Построение систем управления безопасностью и готовность к рискам
в 2 частях

Вячеслав Яшкин
Наталья Раевская

Часть 1
Глобальные изменения XXI века в области безопасности и рисков

Только за первые 23 года нового тысячелетия мир столкнулся с множеством кризисов

Сценарии:

Финансовый

Мировой финансовый кризис 2008-2009
Обвал цен на нефть 2014/2016/2020

Эпидемия

Пандемия 2020

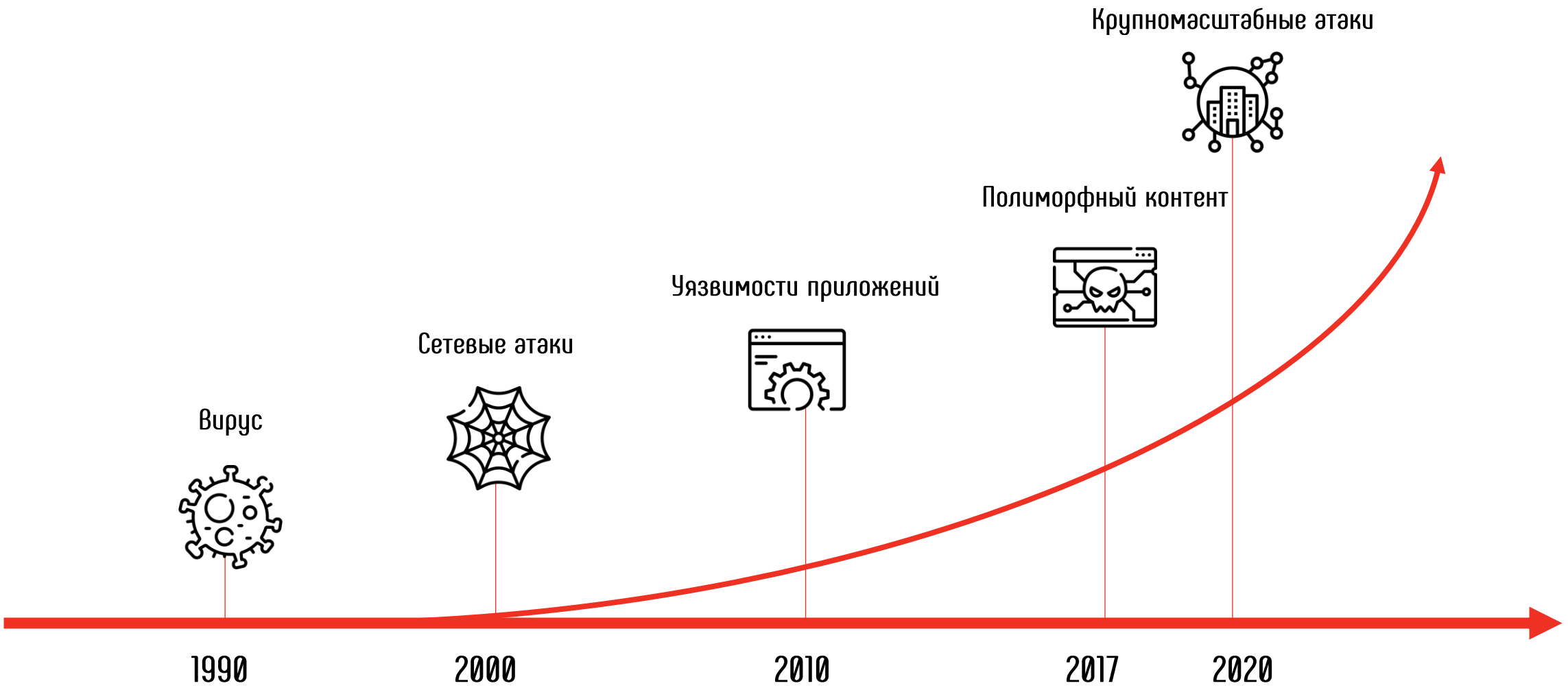
Военный

Санкции против России 2014/2018/2022

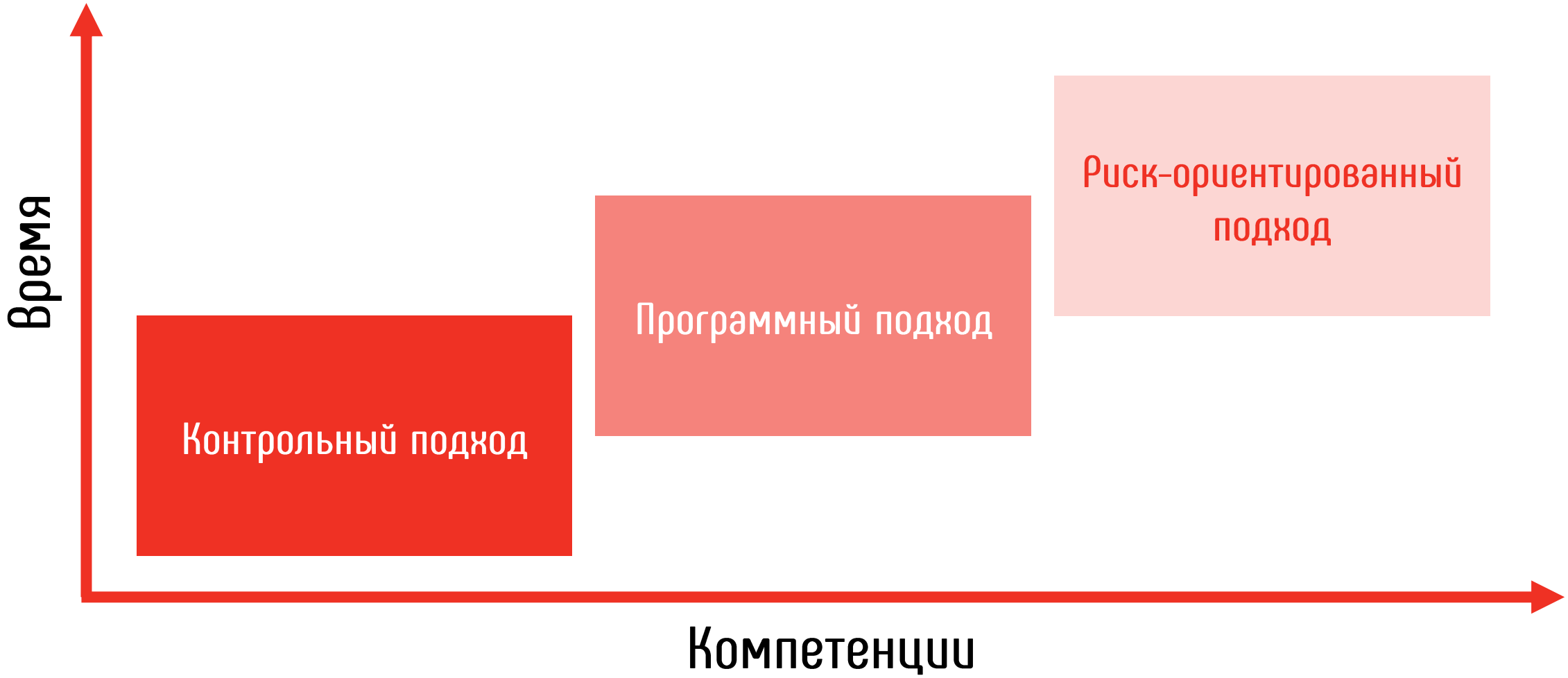
Проактивность и реактивность дают возможность обеспечить устойчивость кибербезопасности

- **Сочетание** в работе проактивного подхода **(определение того, что важно)** и реактивного подхода **(быстрое реагирование на ситуацию, определение решения проблемы)** - помогает **быстро справиться** и **отреагировать на ситуацию** и обеспечивает **устойчивое функционирование** бизнеса вопреки всем внешним неблагоприятным факторам.
- Точь-в-точь как **вождение мотоцикла.**

Вместе с развитием цифрового мира развивается киберпреступность



Эволюционирует также и кибербезопасность



На уровне организаций внедряется риск-культура...

Контекст

На основе анализа изменений в контексте необходимо идентифицировать риски и возможности

Функционирование

Запланированные меры управления рисками и возможностями необходимо внедрить

Лидерство

Высшее руководство должно поддерживать риск-ориентированное мышление

Оценка выполнения

Необходимо проводить оценку результативности внедренных мер

Планирование

Меры управления рисками и возможностями необходимо запланировать

Улучшения

Процессы управления рисками должны улучшаться

... и процессы кризисного реагирования

Действия по идентификации риска

Информирование ТОП-менеджмента

Актуализация мер
Кризисная отчетность

Утверждение комплекса мер и стратегии коммуникаций

Реализация антикризисных мер

Мониторинг и анализ ситуации
Контроль реализации мер

идентификация → информирование → анализ → принятие решений → реализация → мониторинг и контроль

Выявляются ключевые угрозы и риски нового времени

2 ♣

DDoS

2 ♥

Сканирование

внешнего периметра

3 ♠

СМС

Эксплуатация смс-информирования для увеличения затрат и dos

3 ♦

Украденные карты

Снятие денег на спец. терминалах не требующих пин-кода

6 ♥

Фишинг, VPN, обзвоны

как способ проникновения для шифрования данных или отключения сервисов

7 ♥

Цифровые сертификаты сервисов

8 ♠

Отсутствие

запасных частей, инструментов и принадлежностей

9 ♠

Лицензии на программное обеспечение

10 ♣

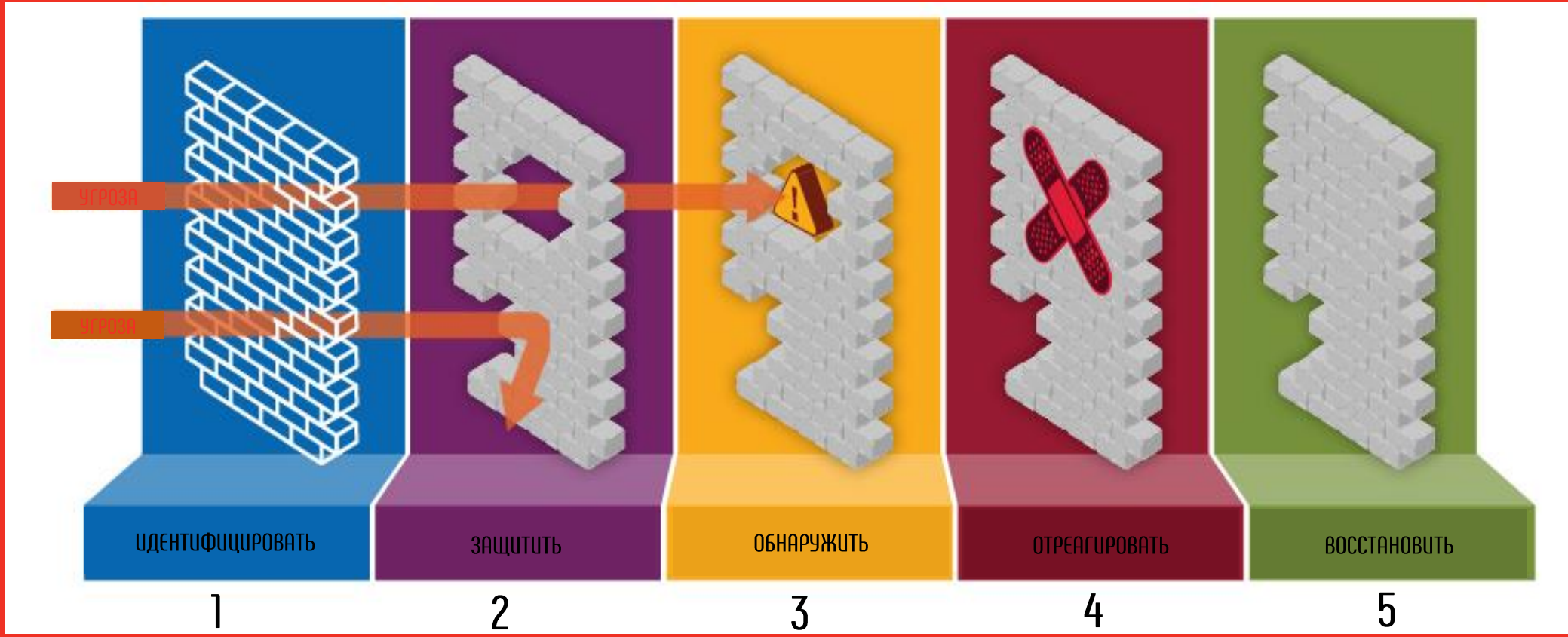
Эксплуатация известных уязвимостей

до февраля 2022 года

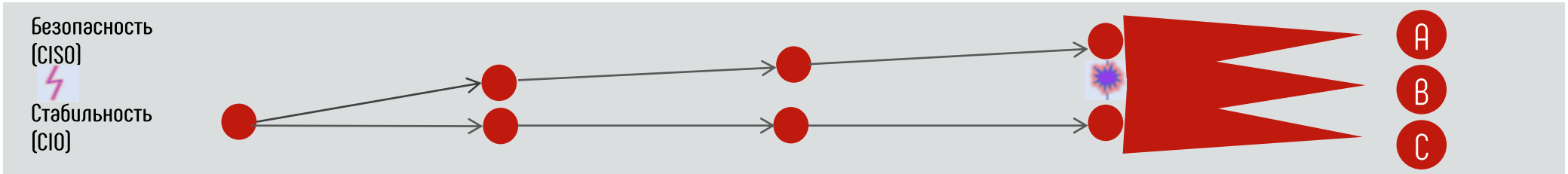
И разрабатываются пути их митигации

Часть 2
Развитие устойчивой безопасности и кибербезопасности организаций

Барьерная модель NIST



Развитие модели NIST на практике

Эра	1980-ые Идентифици-ровать	1990-ые Защитить	2000-е Обнаружить	2010-е Реагировать	2020-е Восстановить
Основные проблемы	Что мы купили и как это поддерживает бизнес?	Вирусы, Атаки на сервер, Небезопасные Конфигурации	Много журналов и предупреждений, атаки на стороне клиента	Проактивный подход, Бушующие Пожары, Слишком Много Привилегий	Вирус вымогатель, MBR Wiper, DDos, Firmware Bricking
Решения	Управление активами, инструменты управления системами	Антивирус, Брандмауэры, Безопасные конфигурации	IDS, SIEM	Реагирование на инциденты и инструменты IR (EDR, SOAR)	DIE (Распределенная, неизменная, эфемерная)
UT/Требования безопасности					
Состав и направленность группы безопасности	Нет	Клуб по интересам, управление уязвимостями	SOC, управление угрозами	Специализированное подразделение/управление рисками	Выбери свой путь

2020-е годы: Эпоха восстановления (устойчивости)

Какие атаки в 2020-х годах могут поставить под сомнение нашу способность
ВОССТАНАВЛИВАТЬСЯ
или причинят **необратимый вред**?

Конфиденциальность

Wikileaks/Doxxing

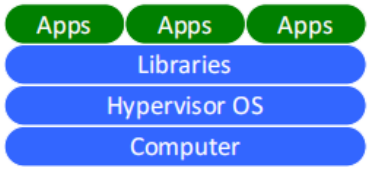
Целостность

Вирус
вымогатель/фейки

Доступность

PDos, MBR Wiper,
Bricking Firmware

DIE (Distributed Immutable Ephemeral)



Распределенный

Неизменяемый

Эфемерный

DDos

Устойчивость

Лучшее решение против распределенной атаки - распределенная служба

Изменения легче обнаружить и отменить

Несанкционированные изменения отмечаются и могут быть изменены

Приближает стоимость активов к 0

Затрудняет взлом злоумышленнику и сохраняет активы

Доступность

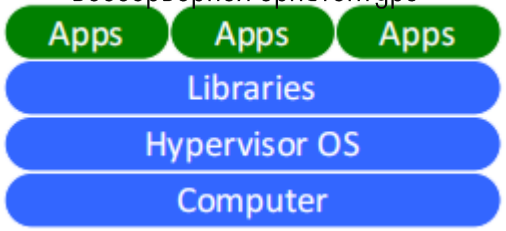
Целостность

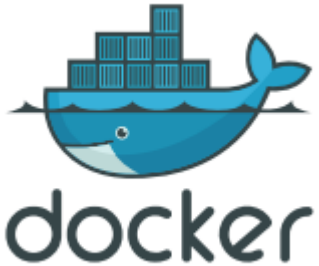
Конфиденциальность

2020-е годы: Эпоха восстановления (устойчивости)

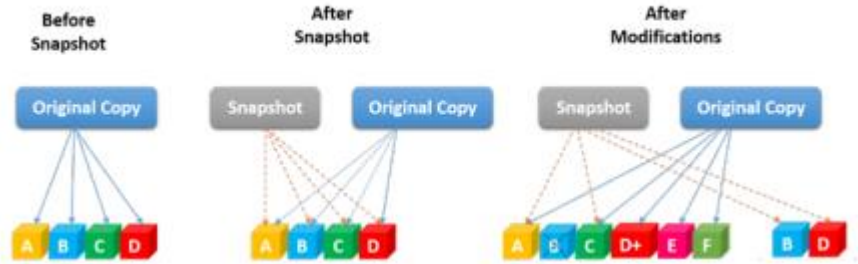
Какие решения помогают
нам ВОССТАНАВЛИВАТЬСЯ или быть УСТОЙЧИВЫМИ?

Бессерверная архитектура

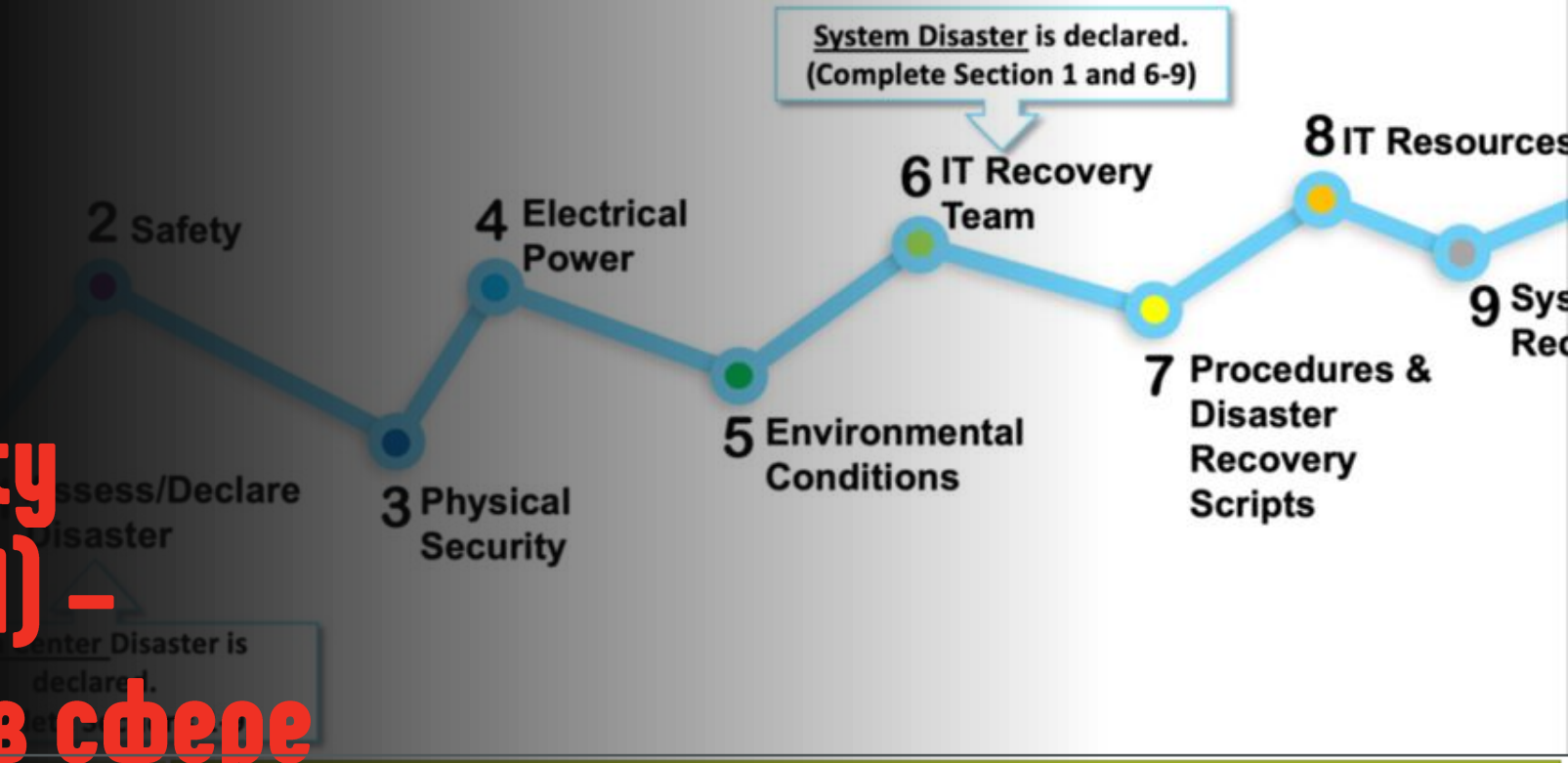


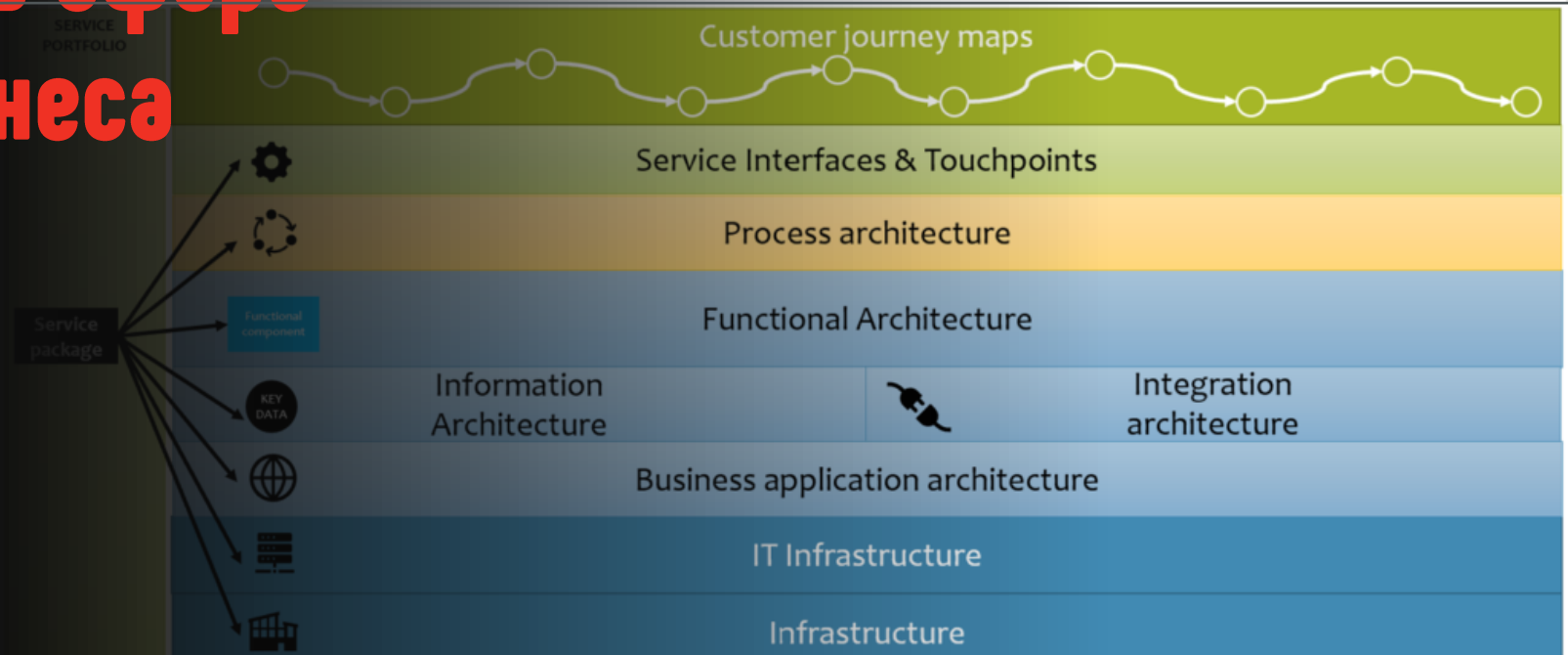


Сеть доставки контента



Business Continuity Management (BCM) – ответ на вызовы в сфере устойчивости бизнеса





Каждая компания в зависимости от задач и потребностей выбирает свой путь развития

Путь A

Хрупкость

C.I.A.

Вред смягчается с помощью обходных путей, которые создают нестабильность

Путь B

Устойчивость

D.I.E.

Вред приводит к разрушению, но без изменения конфигурации

Путь C

D.I.E. + созидательные разрушения

Вред активирует изменения, которые вымещают CIA и делают систему еще более похожей на DIE

Приятно познакомиться