Организационные

- Аудиты и самооценки (ежегодно)
- Тесты на проникновение (пентесты)
- Проведение оценок рисков
- Разработка моделей угроз и нарушителей
- Мониторинг СИБ (выявление нарушений и уязвимостей)
- Мониторинг новых рисков (форумы, конференции, комитеты, отчеты)

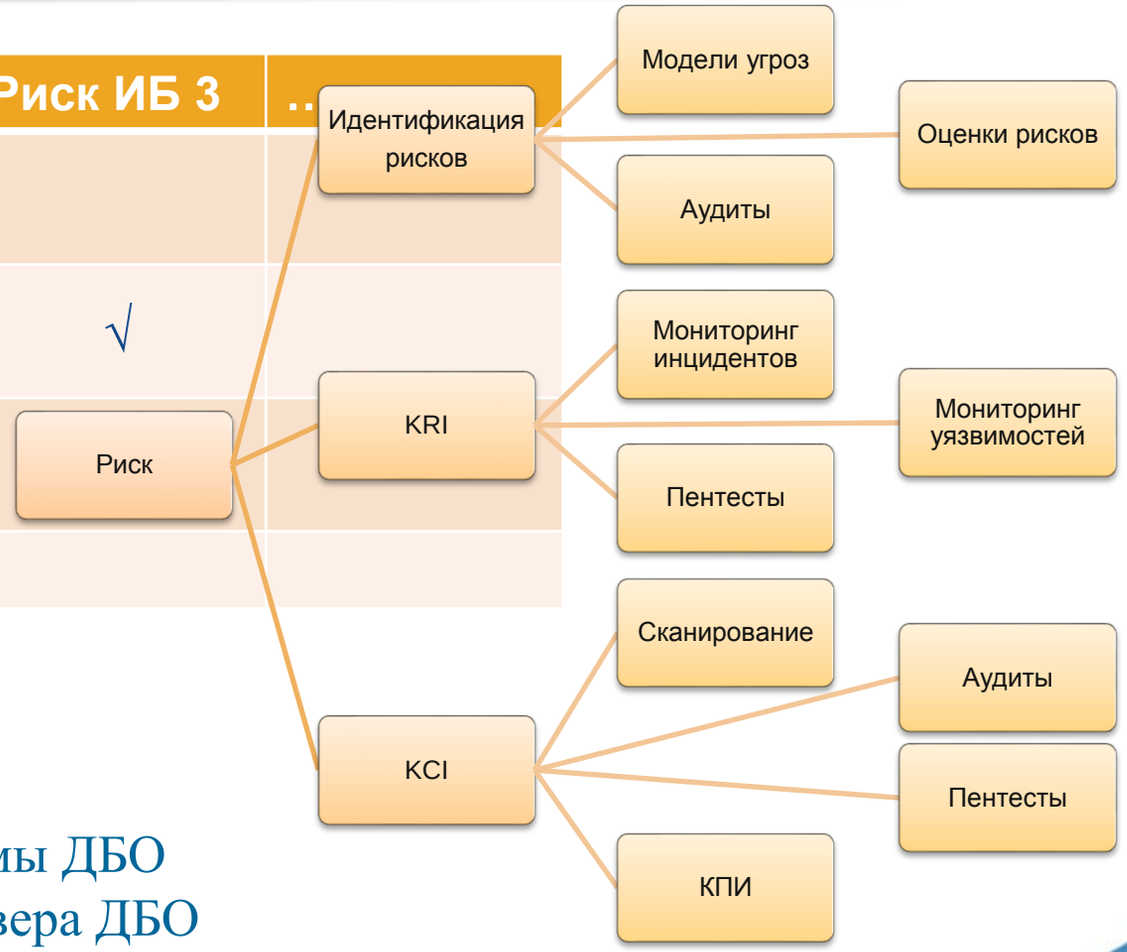
Технические

- Средства регистрации и контроля доступа
- Средства антивирусной защиты
- Сканеры уязвимостей, безопасности
- Средства предотвращения утечек информации
- Средства выявления сетевых вторжений
- Средства мониторинга и корреляции событий безопасности

Информзащита
Системный интегратор

Интеграция рисков

	Риск ИБ 1	Риск ИБ 2	Риск ИБ 3	..
Операционный риск 1	√			
Операционный риск 2		√	√	
Операционный риск 3	√			
…				



Пример:

Оперриск 2: Сбой в системе ДБО

Риск ИБ 2: Остановка работы БД системы ДБО

Риск ИБ 3: Остановка работы WEB сервера ДБО

KRI 1: Количество критических уязвимостей

KRI 2: % соответствия требованиям ИБ

KRI 3: % от максимальной загрузки сервера

KRI 4: количество инцидентов ИБ

Информзащита
Системный интегратор

ПРОЦЕССЫ GRC

	G	R	C
Решение	• Постановка задач • Назначение ответственных • Выделение ресурсов	План обработки рисков	План устранения несоответствий
Оценка	Достижения целей	Уровня рисков	Уровня соответствия
Мониторинг	• Целей бизнеса, ИТ • Исполнения задач	• Новых рисков • Индикаторов риска	• Новых требований • Выполнения политик

Автоматизированная система GRC

Управление активами | Управление угрозами | Управление контролями | Управление уязвимостями | Отчеты и инфопанели | Управление задачами

Ключевые индикаторы риска

INFOWATCH, CISCO, ArcSight, symantec., Код Безопасности, McAfee, MAXPATROL, CMDB, Check Point, Dr.WEB, AUDIT, QUALYS, Информзащита

Выводы

- Разработка СУРИБ
- Интеграция СУРИБ в СУОР (матрицы рисков, факторов рисков, КИР, отчетность)
- Активно используем средства защиты для мониторинга КИР
- Организуем каналы обмена информацией (статистика, новые угрозы, уязвимости, критичность активов,...)
- Выполняем сценарный анализ (моделирование угроз ИБ) по наиболее критичным операционным рискам
- Автоматизируем (GRC)

Информзащита
Системный интегратор

Спасибо за внимание.

Юрий Шелихов

☎ +7(495) 980-2345

y.shelikhov@infosec.ru

Информзащита
Системный интегратор