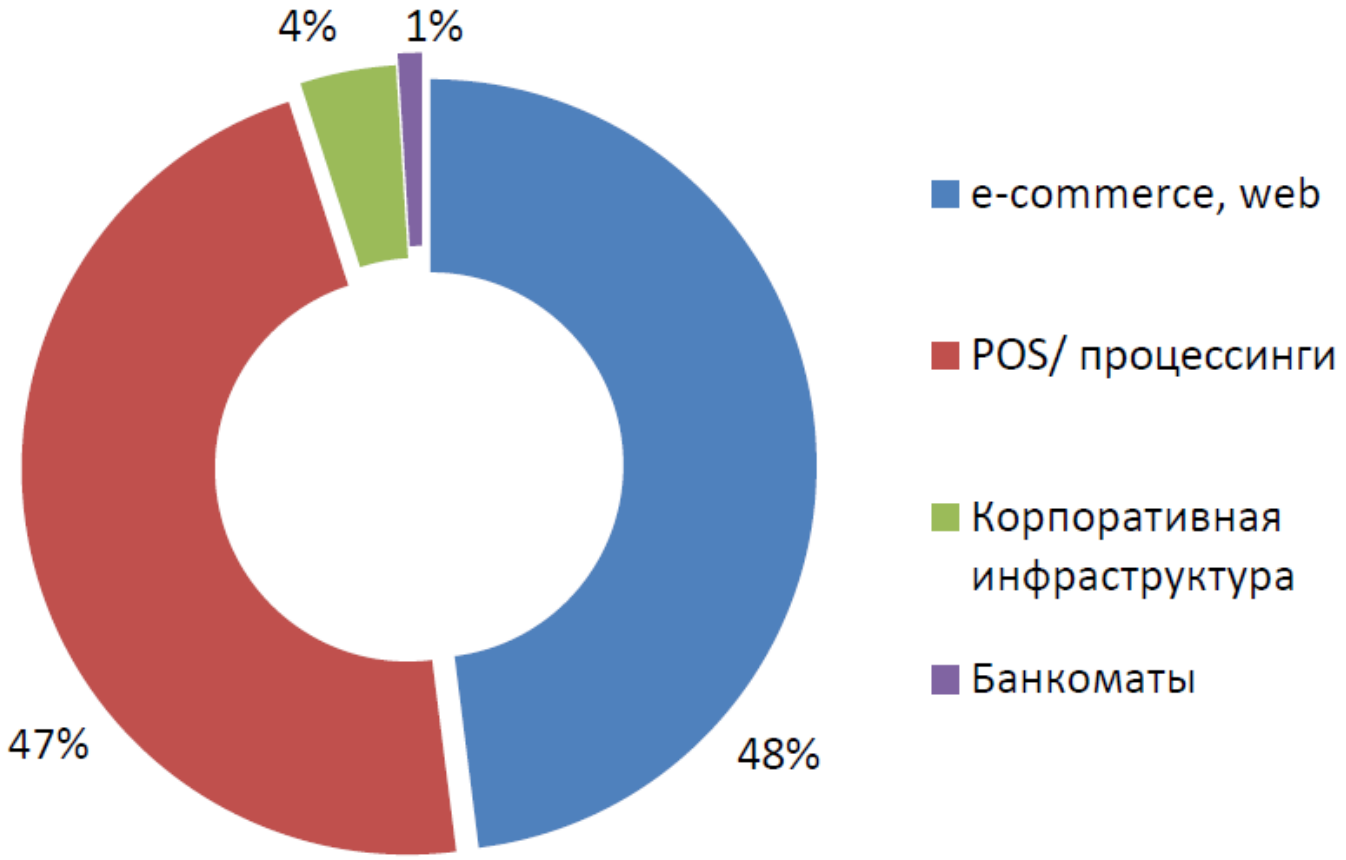
Конференция «E-payments Russia 2013»
Вопросы безопасности электронных платежей
Отель «Ренессанс Москва Олимпик», 3 сентября

Факторы повышения эффективности инвестиций в информационную безопасность электронных платежей (ИБ ЭП): (1)стоимостная оценка рисков, (2)ИБ в формате сервисной модели

Афонин Евгений
Департамент консалтинга и аудита
начальник отдела

Информзащита
Системный интегратор

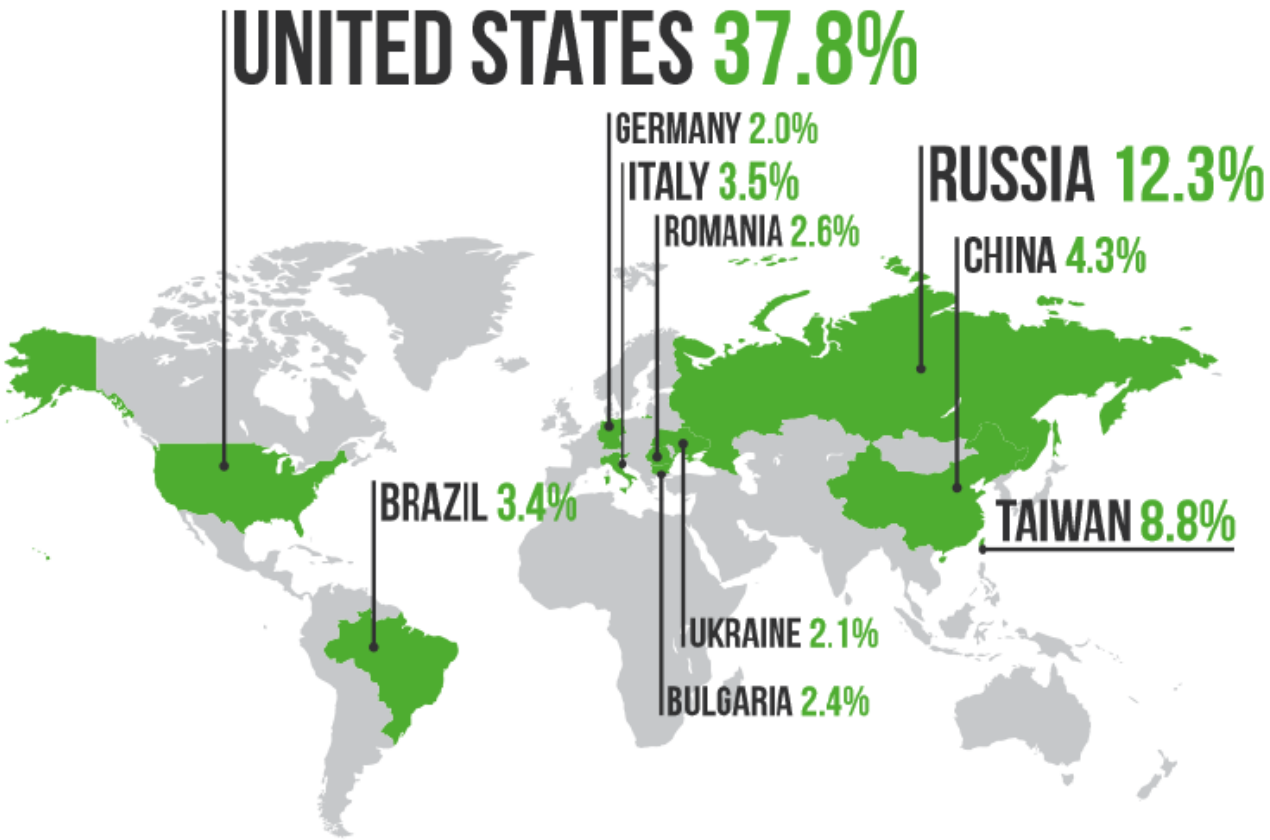
Системы электронных платежей одна из основных целей атак злоумышленников



Источник: Global Security Report 2013, Trustwave

Информзащита
Системный интегратор

Россия на втором месте в мире по источникам атак



Источник: Global Security Report 2013, Trustwave

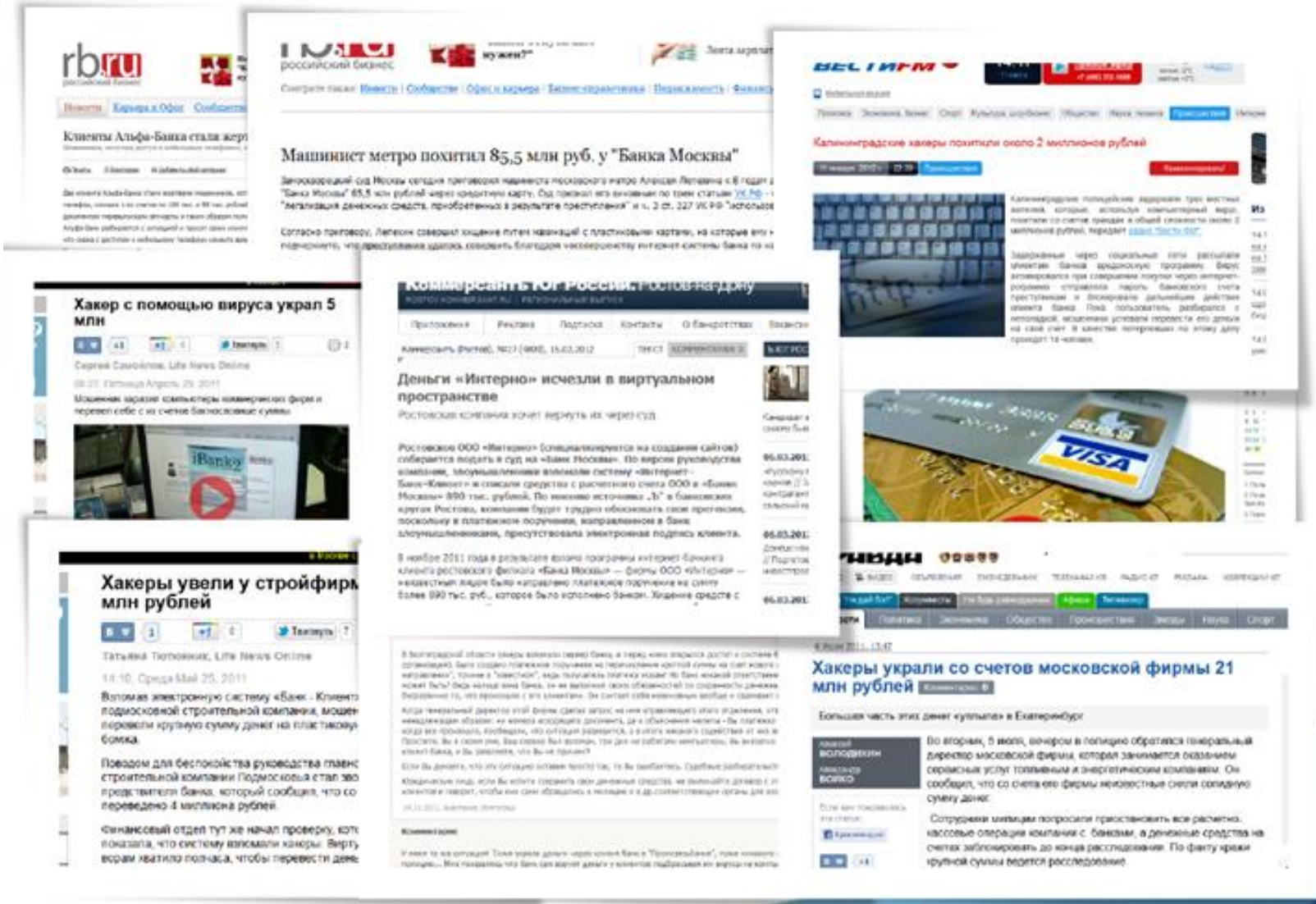
Информзащита
Системный интегратор

Наибольшее количество инцидентов в НПС - попытки несанкционированного перевода денежных средств

Источник: Аналитический обзор инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств (второе полугодие 2012), Банк России

Информзащита
Системный интегратор

Это касается не нас, с ИБ у нас все «Ок»



96% компаний в своих системах имели различного рода уязвимости

Источник: внутренняя статистика компании Информзащита по проведенным тестам на проникновение за 2012 год

Информзащита
Системный интегратор

Требования к кредитным организациям Южной Кореи

- Число ИТ-специалистов должно составлять не менее 5% от числа штатных сотрудников
- Число сотрудников, обеспечивающих ИБ должно быть не менее 5% от числа ИТ-специалистов
- На обеспечение информационной безопасности должно выделятся не менее 7% бюджета организации

- Все финучреждения Сингапура обязаны сообщать контролирующим органам о киберинциндентах и сбоях в работе собственных информационных систем в течение часа, после обнаружения киберугроз и/или неисправностей.
- Подав первичный отчет об инциденте, организация должна подготовить второй отчет, содержащий развернутый анализ инцидента и детальное объяснение вызвавших его причин. Отчет должен подаваться в Денежно-кредитное управление Сингапура (MAS) в течение 14 дней

Источник: информационное агентство Yonhap, http://www.fsc.go.kr, http://www.mas.gov.sg/
http://www.anti-malware.ru/news/2013-04-30/11696
http://www.anti-malware.ru/news/2013-07-12/12235

Информзащита
Системный интегратор

Выводы:

- Обеспечение ИБ электронных платежей (ИБ ЭП) является актуальной задачей
- В условиях ресурсных ограничений для успешного решения задачи ИБ ЭП инвестиции должны быть эффективны
- Существуют целевые ориентиры ресурсного обеспечения ИБ в стоимостном выражении, для некоторых стран они установлены регулятором
- Эффективность инвестиций (затрат) в ИБ = измеренный результат, сопоставление с объемом вложений, сравнение альтернатив, приоритет вложений

Эффективность ИБ на языке бизнеса

- Бизнес говорит на языке денег
- Стандартные показатели эффективности инвестиций, например ROI - не всегда возможно
- Комплаенс, Риски,
- Важны: выстроенная, одобренная руководством процедура, одинаковое понимание, использование стоимостных показателей
- Заинтересованные стороны: ИБ, «Риски», «Финансы», Бизнес

Стоимостная оценка рисков ИБ

- Наиболее убедительный для бизнеса способ измерения результата вложения средств в ИБ
- Электронные платежи – все транзакции имеют стоимостное выражение, как правило уже используются бизнес-показатели, характеризующие риски ИБ (например, недополученная прибыль из-за простоя ДБО)
- Сложности – отсутствие исходных данных, согласованной методики, процедур, …

Информзащита
Системный интегратор

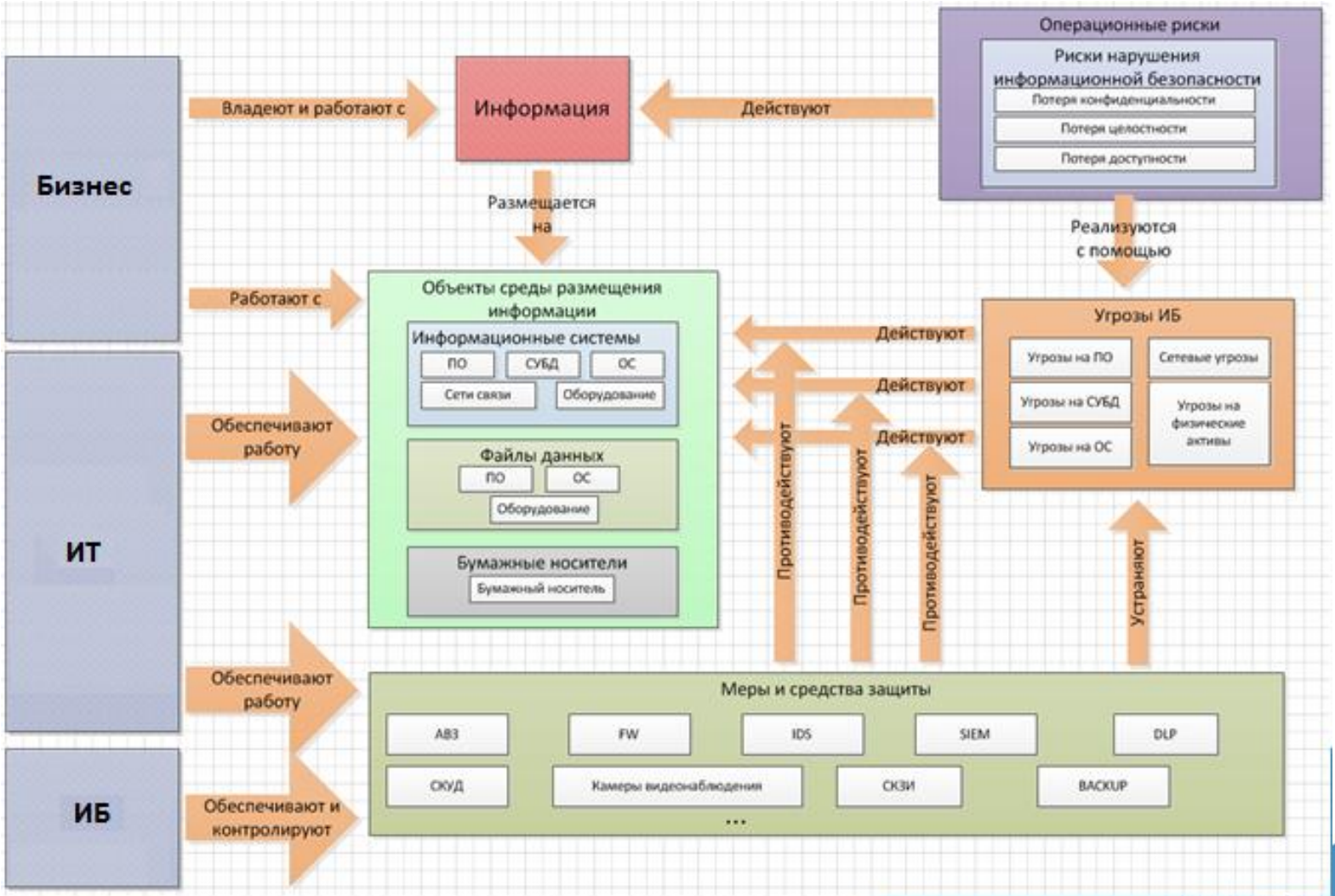
Решение – внедрить Систему Управления Рисков Информационной Безопасности (СУРИБ)

СУРИБ позволяет:

- Идентифицировать, оценить в т.ч. в стоимостном выражении, приоритезировать риски ИБ
- Планировать способы обработки рисков
- Обосновать ИБ\ИТ-бюджеты
- Обеспечить соответствие НПС(382-П), СТО БР ИББС, PCI DSS, ISO 27001

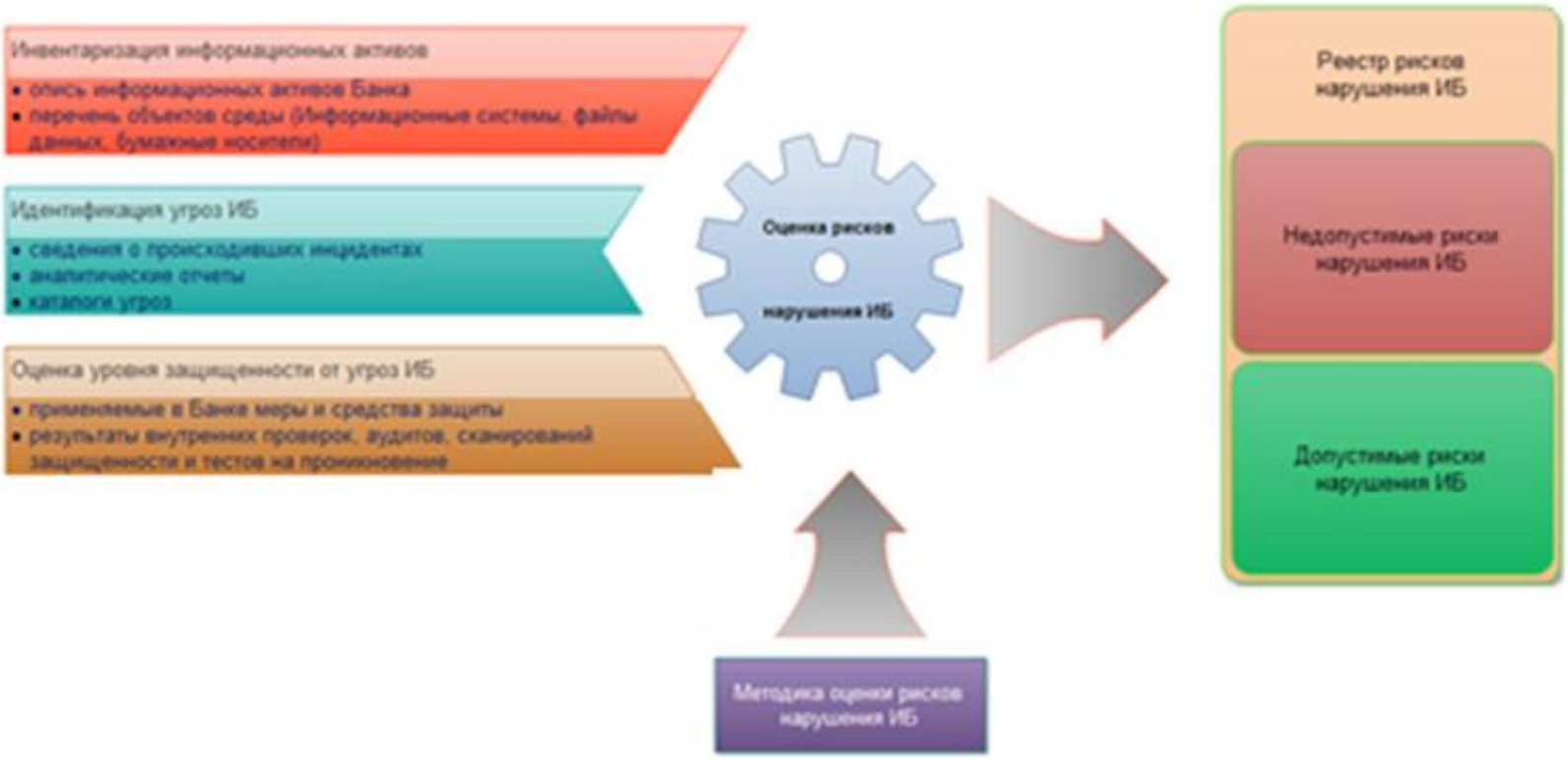
Информзащита
Системный интегратор

СУРИБ: Схема отношений при оценке рисков



Информзащита
Системный интегратор

СУРИБ: Схема управления рисками



Информзащита
Системный интегратор

СУРИБ: элементы

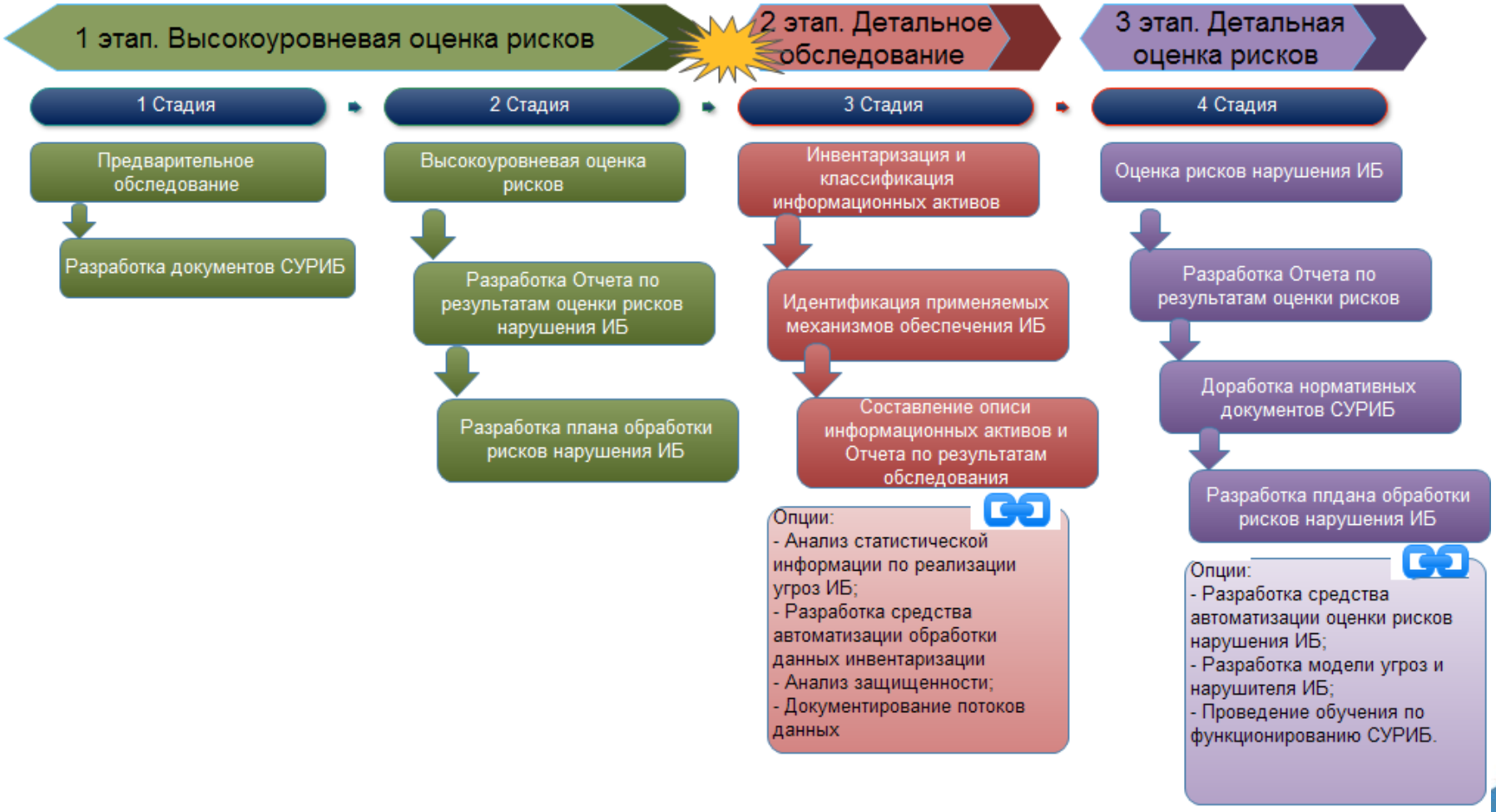
СУРИБ – *совокупность взаимосвязанных процедур, обеспечивающих управление рисками нарушения ИБ*

Элементы СУРИБ:

- ***Документы**, регламентирующие процедуры*
- ***Работники**, выполняющие процедуры*
- ***Средства автоматизации** оценки рисков*
- *Документированные **результаты** выполнения процедур*
- ***Решения руководства***

Информзащита
Системный интегратор

СУРИБ: Roadmap создания



Информзащита
Системный интегратор

СУРИБ: Результаты

- Внедрены и документированы процедуры управления рисками
- Выполнена первичная оценка рисков: составлен реестр информационных активов, автоматизированных систем, объектов среды, определены стоимостные показатели рисков ИБ
- Документирована декларация применимости механизмов контроля
- Подготовлены проекты планов обработки недопустимых рисков
- Разработан прототип средств автоматизации

Информзащита
Системный интегратор

СУРИБ: Результаты

Создана основа для использования в практике стоимостных характеристик рисков ИБ, таких как:

- Потери компании в день\месяц\год от … (простоя ДБО, фрода, вирусных заражений, спама, утечек, несоответствия требованиям регуляторов, инцидентов ИБ…)
- Затраты [разовые\ежедневные\ежегодные] на … (обеспечение доступности ДБО, антифрод, антивирус, антиспам, выполнение требований регуляторов, обработку инцидента ИБ, …)
- Стоимость системы защиты в расчете на одно рабочее место\на одного сотрудника\клиента\на одну транзакцию

ИБ в формате сервисной модели

Зачем сервисная модель?

- Знаем потребителей
- Договариваемся с потребителями о приемлемом уровне услуг
- Четкая процедура предоставления услуг
- Знание себестоимости (затраты своих ресурсов) позволяет оценить эффективность (сравнение с собой вчера, с рынком), обеспечить требуемой количество и доступность

ИБ в формате сервисной модели

- Сервисная модель для службы ИБ на основе ITSM\ITIL или COBIT
- ВАЖНО: Внутренние и внешние потребители, SLA понятные и принятые потребителями
- Структура деятельности = сервисы-услуги
- Формализация процедур
- Для каждой операции метрики себестоимости

ИБ в формате сервисной модели

Принципы

- Заинтересованные стороны (потребители услуг ИБ)
- SLA в терминах и значениях, ориентированных на потребителя
- Регламентация процедур с метриками затрат ресурсов, например трудозатраты в чел.\час.

Результаты

- Известны потребители и уровень их удовлетворенности результатами
- Рассчитывается внутренняя стоимость услуг ИБ
- Возможно планирование ресурсов под потребности бизнеса
- Гармонизация отношений служб ИБ и ИТ

Влияние на эффективность инвестиций в ИБ ЭП

(1)стоимостная оценка рисков (СУРИБ)

- измерения результата вложения средств в ИБ
- сравнение альтернативных вариантов, выбор лучшего
- результат выражен в стоимостных показателях, понятных бизнесу

(2)Обеспечение ИБ в формате сервисной модели

- Известны потребители и уровень удовлетворенности результатами
- Рассчитывается внутренняя стоимость услуг ИБ
- Возможно планирование ресурсов под потребности бизнеса

Спасибо за внимание

Вопросы?

Афонин Евгений
Департамент консалтинга и аудита
начальник отдела

e.afonin@infosec.ru

Информзащита
Системный интегратор