FREEDOM HOLDING CORP.

# Как адаптировать управление ИБ под масштаб

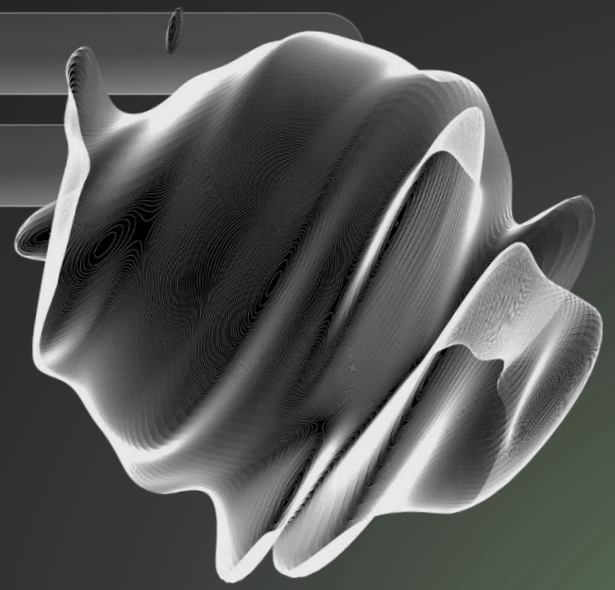
*Объединяем процессы, технологии и людей в экосистему и сохраняем гибкость*

14/11/2025

# О себе

FREEDOM HOLDING CORP.

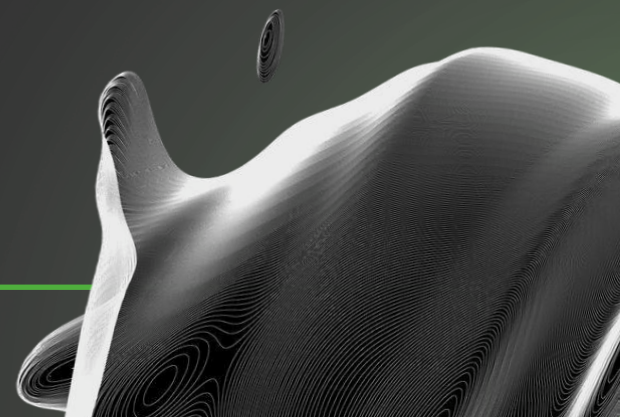
- 16 лет в ИБ (финансовый сектор, регуляторы, e-com)
- Директор по информационной безопасности Freedom Holding Operations
- Vice President ISACA Astana Chapter
- CISSP, CISM



# Потребности международного бизнеса

FREEDOM HOLDING CORP.

- Расширение географии присутствия, а это разные: регуляторика, зрелость процессов компаний, инфраструктура, культура
- Единое окно для ключевых функций ИБ:  управление стратегией, координация и прозрачность по инцидентам\рискам ИБ, при разном уровне самостоятельности бизнеса
- Адаптивное к уровню зрелости распределение ответственности с регионами
- Гибкость для локальных требований и приоритизации
- Измерение эффективности по общим правилам
- Поддержка динамичных изменений: M&A, облака, ИИ, внешние угрозы



# Основы масштабирования стратегии

FREEDOM HOLDING CORP.

Выбор базиса: ISO 27001, NIST CSF, CIS Controls

Единые стандарты и принципы безопасности,
поддерживающие цели бизнеса во всей географии присутствия

Централизованные стандарты — гибкое и риск-
ориентированное применение в регионах

Одинаковые правила взаимодействия между ИБ и бизнесом
(единый комитет по киберрискам, совместные KPI)

# Операционные модели ИБ

## *Централизация против Автономности*

Унификация, повторяемость и масштабируемость процессов
*VS*
Необходимость учитывать уникальные потребности каждой компании

Легкий старт готовых процессов ИБ для новых компаниях с централизованной командой и инструментами
*VS*
Долгое локальное развитие для того же уровня зрелости

Узкоспециализированные эксперты с возможностью роста и смены профиля внутри HQ
*VS*
Широкопрофильные эксперты в каждом регионе

Единый технологический стек с экономией на масштабе и компетенциях
*VS*
Системный риск при уязвимости ключевого продукта вашего стека

# Федеративная модель ИБ

*(баланс централизации и автономности)*


FREEDOM HOLDING CORP.

- **HQ:** стратегия, стандарты, контроль
- **Общий сервис-каталог ИБ** (AppSec/RedTeam/BlueTeam/SOC/Audit/Methodology)
- **Центральный контур:** SOC, IR, Threat Intel, GRC, архитектура
- **Оцифровка эффективности:** метрики, контроль, непрерывное улучшение

- **Регионы:** внедрение, отчётность, локальная адаптация
- **Локальные стейкхолдеры:** DPO/CISO региона, владение рисками и процессами, заказчик централизованных сервисов
- **Использование гибридных архитектур** для киберустойчивости, создания фонда замены, снижения vendor lock
- **Единый RACI** и **регламент эскалаций**

# Процессы и RACI

FREEDOM HOLDING CORP.

**Назначение владельцев процессов:** риск-менеджмент, архитектура, эксплуатация, реагирование

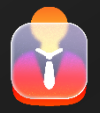
**Где выполняется:** HQ vs Local (Run/Change/Assure)

Согласованные сценарии реагирования, категорирование инцидентов, SLA

**Коммуникации:** частота, уровень участников, комитеты\еженедельные встречи, кризисные коммуникации

Разделение ролей снижает операционные риски и повышает прозрачность

Регулярная коммуникация между HQ и регионами - укрепления культуры единой безопасности



Участие представителя HQ в комитетах по ИБ\рискам регионов

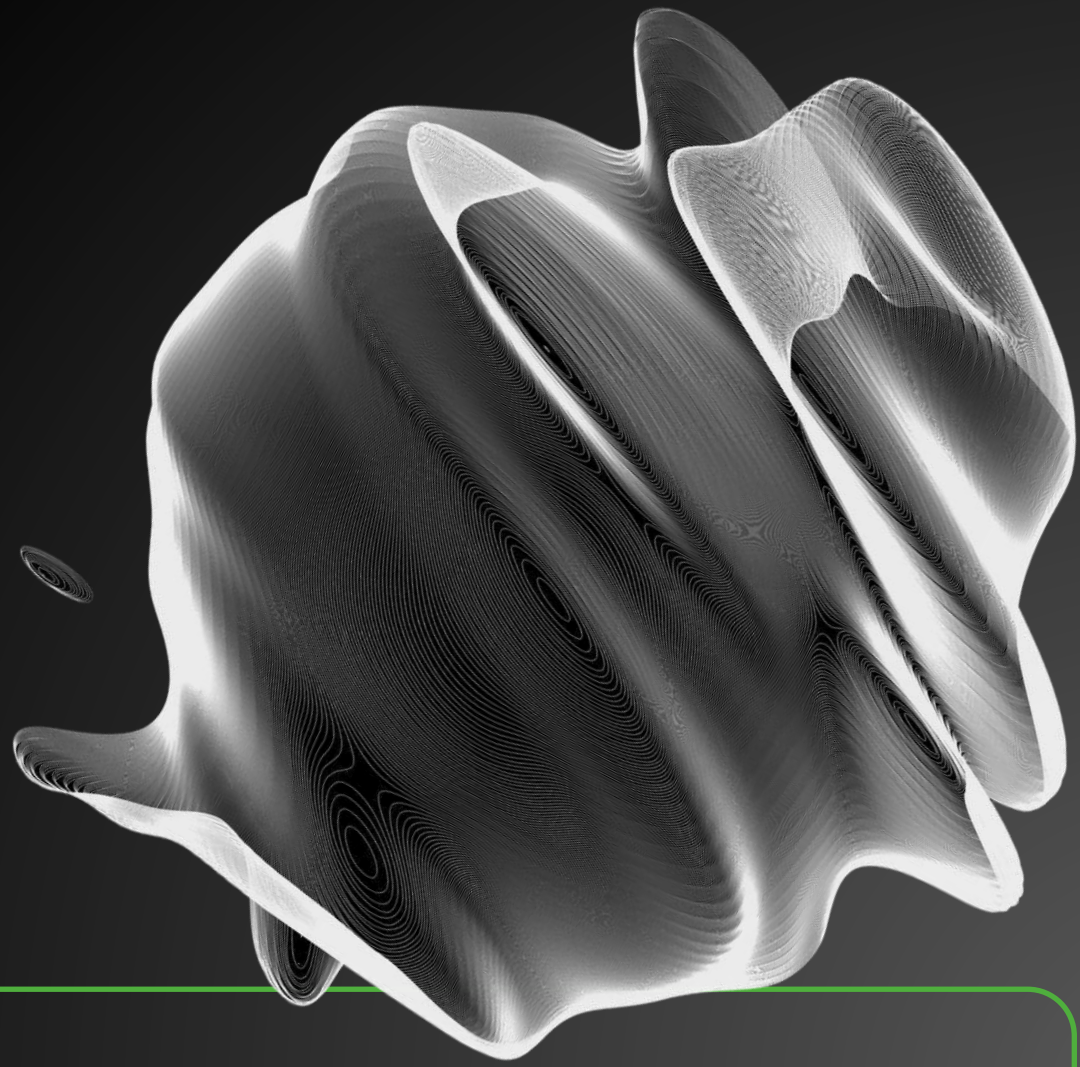
Назначение ключевых ролей по согласованию HQ (CISO, CyberRO)

# Метрики и контроль эффективности

FREEDOM HOLDING CORP.

*Выбирайте то, что поймет ваш бизнес:*

- Зрелость защиты (оценка по CIS)
- Risk-based KPIs через связь с финансовыми показателями:
  1. # инцидентов, повлиявших на выручку
  2. стоимость эксплуатации незакрытых уязвимостей (Value at Risk)
  3. % охвата контролями ИБ активов, генерирующих доход
- Затраты на ИБ (% от ИТ затрат, % от выручки)



# Примеры из практики

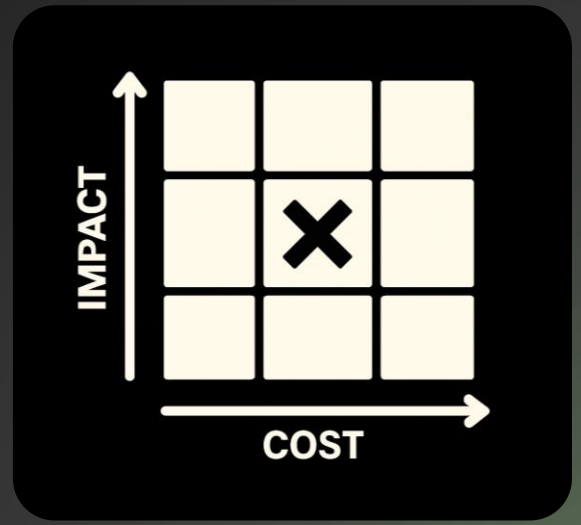
FREEDOM HOLDING CORP.

- **VM Center** - мониторинг уязвимостей внешней поверхности атаки с MasterCard RiskRecon (ROI 147%, Risk –50%)
- **SOC/Threat Intelligence Hub:** мониторинг утечек в DarkWeb и защита бренда группы компаний
- Централизация сервиса awareness и обучение практикам SSDLC *(адаптация под регуляторику страны, например: обработка ПНД, ЭЦП)*
- Формирование базового стандарта контролей ИБ

# Формирования внутреннего стандарта по ИБ

FREEDOM HOLDING CORP.

- CIS Critical Security Controls предлагает внедрить 56 контролей базовой кибергигиены IG1, затем расширять до IG2 (+74) и IG3 (+23)
- Добавляем аналитику рынка CIS Community Defense Model (74% атак из матрицы MITRE ATT&CK снижаются через CIS IG1)
- Cost of Cyber Defense (CIS) - какие контроли внедрять первыми и сколько это стоит
- Используя одинаковую базу - становитесь пресказуемыми
- Добавляйте модель угроз ВАШЕЙ организации и адаптируйте стандарт защиты
- Оценка AS IS текущей области покрытия контролей ИБ, выявление приемлимого ущерба и затрат для перехода к целевому состоянию



# Выводы и рекомендации

FREEDOM HOLDING CORP.

- Поддержка топ-менеджмента - фактор успеха
- Стартуйте с архитектуры, процессов и RACI, а не с инструментов
- Централизуйте аналитику и плейбуки, оставляйте регионам выполнение
- Масштабируйтесь через сервис-каталог и общие метрики
- Планируйте оценку и приведение в соответствие с комплаенс требованиями как часть операционного процесса, не отдельный проект
- Унификация ≠ стандартизация во всём (оставляйте пространство для гибкости)
- Обратная связь + изменение зрелости = новая стратегия ИБ

# Контакты

FREEDOM HOLDING CORP.


## Анатолий ПУДЕЛЬ

Директор по информационной безопасности
Freedom Holding Operations

profit_questions@frhc.group