

# От нуля к единице

Как мы совершили «прыжок» в зрелости кибербезопасности



## Иван Дмитриев

Заместитель генерального директора  
по информационной безопасности – директор  
дирекции по безопасности

- ✓ 15 лет в ИБ
- ✓ MBA Стратегический менеджмент
- ✓ Сертифицированный аудитор

[@idmitriev](#)

[Dmitriev.iv@esphere.ru](mailto:Dmitriev.iv@esphere.ru)

**СберКорус** - разработчик цифровых продуктов и сервисов, которые создают комфортную среду для ведения и развития бизнеса

37

компаний из списка Forbes «200 крупнейших компаний России» работают с нами

1 млн+

клиентов пользуются нашими сервисами

6000

Элементов серверной инфраструктуры

200+

Интеграций с информационными системами Банка и клиентов

Мы ваш недуг в подвиг обратим:

## Решили строить процессы, а не копить артефакты



**Май 2022**

Инцидент  
кибербезопасности



**Ноябрь 2023**

Ликвидированы  
последствия инцидента.  
Подготовлена стратегия  
Безопасности



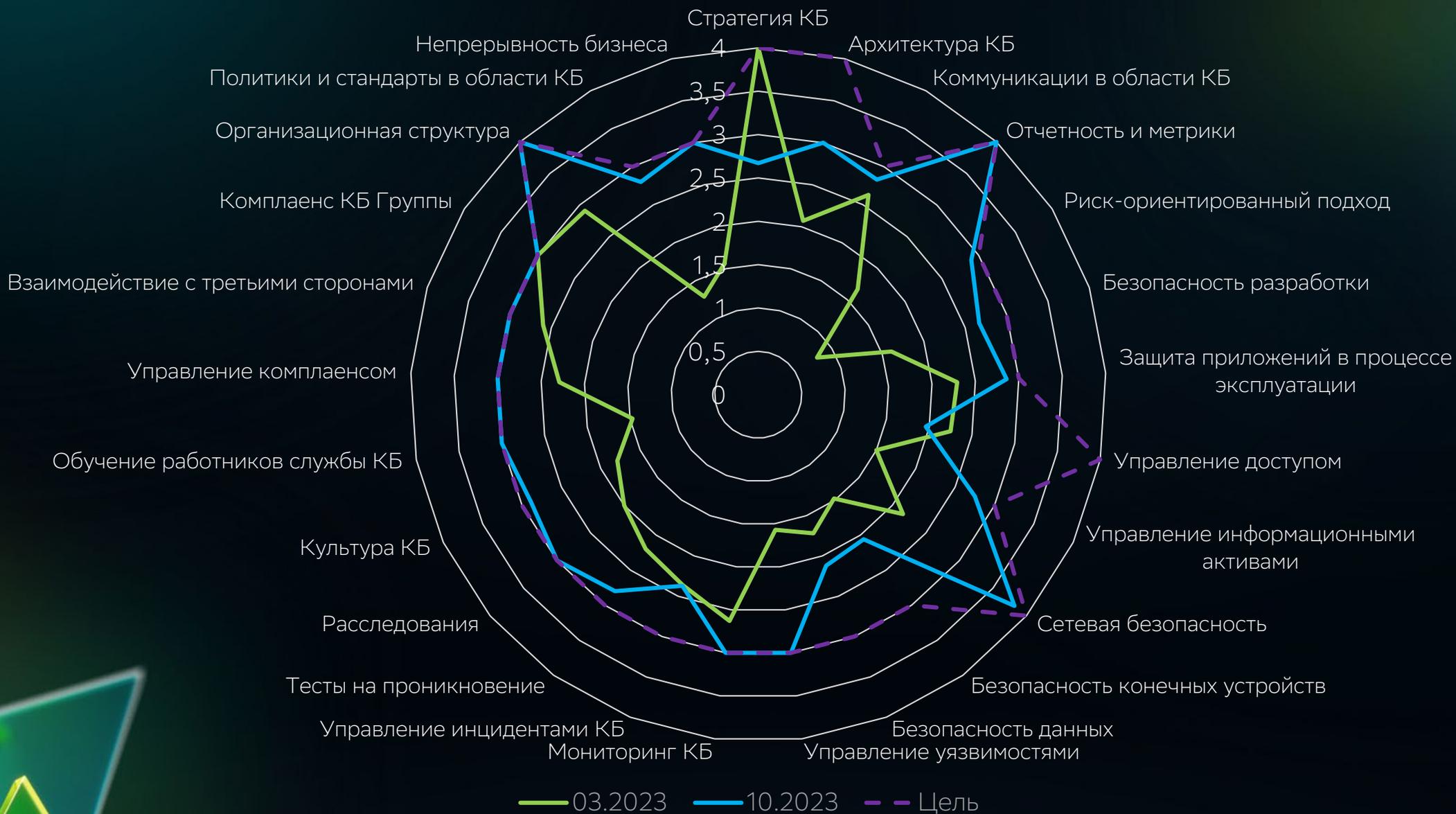
**Февраль 2023**

СберКорус признан  
«Фокусным» ДЗО.  
Стратегия Меняетс



**Октябрь 2023**

Выход в «Зеленую»  
зону уровня зрелости  
КБ. Очередная смена  
стратегии



# Пирамида результата

## Миссия:

Мы создаем удобный цифровой мир для развития бизнеса

## Ценности:

Клиент. Команда.  
Непрерывные улучшения



## Мечта:

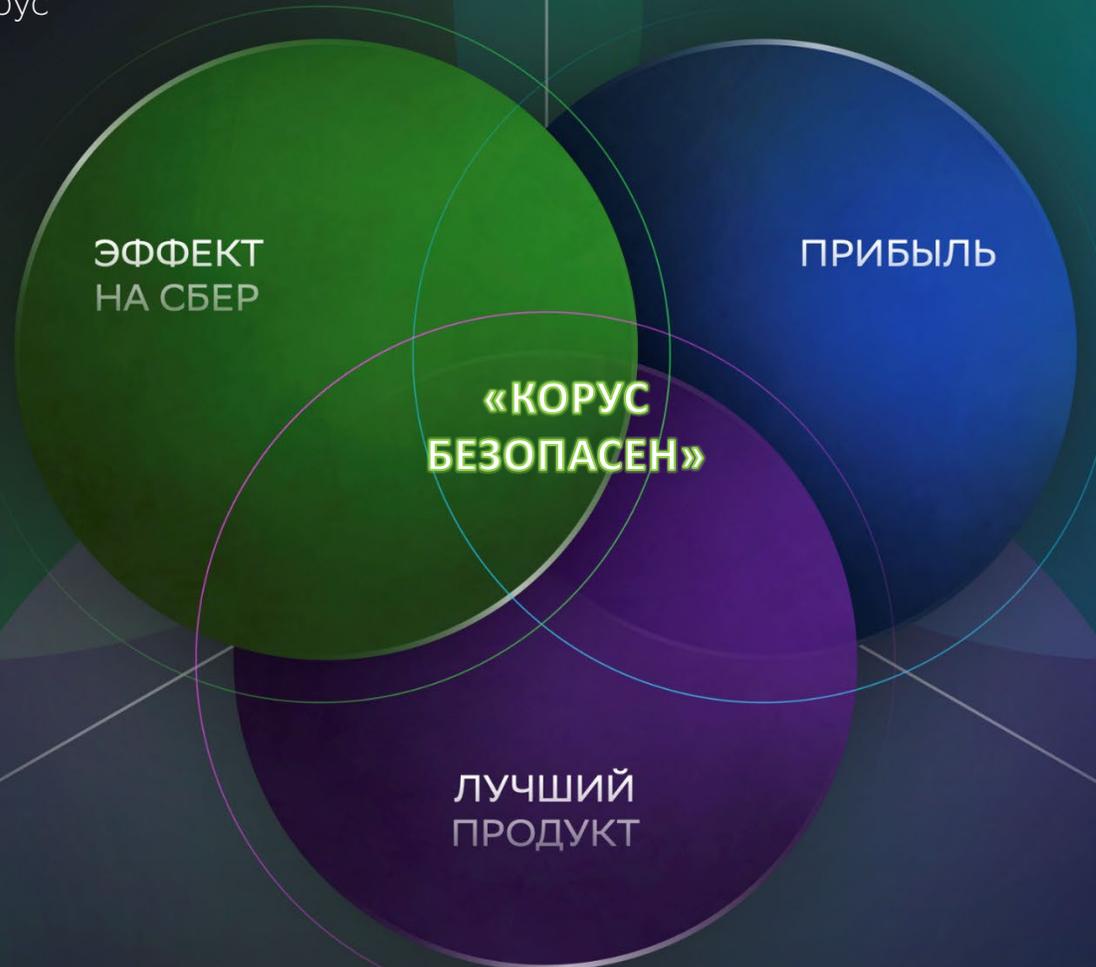
С гордостью рассказать о прыжке от нуля к единице

## Цель:

Сделать безопасность, которая позволяет бизнесу развиваться

# Стратегия и целеполагание (ЧТО?)

Минимальные риски для Банка и компаний экосистемы – Корус компания первого выбора для экосистемы.

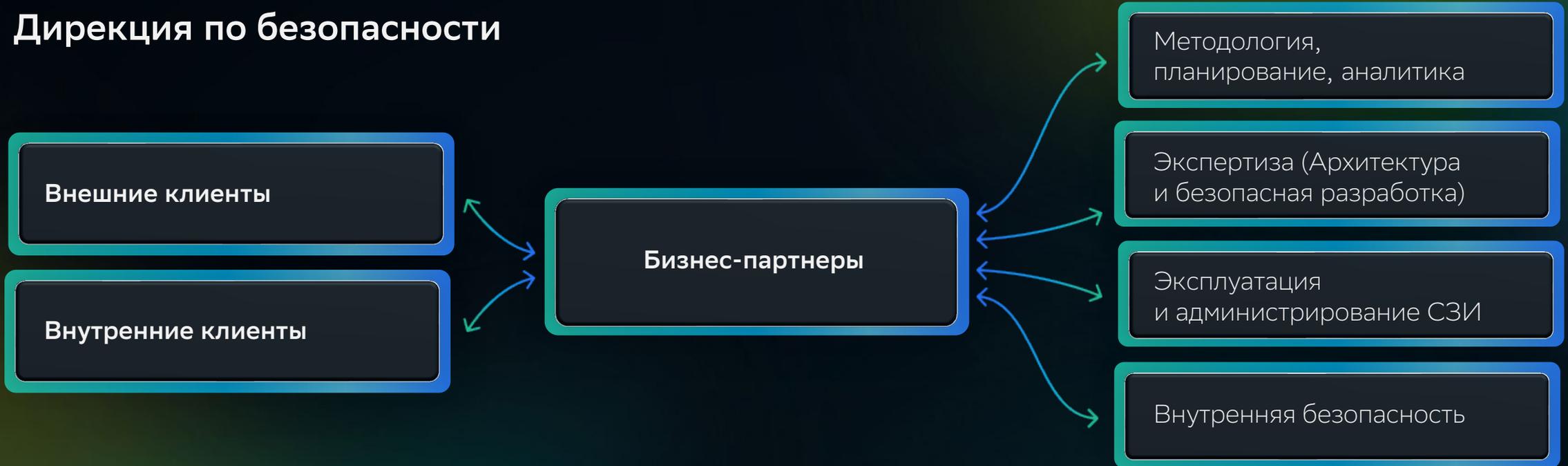


Оптимизация расходов на безопасность.

Нулевые потери от инцидентов

Безопасность продукта – конкурентное преимущество компании

## Дирекция по безопасности



## Основные принципы

1. Несоответствие профилю позиции по софт-скиллам и ценностям критично
2. Прозрачная мотивация и целеполагание
3. Специализация со взаимозамещением
4. Лидеры направлений
5. Делегирование
6. Обратная связь и поощрение чемпионов

## Безопасность инфраструктуры и сетей

Безопасность корп. сети (IaaS, PaaS) и внешнего периметра ✓

Защита web-приложений ✓

Защита от ddos ✓

Шифрование канала (IPSEC/L2TP) ✓

Защищенный удаленный доступ ✓

Безопасность Wi-Fi ✓

Межсетевое экранирование ✓

Микро сегментация ✓

NGFW ✓

Host based Firewall ✓

Защита от вторжений (IPS/IDS) ✓

Контентная-фильтрация (url-filtering) ✓

Защита почты ✓

Защита от ботов ✓

anti-bot ✓

Captcha ✓

Антивирусная защита ✓

Анализ безопасности файлов (sandbox) ✓

Анализ сетевого трафика (NTA) ✓

Безопасность SaaS ✓

Защита web-приложений ✓

Защита от ddos ✓

Защита от ботов ✓

Шифрование сессии ✓

Шифрование канала ✓

SSO ✓

Контроль работы в облаках (CASB) ✓

## Безопасность сред контейнеризации

Безопасность репозитория ✓

Подписание образов ✓

Безопасность контейнеров RunTime ✓

Управление секретами ✓

CI/CD ✓

## Service mesh

Управление аутентификацией ✓

Шифрование сессии ✓

Микросегментация ✓

Логирование событий аудита ✓

Сегментация ✓

## Защита конечных устройств

Freeboot шифрование ✓

Средства доверенной загрузки (HSM) ✓

Управление конфигурациями ✓

Контроль доступа к сети (NAC) ✓

Контроль отчуждаемых носителей ✓

Управление мобильными устройствами (EMM) ✓

Управление сертификатами ✓

Контроль приложений ✓

Антивирусная защита ✓

Управление обновлениями ✓

## Управление правами и пользователями

Управление УЗ и идентификаторами (IAM) ✓

Управление ролями и полномочиями ✓

Разделение полномочий ✓

Управление привилегированными пользователями (PAM) ✓

Управление ТУЗ ✓

## Аутентификация

Управление паролями и парольной политикой ✓

Многофакторная аутентификация (MFA) ✓

PasswordLess ✓

Аппаратные ключи ✓

## Управление аутентификацией

SSO ✓

Управление сессиями пользователей ✓

Управление сессиями ТУЗ ✓

## Управление правами и доступами

## Управление уязвимостями

Управление уязвимостями (VMP) ✓

Анализ защищенности периметра (pentest) ✓

Платформа анализа информации о внешних угрозах (TIP) ✓

Технологии обмана и запутывания атакующих и злоумышленников (honeypot) ✓

Инвентаризация и управление активами (CMDB) ✓

## Мониторинг и реагирование на инциденты ИБ

Логирование событий аудита ✓

Расширенный мониторинг ИБ (EDR) ✓

Анализ поведения пользователей (UEBA) ✓

## Управление инцидентами ИБ (SIEM)

Автоматизированное управление инцидентами ИБ (IRP/SOAR) ✓

Расследование инцидентов ИБ ✓

anti-fraud ✓

## Управление ИБ, рисками и compliance

Обучение по ИБ ✓

## Проведение социо-технических исследований

Система управления ИБ (SGRS) ✓

## Безопасность приложений

Анализ безопасности кода (SAST) ✓

Анализ OpenSource компонентов (SCA/OSSA) ✓

Анализ защищенности образов ✓

Анализ защищенности web-приложений (DAST) ✓

Безопасность api ✓

Управление секретами ✓

Безопасность мобильных приложений (MAST) ✓

Поиск утечек исходных кодов ✓

Шифрование сессии ✓

Обезличивание данных ✓

## Безопасность данных

Сегментация данных ✓

Классификация данных ✓

Контроль неструктурированных данных ✓

Контроль целостности ✓

Токенизация данных ✓

Маскирование данных ✓

Защита БД (DAM) ✓

Контроль утечек данных (DLP) ✓

Шифрование данных ✓

## Безопасность BigData

Классификация данных ✓

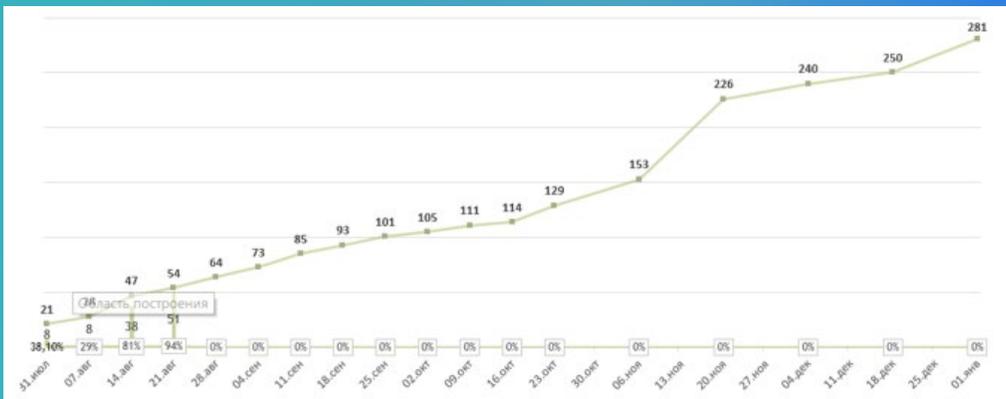
Контроль целостности данных ✓

Шифрование данных ✓

Вопрос 2. Для основных процессов КБ определены метрики.

ДА

Да, в компании определен ряд фокусных метрик по КБ. Отчетность по данным метрикам предоставляется СЕО и СЕО-1, а также ВР Банка еженедельно.

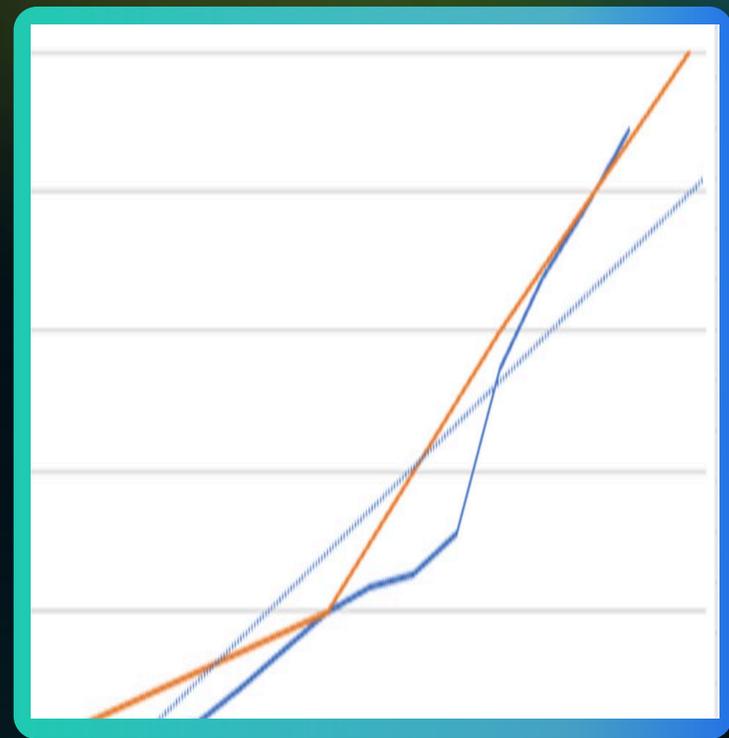


## Основные принципы

1. Контроль != ответственность и авторитарные указания
2. Разделение ЛНА, рабочих документов и гайдов
3. Смежники справа-слева тоже команда, они имеют доступ ко всей информации и тоже профессионалы
4. Взаимная подотчетность
5. Непрерывные измерения
6. Открытость в признании факапов

# Пример измеримости достижения результата

Всего доменов	As is	За VPN	За WL	Удалено	В публичном доступе	Отправлена заявка в BI.Zone	Подготовлен профиль	Тестирование	Переведен за WAF	ФАКТ	ПЛАН
368	0	0	0	0	368	60	2	15	7	2%	0%
368	0	0	0	0	368	0	4	73	7	2%	
368	0	0	0	0	368	0	4	69	11	3%	
368	0	0	0	0	368	6	2	70	12	3%	
368	0	0	0	0	368	0	4	71	15	4%	
368	0	0	0	0	368	0	4	53	33	9%	
368	0	0	0	1	367	7	3	34	53	14%	
368	0	0	0	5	363	0	0	29	73	20%	20%
368	0	0	0	20	348	0	0	20	82	24%	
368	0	0	0	23	345	1	0	15	87	25%	
368	26	0	0	56	286	7	0	37	89	31%	
372	31	0	0	136	205	16	0	23	112	55%	60%
373	34	0	0	155	184	14	0	13	124	67%	
373	34	0	18	156	165	12	0	10	128	78%	
373	34	0	33	153	153	0	0	12	136	89%	
											100%



# Q&A

**Иван Дмитриев**

Заместитель генерального директора  
по информационной безопасности

[@idmitriev](#)

