



**Регулярная оценка уровня зрелости ИБ
в рамках территориально
распределенной группы компаний.**

Александр Дворянский

Проблематика/специфика Группы

#1

Территориально
распределенные дочки

#2

В каждой ДЗК различный
уровень зрелости ИБ

#3

Недостаточное
финансирование ИБ

#4

Недоукомплектованность
штата



#5

В каждой ДЗК различный
уровень цифровизации бизнеса

Оценка базовых показателей



- ☐ Безопасность при работе с внешними подрядчиками
 - ☐ Безопасность на стадиях жизненного цикла информационных систем
 - ☐ Антивирусная защита
 - ☐ Регистрация и мониторинг событий ИБ
 - ☐ Безопасность удаленного доступа
 - ☐ Резервирование и резервное копирование
 - ☐ Защита от утечек конфиденциальной информации
 - ☐ Безопасность при управлении персоналом
 - ☐ Безопасность при работе с мобильными устройствами
 - ☐ Безопасность сети и сетевого доступа
 - ☐ Управление доступом и парольная защита
 - ☐ Криптографическая защита информации
 - ☐ Управление техническими уязвимостями и безопасная конфигурация
-

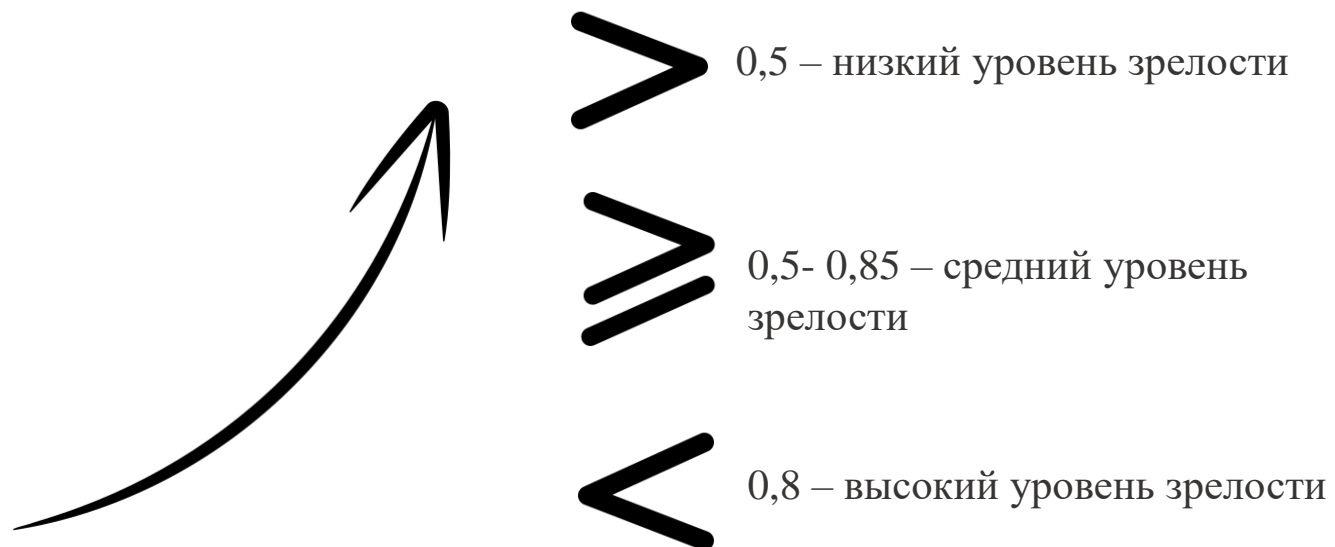
Оценка индивидуальных показателей и требований регулятора



- ☐ Защита персональных данных
 - ☐ Защита коммерческой тайны
 - ☐ Управление инцидентами ИБ
 - ☐ Вовлеченность менеджмента в вопросы информационной безопасности
 - ☐ Обеспечение защиты КИИ
 - ☐ Управление активами и рисками ИБ
 - ☐ Обучение и повышение осведомленности в области ИБ
 - ☐ Управление непрерывностью бизнеса
 - ☐ Иные показатели
-

Итоговая интерпретация результатов

Оценка частного показателя ИБ	Критерий выставления оценки
0	Требования частного показателя ИБ не выполняются
0,5	Требования частного показателя ИБ выполняются не полностью или не для всех типов конфиденциальной информации к которым они применимы
1	Требования частного ИБ выполняются полностью и для всех типов конфиденциальной информации к которым они применимы



Единая концепция развития

**Для чего нам это
надо?**

#1

Динамика развития от ИБ к КБ

**И что мы с этим
делаем?**

#2

Индивидуальная модель развития
для разных групп ДЗК

**Для чего им это
надо?**

#3

Гармоничный рост и развитие ДЗК

Экосистемный подход

#1

- Определение политики развития ИБ в рамках Группы Компаний.
- Контроль уровня зрелости ИБ, определение и реализация мероприятия по противодействию векторам атак по Группе компаний

#2

- Мониторинг и реагирование на инциденты 24/7.
- Осуществление развития централизованных сервисов по безопасности и интеграция решений (с учетом потребностей ГК)



#3

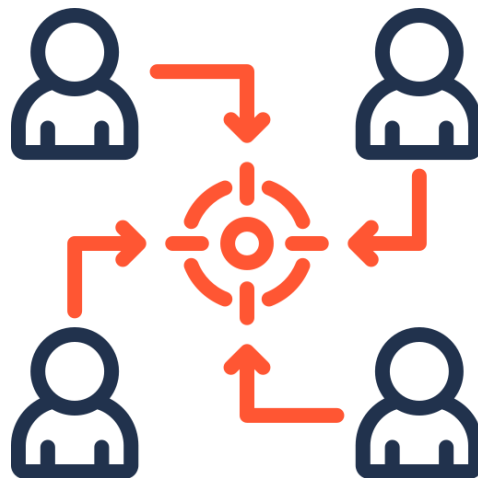
- Регулярное тестирование инфраструктуры на устойчивость, выявление недостатков в линиях защиты.
- Консолидация экспертизы в области информационной безопасности с привлечением внутренних и внешних экспертов

#4

- Нормативное регулирование процессов информационной безопасности и локальной нормативной базы
- Контроль выполнения федерального законодательства в области обеспечения защиты информации

Сервисная модель

Общая цель



#1

Централизованное обеспечение защиты каналов связи между ДЗК и системы межсетевого экранирования

#2

Регулярный обмен опытом и экспертизой в рамках Группы

#3

Оценка безопасности информационных систем путем моделирования атаки злоумышленников на ДЗК (Пентест)

#4

Укомплектование штатов в области ИБ в ДЗК/формирование кадрового резерва

#5

Организация централизованной системы обучения и повышения осведомленности пользователей Группы в вопросах ИБ