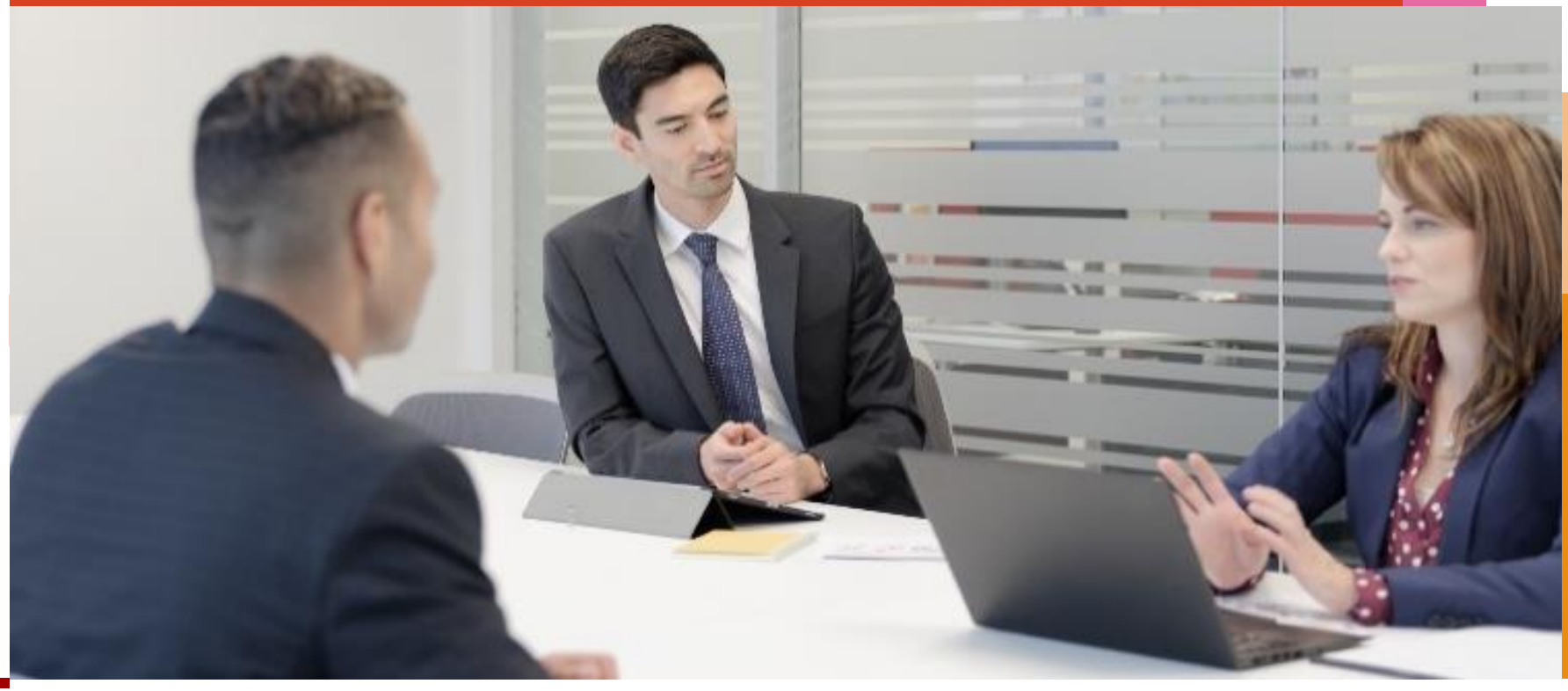
www.pwc.ru/cybersecurity

Показатели эффективности ИБ понятные бизнесу

22 марта 2018



pwc

BIS Summit St. Petersburg 2018

Содержание

1. В чем трудности внедрения KPI по ИБ?

2. Подход к формированию KPI по ИБ

3. Пример формирования KPI

В чем проблемы с внедрением KPI по ИБ?

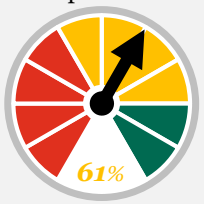
Основные проблемы KPI по ИБ

Готовы ли Вы ответить на эти вопросы бизнеса?

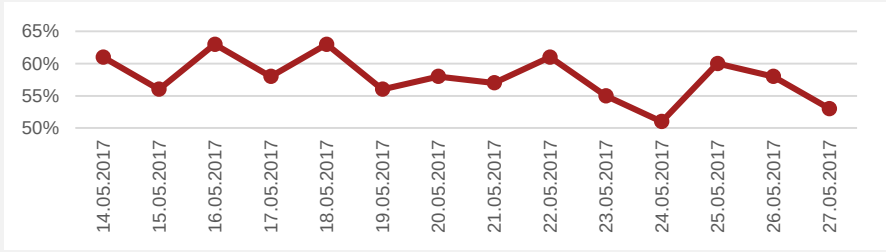
- Достаточно ли защищены наши основные продукты и сервисы?
- Что делает служба ИБ, чтобы поддержать новые бизнес-проекты?
- К каким финансовым последствиям может привести инцидент ИБ?
- Можем ли мы снизить затраты на ИБ не подвергая бизнес значительным рискам?
- Насколько сейчас защищены наши информационные активы? Насколько они должны быть защищены?

Пример отчетности по ИБ

Эффективность контролей ИБ

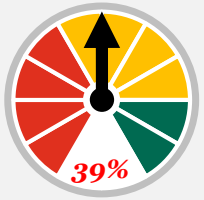


Динамика изменения интегрального уровня контролей ИБ

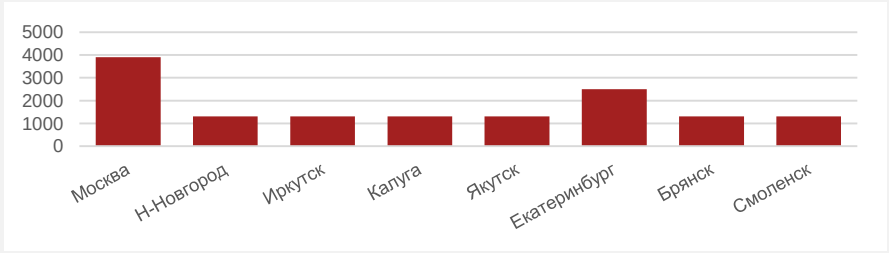


Защищенность сети

Кол-во инцидентов решенных в SLA

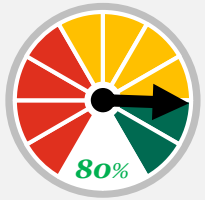


Количество инцидентов SOC

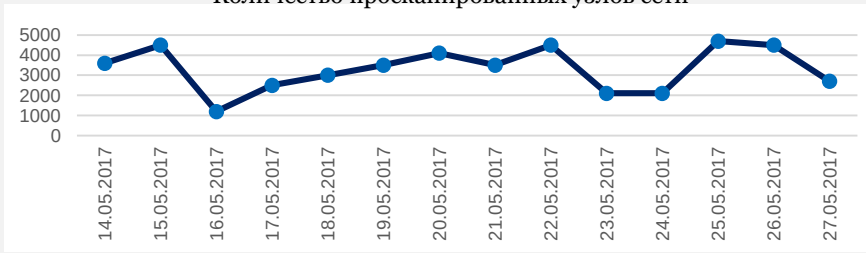


Эффективность операторов SOC

% просканированных узлов сети



Количество просканированных узлов сети



Охват информационных активов

Основные проблемы KPI по ИБ

- Отсутствие связи KPI по ИБ с бизнес инициативами и проектами
- Сложность выбора правильных KPI по ИБ
- Недостаточная автоматизация процесса
- Сложность выбора правильной аудитории и подходящего им формата презентации
- Переизбыток технической информации

Подход к формированию KPI по ИБ

Основные цели отчетности по ИБ

ISF research © 2015

Две основные цели отчетности ИБ:

1. **мониторинг деятельности** Службы ИБ относительно выполнения стратегических задач и рабочих процессов

2. **управление рисками ИБ**, способными помешать достижению стратегических задачи и бизнес-целей компании

Текущий подход связывает **мониторинг деятельности** Службы ИБ и **управление рисками ИБ** через составление комбинаций KPI/KRI.

Связь целей отчетности с KPI/KRI

KPI

Отражает прогресс относительно стратегических задач и целей

Преимущественно оценивает **прошлое**

Отражает:

Фактический результат работы Службы ИБ относительно планов и намеченных целей

Также предоставляет основу для:

выявления трендов при планировании ресурсов (персонал, оборудование и т.д.) и их загрузки

KRI

Риск, который может повлиять на выполнение стратегических задач и достижение целей бизнеса

Преимущественно оценивает **будущее**

Отражает:

Новые и ранее идентифицированные риски, выраженные в виде вероятности их наступления и потенциального негативного воздействия

Также предоставляет основу для:

оценки ранее сделанных прогнозов по рискам ИБ и трендов развития бизнеса

Подход к отчетности по ИБ

Этап 1. Определение целей бизнеса и ключевых участников посредством изучения стратегий, отчетов и бизнес-процессов других подразделений с целью выявления общих интересов и создания комбинаций KPI/KRI.

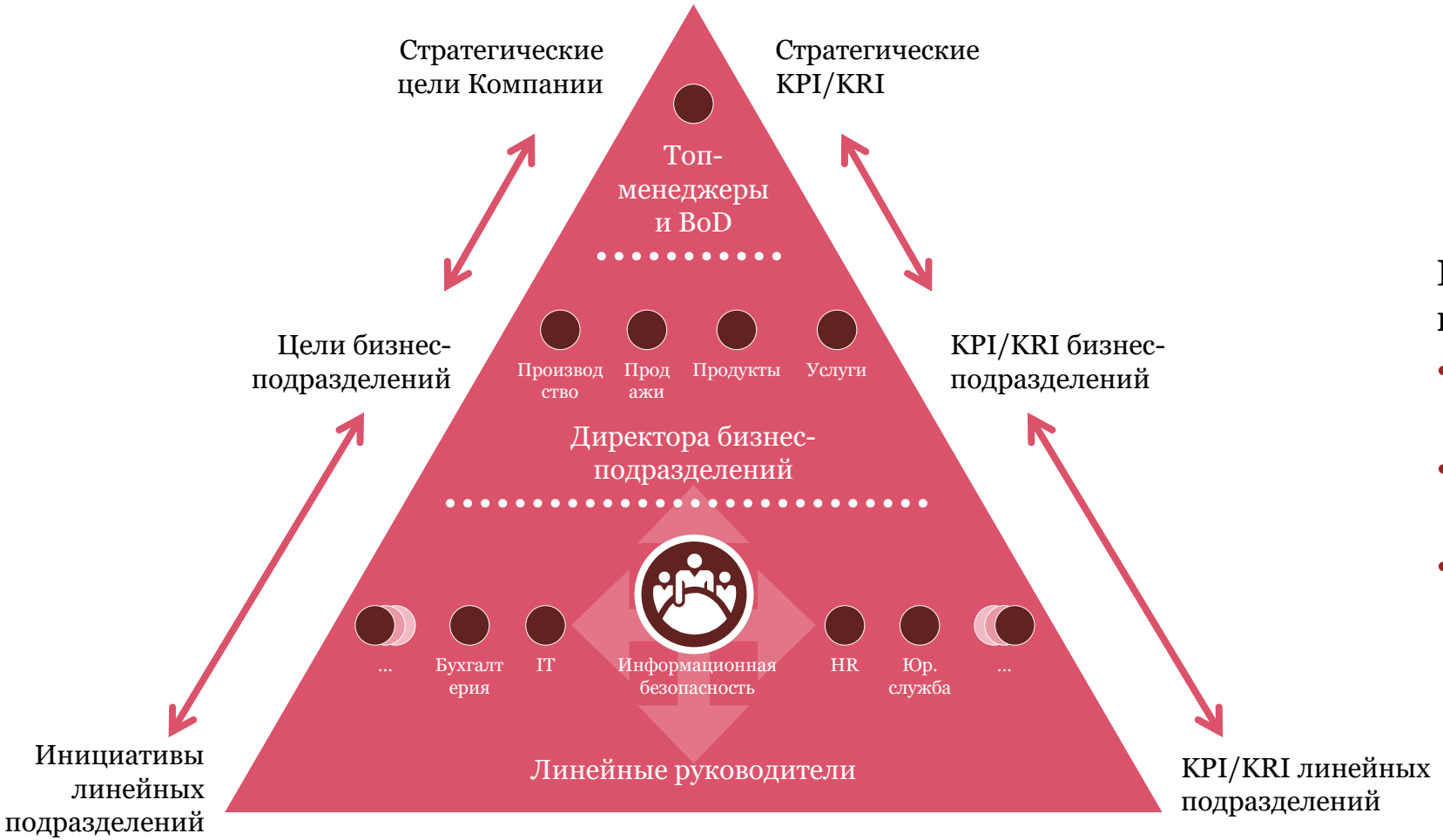
Этап 2. Подготовка и тестирование KPI/KRI вместе с лидерами бизнес-подразделений. Совместная интерпретация полученных результатов.

Этап 3. Презентация результатов отчетности и утверждение совместных инициатив.

Этап 4. Сбор обратной связи и подготовка плана по улучшению отчетности.

Вовлечение бизнес подразделений

Вовлечение бизнес-подразделений



Вовлечение

Вовлечение бизнес-подразделений в создание KPI/KRI ИБ позволяет:

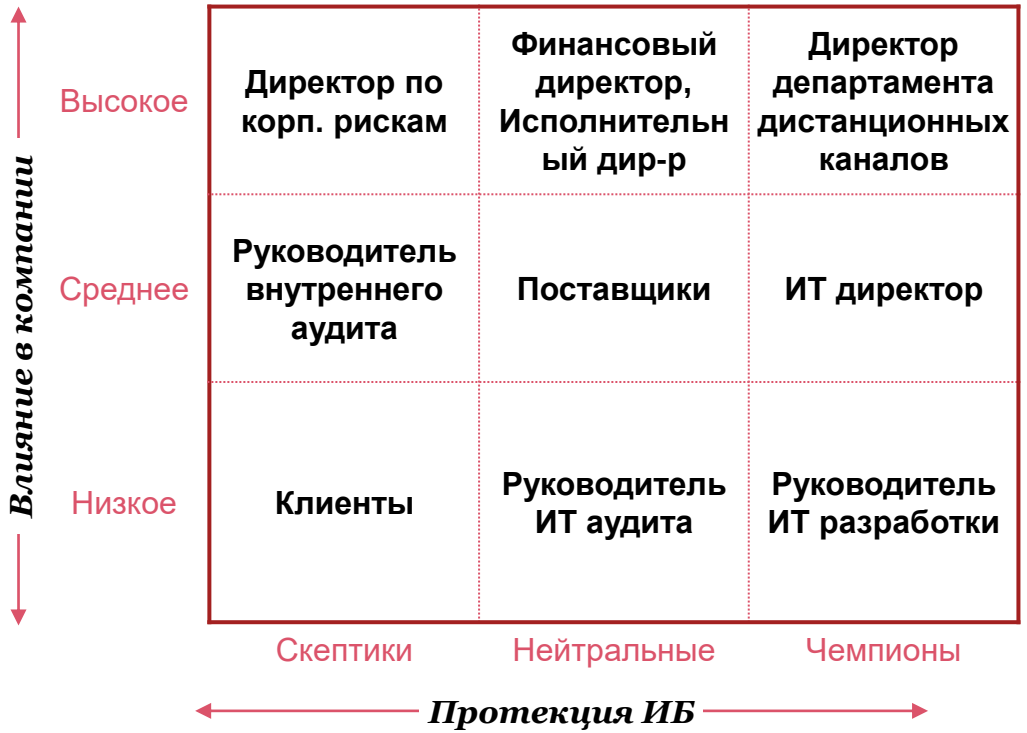
- информировать их о современных угрозах и рисках ИБ
- идентифицировать возможности для взаимовыгодного сотрудничества
- доносить важность функции ИБ до каждого подразделения

Этап 1. Определение целей бизнеса и ключевых участников

Определение целей бизнеса

Определение текущих целей бизнес-подразделений позволяет согласовать ключевые показатели эффективности ИБ с потребностями и задачами бизнеса.

Шаг 1	Понимание контекста, в котором работает бизнес (стратегии, планы, процессы и др.)
Шаг 2	Определение ключевых заинтересованных сторон
Шаг 3	Составление списка интересов бизнес-подразделений
Шаг 4	Подготовка предложений по совместным инициативам с бизнес-подразделением



Этап 2. Подготовка KPI/KRI с бизнес-подразделениями

Подготовка KPI/KRI

На данном этапе бизнес-подразделения вовлекаются для подготовки KPI/KRI и определения пороговых значений KPI. Проводится интерпретация и анализ полученных результатов.

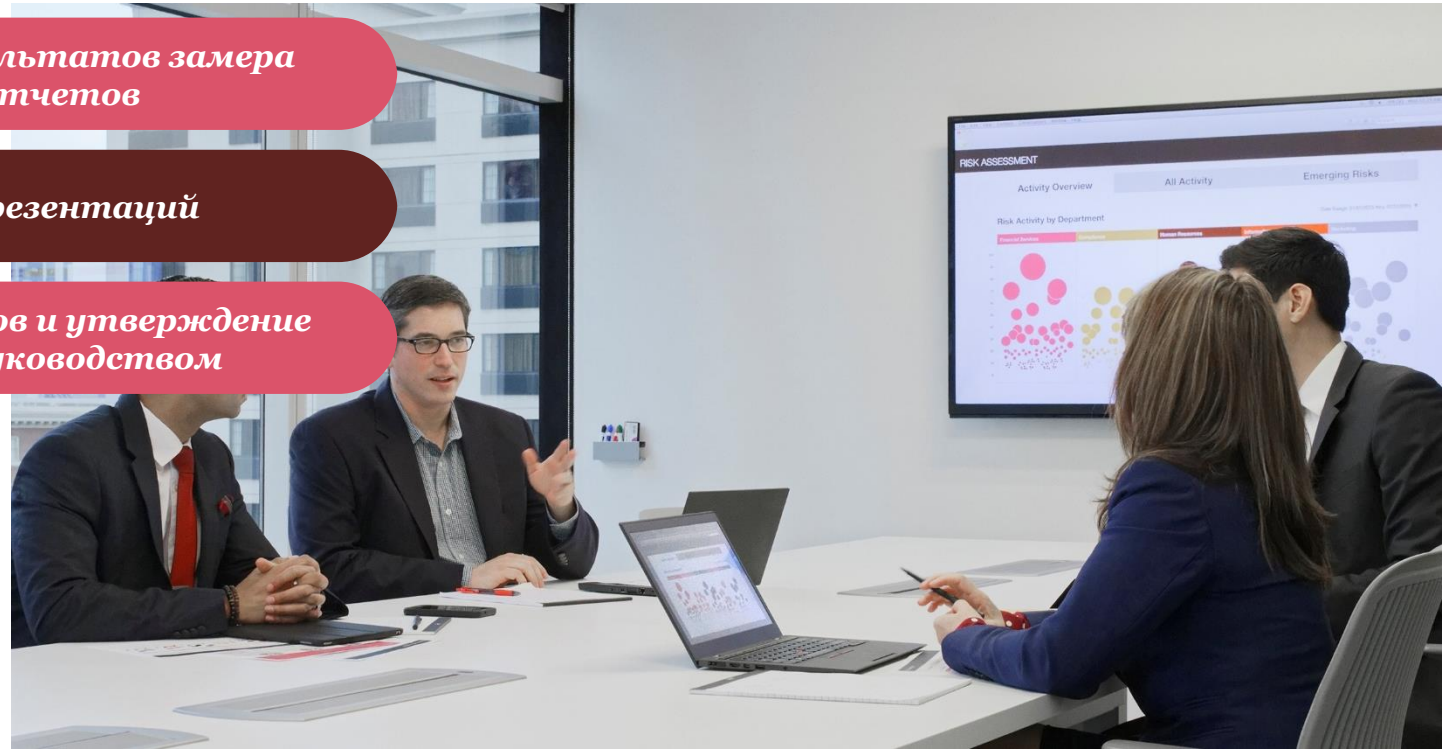
Шаг 1	*Подготовка KPI/KRI с бизнес-подразделениями*
Шаг 2	*Сбор данных для реализации и автоматизации KPI/KRI*
Шаг 3	*Тестирование и отладка KPI/KRI*

Этап 3. Презентация результатов отчетности

Презентация результатов

На данном этапе собранная информация и анализ результатов замера KPI/KRI докладывается в формате, понятном руководству и бизнес-подразделениям с целью принятия ими последующих информированных решений.

Шаг 1	***Накопление и анализ результатов замера KPI/KRI для подготовки отчетов***
Шаг 2	***Подготовка отчетов и презентаций***
Шаг 3	***Презентация результатов и утверждение дальнейших действий с руководством***



Формула взвешенных решений

Примеры KPI/KRI по ИБ

Пример определения KPI/KRI (1/2)

Ключевая роль	Инициативы	Общие интересы	Предложения Службы ИБ
ИТ директор	• Оптимизация затрат на ИТ • Повышение уровня автоматизации бизнес-процессов • Повышение отказоустойчивости ИТ систем • Сокращение времени введения новых ИТ систем	• Автоматизация процесса предоставления доступов • Снижение количества недостатков по итогам ежегодного аудита • Повышение защищенности критичных систем • Повышение уровня ИБ при сокращении затрат	• Внедрение системы IDM • Разработка ролевой модели доступа для критичных систем • Внедрение автоматизированного средства тестирования и установки обновлений ИБ • Обучение разработчиков основам безопасной разработки • Внедрение средства контроля привилегированных пользователей
Директор департамента дистанционных каналов обслуживания	• Увеличение количества пользователей мобильного-банка • Повышение удовлетворенности клиентов мобильного-банка	• Повышение доверия клиентов к мобильному-банку • Сокращение уровня мошеннических операций • Повышение уровня защищенности мобильного-банка	• Внедрение безопасного модуля API по защите мобильного-банка • Реализация одноразовых кодов на базе push-уведомлений • Упрощение аутентификации при входе в мобильный-банк и при критичных транзакциях

Пример определения KPI/KRI (2/2)

Ключевая роль	Предложения Службы ИБ	KPI	KRI
ИТ директор	Внедрение системы IDM	• % систем подключенных к IDM • % критичных систем подключенных к IDM	• Несанкционированный доступ к КИ под УЗ уволенного сотрудника • Вероятность и последствия разглашения конфиденциальной информации • Финансовые или репутационные потери в результате компрометации ИС • Нарушение бизнес-процесса в следствии несвоевременного устранения уязвимости ИБ
	Разработка ролевой модели доступа для критичных систем	• % сокращения заявок на открытие доступов • % сокращения времени выполнения заявки на предоставление доступа	
	Внедрение автоматизированного средства установки обновлений ИБ	• % уязвимостей устраненных в срок SLA	
	Обучение разработчиков основам безопасной разработки	• % сокращения критичных уязвимостей в новых системах	
	Внедрение средства контроля привилегированных пользователей ИС	• % сокращения инцидентов с привилегированными пользователями	
Директор департамента дистанционных каналов обслуживания	Внедрение безопасного модуля API по защите мобильного-банка	• % повышения доверия мобильному-банку со стороны клиентов (на основе ежегодного опроса)	• Потери компании вследствие фрода с использованием мобильного-банка • Падение капитализации и доверия к компании вследствие публично известных инцидентов ИБ • Отток клиентов вследствие сложной аутентификации
	Реализация одноразовых кодов на базе push-уведомлений	• % снижения инцидентов, связанных с фродом на мобильном-банке	
	Упрощение аутентификации при входе в мобильный-банк и при критичных транзакциях	• % снижения времени при аутентификации • % снижения обращений клиентов, связанных с проблемами при аутентификации	

Пример каскадирования KPI/KRI

Стратегические цели компании

- Предоставление лучшего клиентского сервиса
- Повышение капитализации компании

KPI

- % повышения доверия к мобильным и online каналам обслуживания со стороны клиентов (на основе ежегодного опроса)

KRI

- Падение капитализации и доверия к компании вследствие публично известных инцидентов ИБ

Цели бизнес-подразделений

- Повышение удовлетворенности клиентов мобильного-банка
- Повышение автоматизации бизнес-процессов

KPI

- % снижения инцидентов, связанных с фродом
- % автоматизации бизнес-процессов

KRI

- Падение выручки вследствие мошеннических операций
- Остановка бизнес-процесса вследствие проблем с доступом

Инициативы линейных подразделений

- Повышение безопасности мобильного-банка
- Автоматизация процесса предоставления доступов

KPI

- % снижения инцидентов, связанных с фродом на мобильном-банке
- % систем, подключенных к IDM

KRI

- Падение выручки вследствие мошеннических операций в мобильном-банке
- Несанкционированный доступ к КИ под УЗ уволенного сотрудника

Рекомендации

- Связывайте метрики ИБ с целями и задачами бизнес-подразделений
- Каскадируйте KPI «сверху-вниз» для донесения ценности мер защиты и проектов ИБ до бизнеса
- Создавайте метрики, которые ведут к конкретным решениям и действиям
- Используйте KPI как точки образования диалога с бизнес-подразделениями
- Начните с малого. Не создавайте KPI и отчетность по тем процессам ИБ, которые не существуют или недостаточно зрелые
- Начните диалог с теми бизнес-подразделениями, кто уже на вашей стороне
- Создавайте выгоды для тех, кто принимает решения
- Заложите ресурсы на поддержку процесса отчетности по ИБ

www.pwc.ru/cybersecurity

Курзин Михаил
Старший менеджер
Cyber security
+7 (903) 733-69-44
mikhail.kurzin@pwc.com