Масштабируем защиту на группу компаний: в чем отличия?

КОНСТАНТИН ТИТКОВ

начальник Центра информационной безопасности дочерних и зависимых обществ

Банк ГПБ (АО)

О чем пойдет речь:

Часть 1. “Кибербезопасность? Нет, не слышали.”

Часть 2. “Сделал безопасно? А можешь повторить на 100-500?”

Часть 3. “А если проверю?”

Коротко о главном

РАЗДЕЛ 1. КАК ОБЫЧНО СТРОИТСЯ КИБЕРЗАЩИТА В КОМПАНИИ?

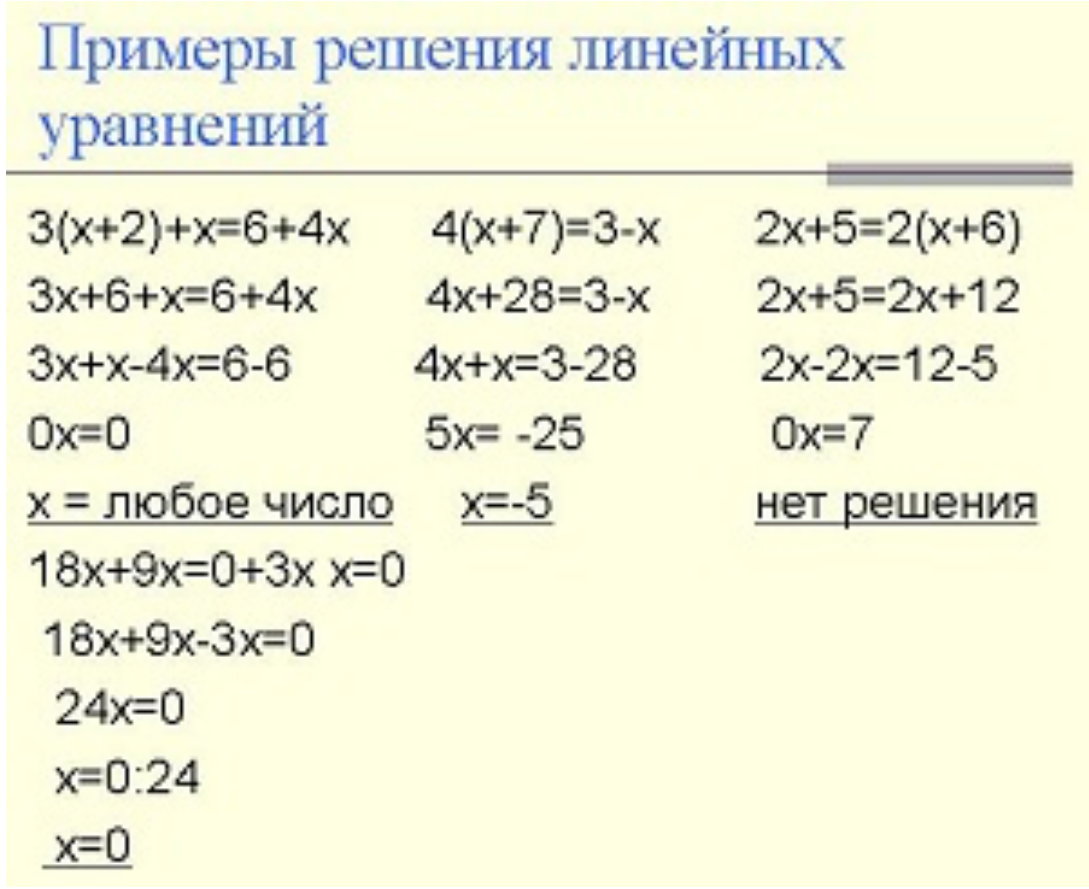
Вариант №1. КОМПАНИЯ С ИСТОРИЕЙ

Дано:

- Ответственный за ИБ
- Антивирус
- МСЭ периметра

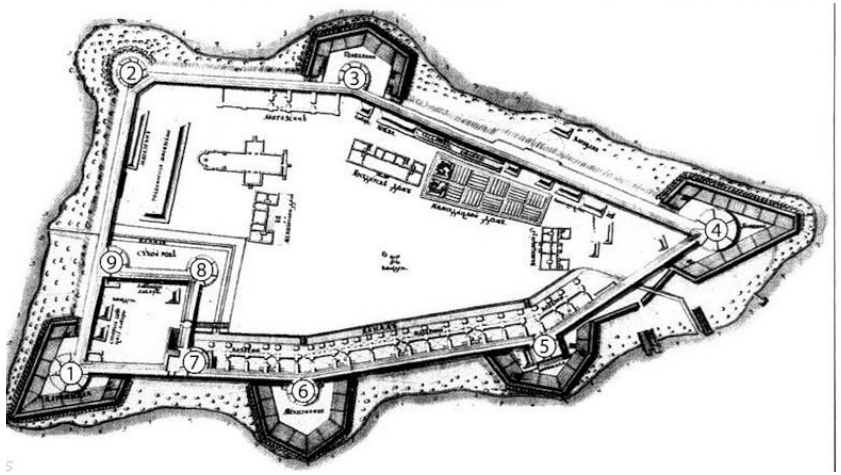
Что-то одно из:

- сканер уязвимостей инфраструктуры
- VPN для пользователей
- DLP-система



Раздел 1. Как обычно строится киберзащита в компании?

№1 Компания решает строить собственную кибербезопасность



Ответственный за ИБ —> Директор по ИБ (aka CISO)

- Оценка текущей ситуации в ИБ
- Инвентаризация ИТ
- Планы развития компании
- Масштаб и этапность работ и инвестиций в кибербезопасность
- Стратегия ИБ
- План развития ИБ

- ЧТО, ГДЕ И КОГДА (+ кто и по какой цене) будет делать
- Срочные “косметические” изменения в текущий бюджет
- Найм персонала первой очереди
- Аудит и пен-тест (опытный директор также заказывает поиск и оценку признаков компрометации)
- Бюджет на следующий год

Раздел 1. Как обычно строится киберзащита в компании?

№1 Компания решает строить собственную кибербезопасность

Директор по ИБ / CISO

2-й год

- Укрепление периметра
- Организация мониторинга ИБ
- внедрение СЗИ и процессов ИБ первой очереди
- внесение точечных изменений в ИТ
- повторные пен-тесты

3-й год

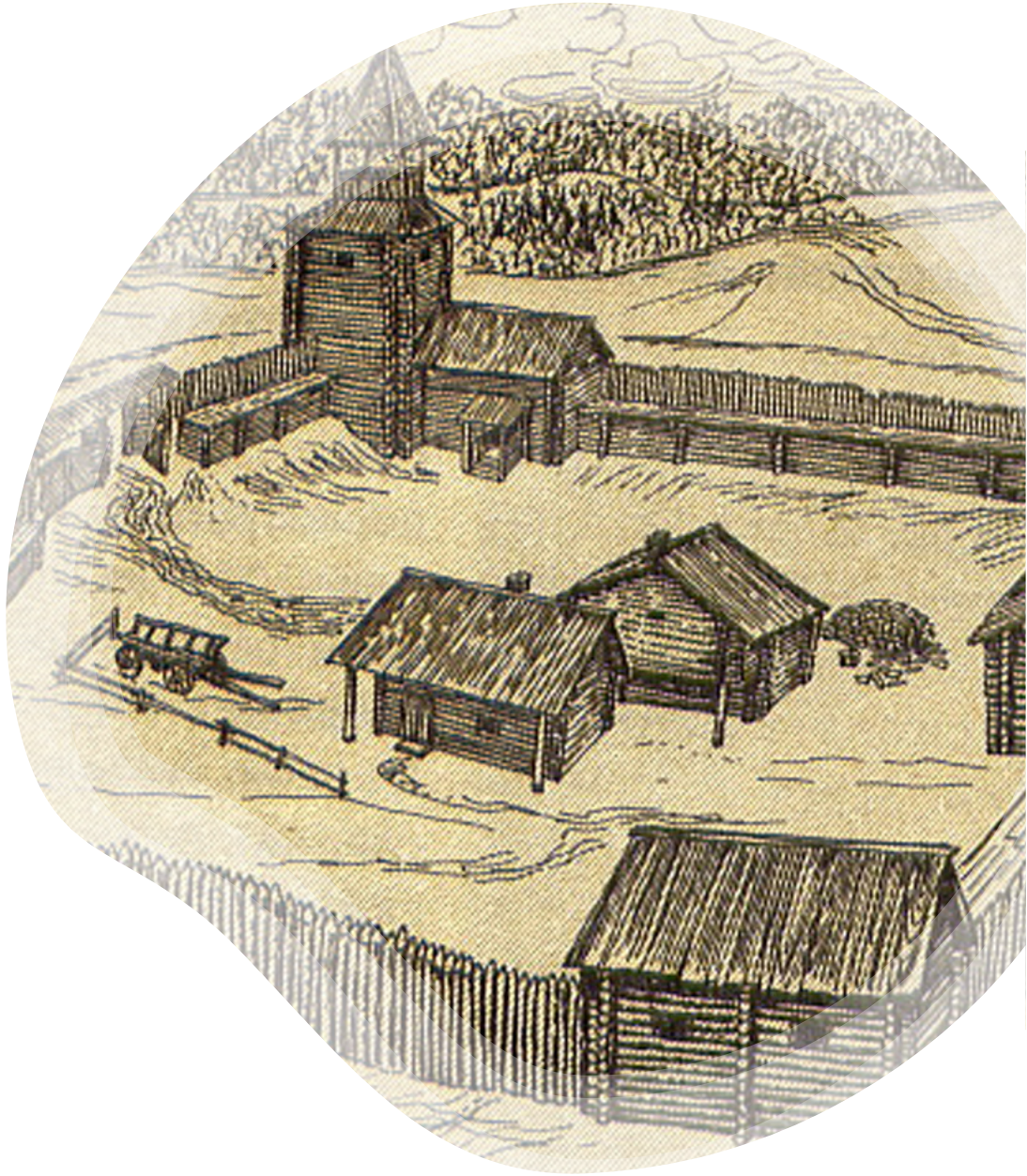
- внедрение СЗИ и выстраивание процессов второй очереди
- интеграция СЗИ в ИТ
- проведение повторного комплексного аудита

Если получилось так - это уже очень хорошо. Если совсем не получилось - при повторном аудите происходит смена директора по ИБ и цикл повторяется

РАЗДЕЛ 1. КАК ОБЫЧНО СТРОИТСЯ КИБЕРЗАЩИТА В КОМПАНИИ?

Вариант №2. СТАРТАП

- Информационная безопасность – пассивна
- Изменения в ИБ - по факту инцидентов («латаем дыры»)
- Минимальное влияние на TTM и бюджет компании
- Уровень кибербезопасности не меняется во времени
- Риски ИБ растут вместе с финансовыми показателями, узнаваемостью продуктов и сервисов
- С ростом компании приходит осознание необходимости инвестиций в кибербезопасность и ….
- … компания - стартап повторяет путь компании с историей по варианту № 1



Вывод №1

- Кибербезопасность:
  - долго (минимум 3 года),
  - дорого,
  - зависит от человеческого фактора,
  - оценивается периодически (хорошо если раз в год-два)
- Цена ошибки при планировании и реализации стратегии ИБ высока, чтобы минимизировать ошибки можно:
  - привлечь консультантов при разработке стратегии ИБ
  - чаще проводить оценку и применять корректирующие воздействия

Раздел 2. «Сделал раз - сделаешь и сто раз», но есть нюанс...

- Повторить 100-500 - другая задача, нужен иной подход
- Треугольник “быстро-дешево-хорошо”
- Регуляторы - исходно та же задача и те же трудности

Группа компаний - это возможности:

- доверие
- общие цели
- общее управление (акционеры)
- ресурсы (человеческие, финансовые)
- совместные закупки
- ….

Общие принципы безопасности группы компаний

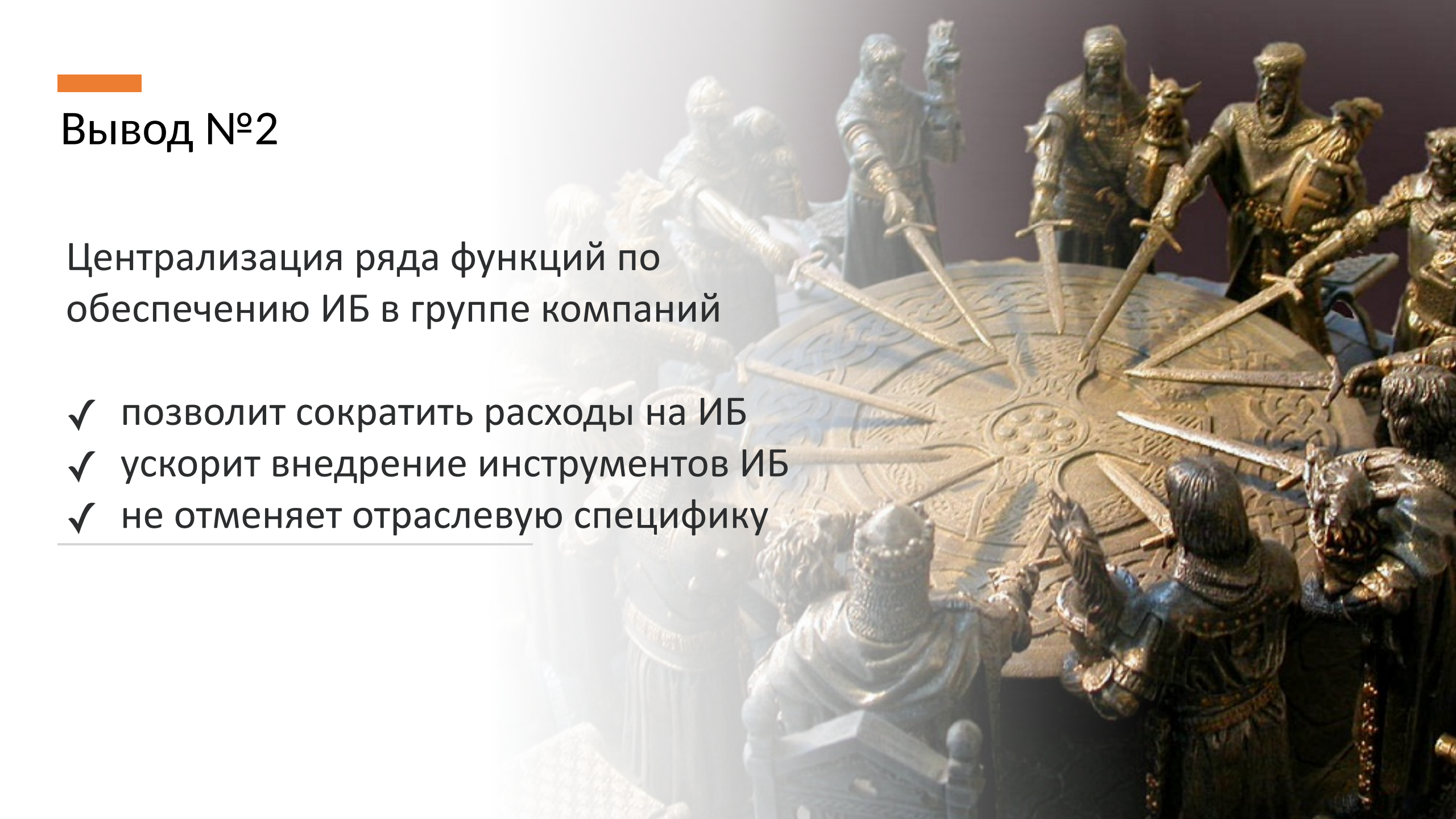
- Найти общее во всех компаниях группы и сделать типовые/ централизованные решения по защите
- Типизировать некоторые процессы и документы
- Найти различное и уникальное (или сложноповторяемое)
- Обеспечить выделение ресурсов на киберзащиту уникального в каждой компании в отдельности:

  - конфиденциальная информация, коммерческая тайна, персональные данные - DLP, DAG, …
  - локальные СЗИ, не допускающие простоя в доступности и в управлении - МСЭ, IDS, VPN, AV, …
  - микроменеджмент - IAM, MDM & EDM, …
  - бизнес-процессы (архитектура ИБ сервисов компании) и управление рисками ИБ …
  - требования отраслевого регулятора
  - …

Вывод №2

Централизация ряда функций по обеспечению ИБ в группе компаний

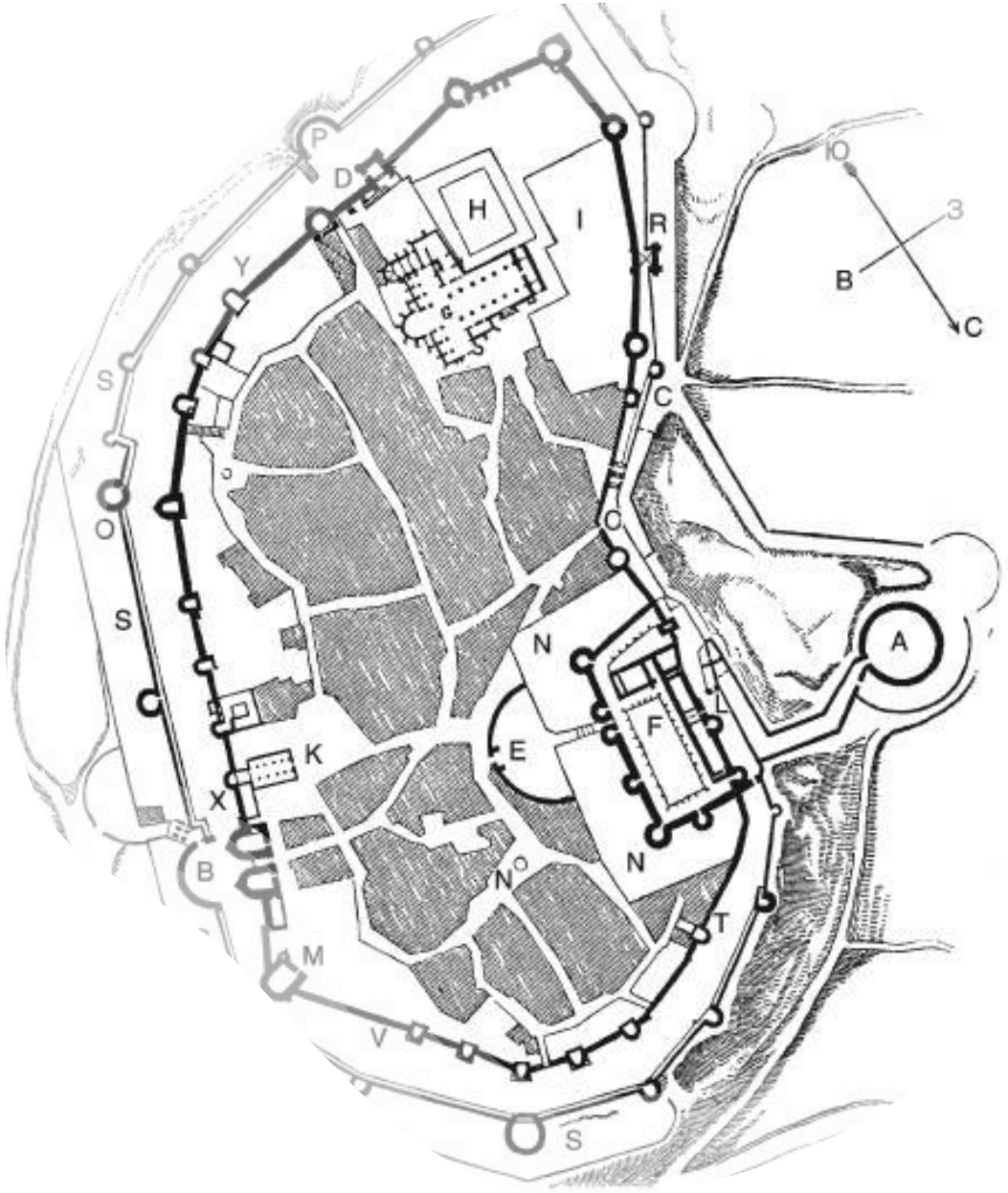
- ✓ позволит сократить расходы на ИБ
- ✓ ускорит внедрение инструментов ИБ
- ✓ не отменяет отраслевую специфику



Раздел 3. Как оценить киберустойчивость компаний группы?

Подходы

- Используем рекомендации регуляторов и свой опыт
- Применяем различные методы оценки
- Централизованные и тиражируемые решения – на основе собственного опыта и экспертизы
- Разработка критериев оценки эффективности уникальных (нетиражируемых) решений



Раздел 3. Как оценить киберустойчивость компаний группы?

Учесть в критериях оценки

- Централизованно выбраны и внедрены необходимые общие СЗИ
- Специфические СЗИ, учитывающие уникальность компании
- СЗИ покрывают всю инфраструктуру, не простаивают, настроены корректно и эффективно
- Есть интеграции между СЗИ и ИТ системами
- Процессы ИБ внедрены, описаны и выполняются
- Формируются артефакты выполнения процессов
- Достаточное количество персонала

Методология: корпоративный стандарт для компаний группы, предусматривающий несколько уровней (наборов) требований, исходя из ряда финансовых и иных параметров компаний

Раздел 3. Как оценить киберустойчивость компаний группы?

Методы

- Корпоративный стандарт ИБ - выездные и дистанционные мероприятия по оценке соответствия
- Оценка эффективности настройки локальных СЗИ
- Регулярный сбор метрик, подтверждающих выполнение процессов
  Источники метрик - сами компании + внешние источники
- Пен-тест - результаты пен-теста могут скорректировать оценку эффективности процессов кибербезопасности и СЗИ

Раздел 3. Как оценить киберустойчивость компаний группы?

Головная компания определяет уровни оценки и методику их расчета

- **5 балльная шкала:**

2 балла – к устойчивость ко взлому случайно или за компанию для “начинающего” хакера

3 балла – устойчивость ко взлому профессиональными пентестерами с ограниченным ресурсом

Требования к целевой оценке каждой конкретной компаний группы формируются исходя из:

- финансово-экономических параметров
- степени сетевой и иной интеграции
- состава информационного обмена
- совместного использования ресурсов и сервисов, бренда

Определение приоритетных требований ИБ - с учетом модели угроз/перечня недопустимых событий для конкретной компании

Организация выделения ресурсов на повышение кибербезопасности

Внедрение инструментов корпоративного контроля за достижением целевых уровней кибербезопасности

Вывод №3

Оценка кибербезопасности:

- проводится по заказу в интересах владельца бизнеса
- ступенчатая или градиентная (можно использовать в риск-модели и обеспечивать необходимые и достаточные инвестиции в кибербезопасность с учетом модели рисков бизнеса компании)
- должна быть понятна для всех, в первую очередь - для бизнеса

Оценка кибербезопасности – важный параметр при оценке риска бизнеса

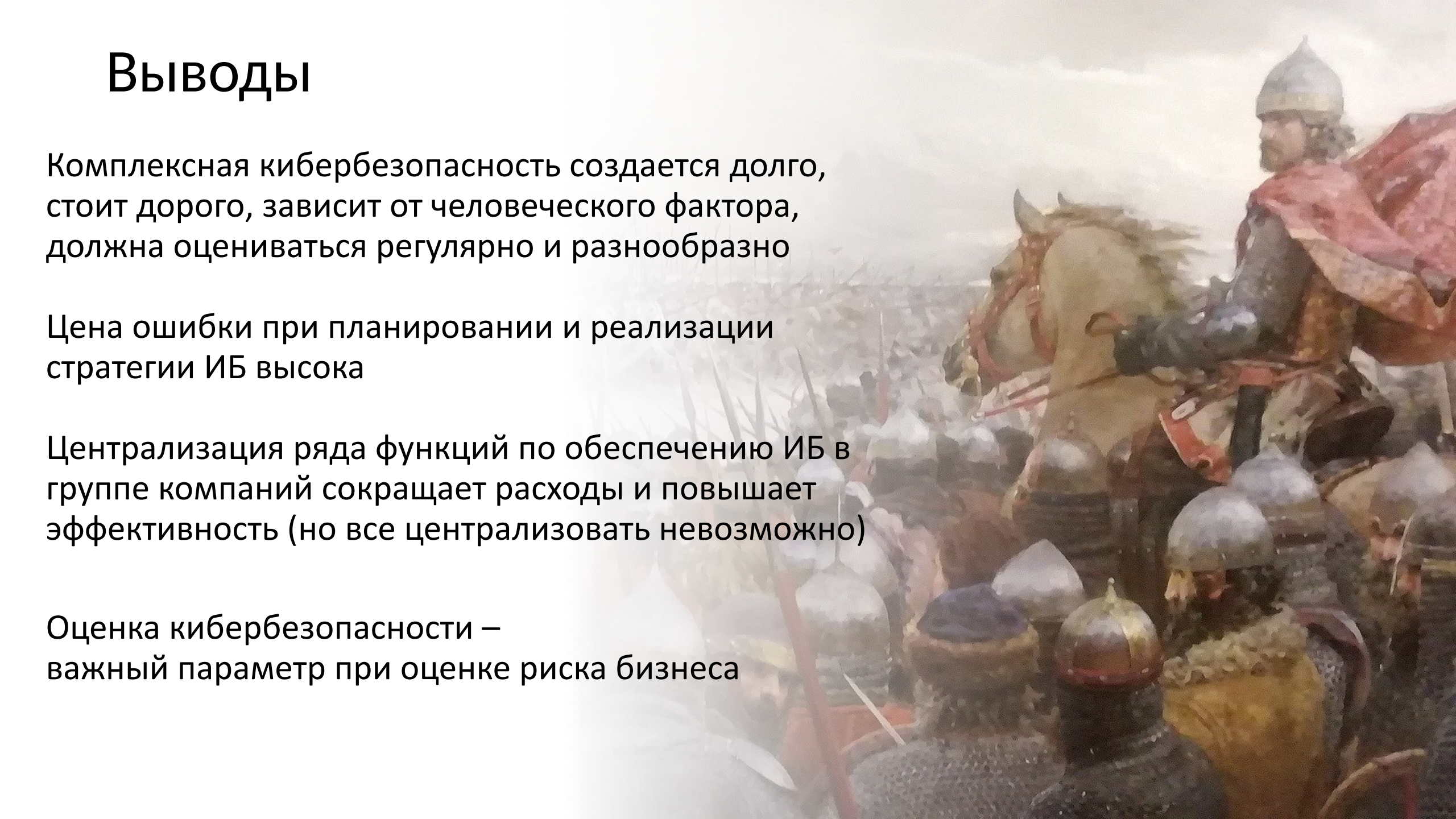
Выводы

Комплексная кибербезопасность создается долго, стоит дорого, зависит от человеческого фактора, должна оцениваться регулярно и разнообразно

Цена ошибки при планировании и реализации стратегии ИБ высока

Централизация ряда функций по обеспечению ИБ в группе компаний сокращает расходы и повышает эффективность (но все централизовать невозможно)

Оценка кибербезопасности –
важный параметр при оценке риска бизнеса



Константин Титков

Центр информационной безопасности дочерних и зависимых обществ

Банк ГПБ (АО)

tg: @ktitkov