Риск-ориентированная модель информационной безопасности

Защита, которая реально работает, не тормозит бизнес и дает прогнозируемый эффект

СТРУКТУРА СЛАЙДОВ

РУКОВОДИТЕЛЬ НАПРАВЛЕНИЯ ИБ - ПИВАК ПАВЕЛ

- Опыт работы 16+
- Имею 3 высших образования и степень MBA
- Являюсь экспертом ИБ в ритейле
- Являюсь квалицированным экспертом DPO
- Офицер запаса

ТРЕНДЫ ИБ И ПРИОРИТЕТЫ РАЗВИТИЯ

ТРЕНДЫ ИБ

- Атака вирусом-шифровальщик
  - Практическое бэкапирование, как обязательное условие для надежной работы
  - Скрытое и долгое нахождение хакеров в корп.сети Продолжается продажа доступов в Darknet
- Участившиеся DDoS-атаки, brute force-attack
- Эксплуатация уязвимостей в сервисах компаний и веб-приложениях
- Атаки на Retail удвоились сначала 2025 года
- Роскомнадзор ужесточает правила работы с ПДн и штрафные санкции за их утечку
- Россия будет оставаться в уже привычном для себя режиме «повышенной опасности», атаки DDoS, ВПО, фишинг, соц.инжерения и тп

Культура ИБ

- Развитие компетенций ИБ
- Повышение осведомленности
- Проведение киберучений

Технологии

- «Shift left» на всем этапе ЖЦ
- Эффективное реагирование
- Современные методы защиты

Комплаенс

- Соблюдение НД по ИБ и ФЗ
- Распределение обязанностей в системе управления ИБ
- Развитие практик управления рисками кибербезопасности

АКТУАЛЬНОСТЬ

ПРОБЛЕМАТИКА

- Все компании идут в цифровизацию и трансформацию бизнеса, чтобы осваивать новые сегменты, создавать новые услуги и сервисы либо продолжают экспансию
- Хакеры становятся все изобретательнее (эволюция ИИ, ML, Deepfake)
- Длительный жизненный цикл систем (либо устаревшее ПО)
- Кадровый дефицит специалистов ИБ

ПРИОРИТЕТЫ РАЗВИТИЯ ИБ (ЦЕЛИ)

- Повышение киберустойчивости и отказоустойчивости бизнеса
- Выстраивание практической безопасности
- Повышение взаимодействия с бизнесом и ИТ (реализация подхода «Shift Left»)
- Необходимость развития собственной экспертизы ИБ для сокращения time-to-market
- Повышение культуры кибербезопасности и обучение сотрудников кибергигиене
- Выстраивание периметровой и эшелонированной защиты
- Повышение эффективности контролей ИБ
- Импортозамещение продолжается…

РИСК-ОРИЕНТИРОВАННАЯ МОДЕЛЬ

ПРОБЛЕМА ВОСПРИЯТИЯ РИСКОВ ИБ

- Трудно спрогнозировать вероятность возникновения и точно оценить ущерб
- Бизнес часто не осознает реальность рисков ИБ, считая их нереализуемыми

МЕНЯЕМ ВОСПРИЯТИЕ БИЗНЕСА

- Фокус на анализе рисков
- Сценарный подход
- Приоритизация мер защиты
- Оперативное реагирование
- Постоянная актуализация

«ЧТО ГОВОРИТ БИЗНЕС?»

КЛЮЧЕВЫЕ РИСКИ НА ОСНОВЕ ИНТЕРВЬЮ С CEO-1

Остановка ключевых систем
(Нарушения работы критических бизнес-процессов)

Утечка персональных данных
+ (Нарушение требований законодательства в части обработки ПДн)

Утечка коммерческой тайны

ЭКСПЕРТНАЯ ОЦЕНКА РИСКОВ ИБ

Бизнес-риск/описание события	Присущий или остаточный риск	Митигация рисков
Риск № 1 Нарушения приведшие к остановке ключевых систем	КРИТИЧНЫЙ	Инвентаризация и ресертификация доступов (разграничение прав и полномочий); Внедрение IDM-системы; Аудит ключевых ИС
Риск № 2 Нарушение функционирования операционных процессов, из-за остановки критичных ИС	ВЫСОКИЙ	Внедрение процессов управления уязвимостями и патч-менеджментом; почтовая песочница; сегментация сети/ РЦОД; Контроль доступа; DRP и BCP, MFA
Риск № 3 Утечка персональных данных, и, впоследствии, наложение штрафа до 500 млн.	СРЕДНИЙ	Аудит персональных данных и приведение в соответствии с 152-ФЗ и 21 приказом ФСТЭК ИСПДн и документов Компании
Риск № 4 Утечка коммерческой тайны	НИЗКИЙ	Внедрение DLP-системы; NDA, Внедрение Режима КТ и Перечня ИКТ; Формирование внутренней культуры ИБ
Риск № 5 Остановка ключевых бизнес-процессов по причине сбоя в ключевых системах	ИНФОРМАТИВНЫЙ	Разработка регламентов BCP, Внедрение Политики ИБ и требований ИБ; сегментация сети/ РЦОД; WAF/Anti-DDoS/Anti-bot;

СВОДНАЯ ОЦЕНКА РИСКОВ

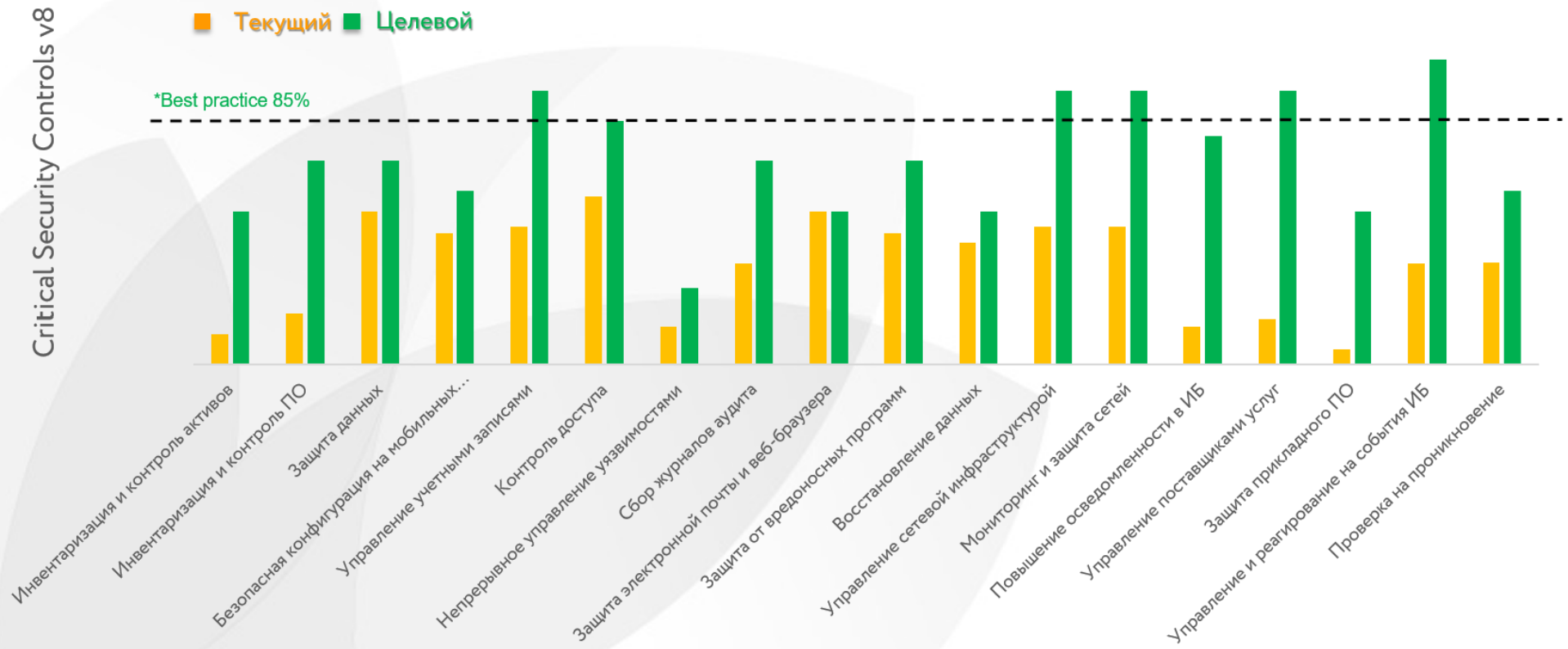
Полный реестр рисков ИБ			
Наименование риска	Описание угрозы	Описание типа актива	Уровень риска
Риск 1	XXX	XXX	ВЫСОКИЙ
Риск 2	XXX	XXX	ВЫСОКИЙ
Риск 3	XXX	XXX	ВЫСОКИЙ
Риск 4	XXX	XXX	ВЫСОКИЙ
Риск 5	XXX	XXX	ВЫСОКИЙ
Риск 6	XXX	XXX	ВЫСОКИЙ
Риск 7	XXX	XXX	ВЫСОКИЙ
Риск 8	XXX	XXX	ВЫСОКИЙ
Риск 9	XXX	XXX	ВЫСОКИЙ
Риск 10	XXX	XXX	ВЫСОКИЙ

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ СТАНДАРТ CIS CONTROL 18

40%
Уровень реализации

18 из 56 реализовано
Базовые контроли CIS IG1:

НИЗКИЙ
Уровень зрелости процессов ИБ



ПОДХОД ИБ - ЧЕРЕЗ ЗАБОТУ И ДОВЕРИЕ К РЕЗУЛЬТАТУ

БЕЗОПАСНО

- Внедрение механизмов безопасности на моменте разработке дизайна проекта
- Делаем взаимодействие с ИБ удобным и простым как для клиента так и для бизнеса

ДОВЕРИЕ

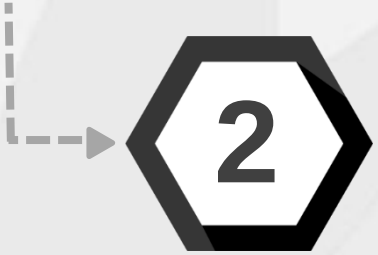
- Клиент-ориентированная ИБ
- Прозрачные процессы ИБ
- Своевременно говорим о проблемах и помогаем в их решении

УСТОЙЧИВОСТЬ

- Проактивная защита и восстановление до нанесения вреда интересам бизнеса

КИБЕРЗАЩИЩЕННОСТЬ

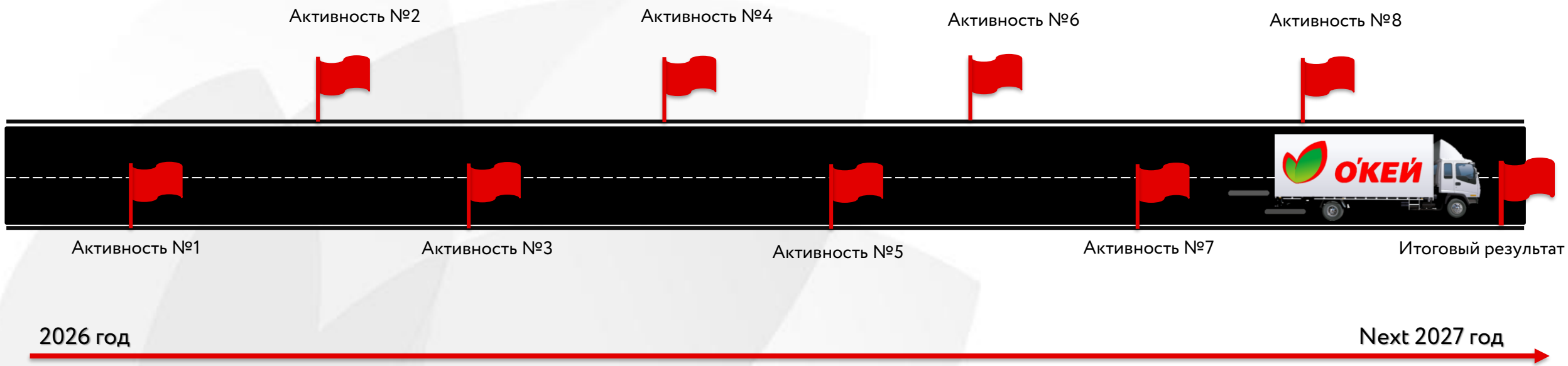
- Все продукты и сервисы проходят аудит ИБ, результаты работы понятны, измеримы и прозрачны



С ЗАБОТОЙ О КЛИЕНТЕ И БИЗНЕСЕ

- Вместе с бизнесом решаем проблемы с безопасностью
- Знаем о угрозах, просвещаем о рисках и учим их митигировать

ТАКТИЧЕСКИЙ ROADMAP



ИТОГО

Погружение в бизнес

Слушать, понимать, участвовать. Идём на планёрки продаж, в магазины, на склад и тп

Фокус на реальных угрозах

Не гонимся за модными атаками. Угроза без бизнес-сценария — гипотеза, не задача

Мост между ИТ и бизнесом

Говорим на языке рисков и денег для бизнеса, на языке доступности для ИТ

Спасибо за внимание!