Безопасность 4.0

самодиагностика бизнес-процессов как инструмент безопасности

Индустрия 4.0

Цифровые продукты

Цифровые процессы создания продуктов

Высокий темп развития технологий

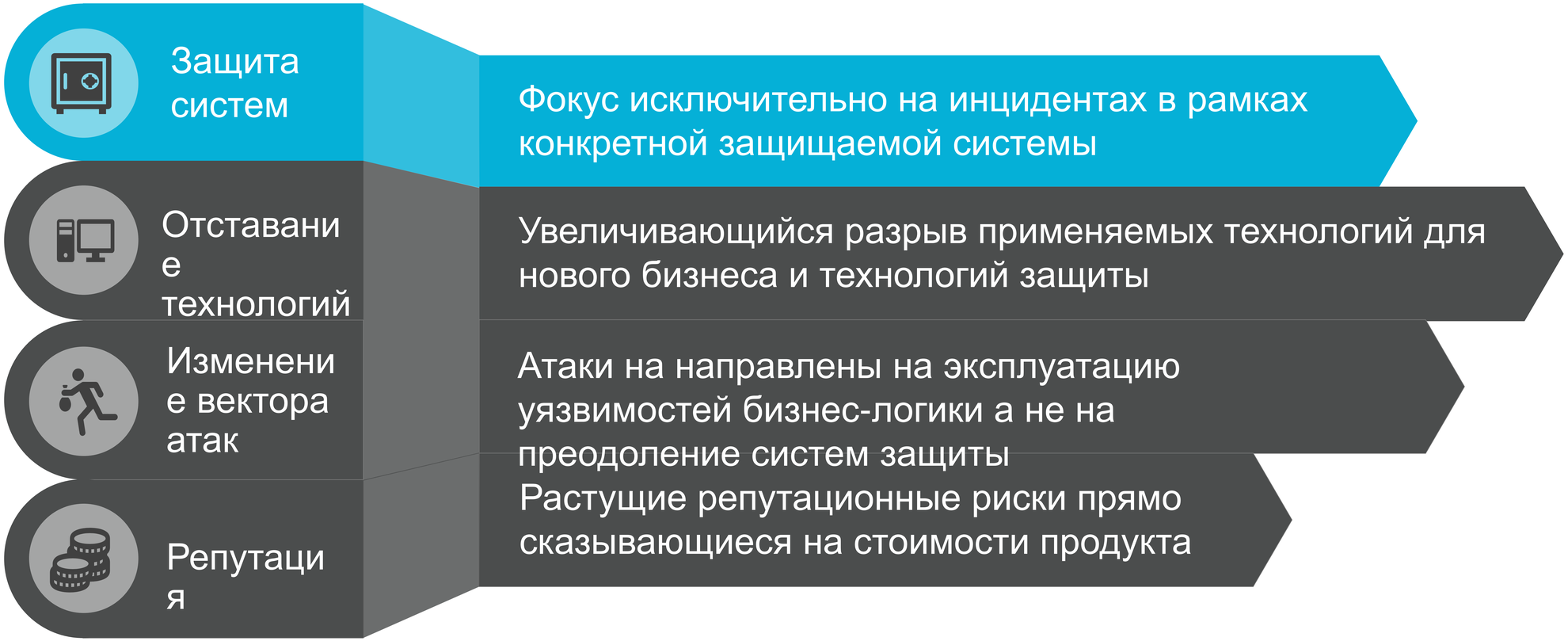
Безопасность как свойство продукта\процесса

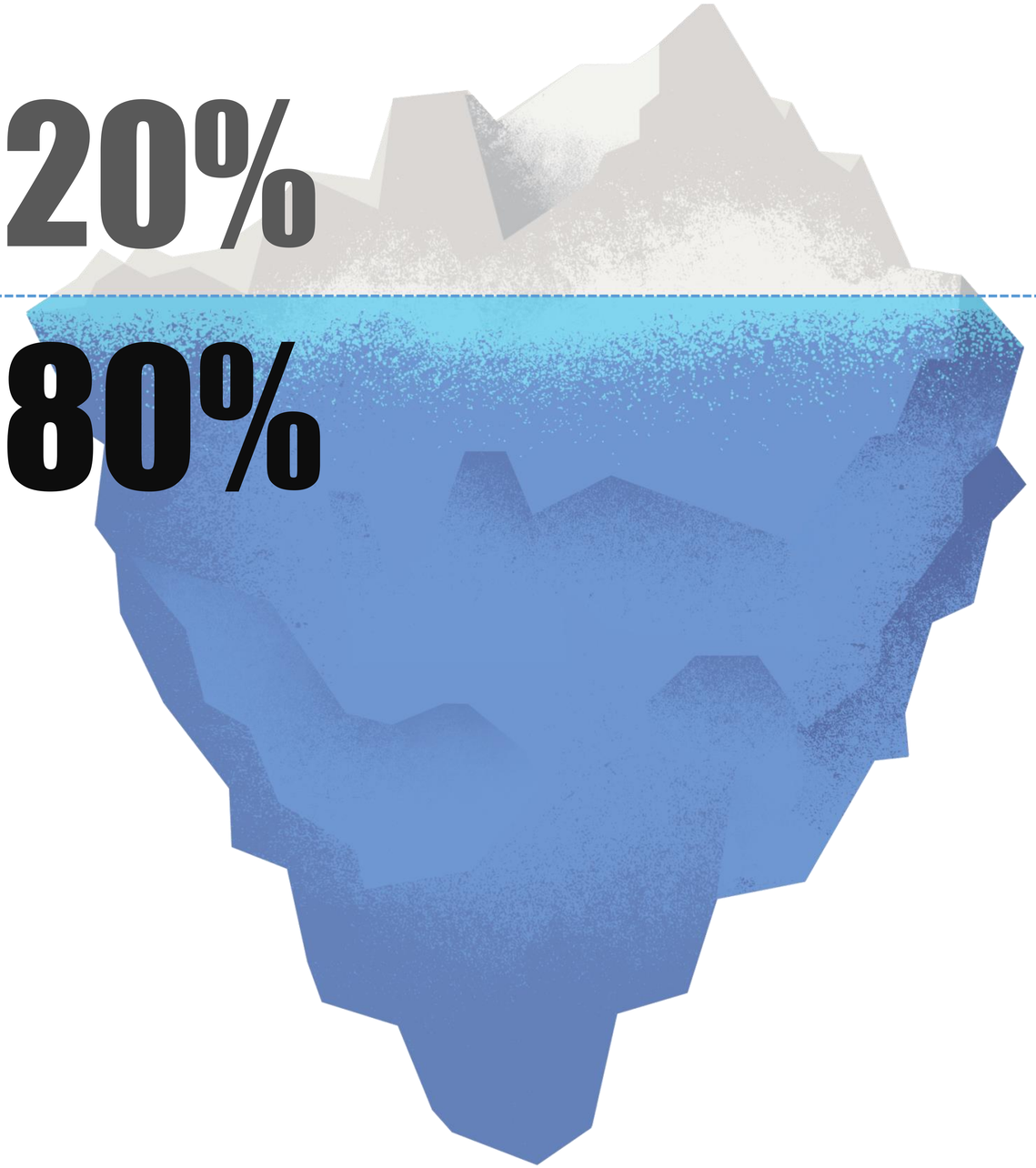
«прогнозируемое событие, массовое внедрение киберфизических систем в производство (индустрия 4.0), обслуживание человеческих потребностей, включая быт, труд и досуг. Изменения охватят самые разные стороны жизни: рынок труда, жизненную среду, политические системы, технологический уклад, человеческую идентичность и другие. Вызываемая к жизни экономической целесообразностью и привлекательностью повышения качества жизни, четвёртая промышленная революция несёт в себе риски повышения нестабильности и возможного коллапса мировой системы, в связи с чем её наступление воспринимается как вызов, на который человечеству предстоит ответить» -

Wikipedia

Проблематика

традиционных систем обеспечения безопасности





ИНЦИДЕНТЫ БЕЗОПАСНОСТИ

ИНЦИДЕНТЫ БИЗНЕС-ПРОЦЕССОВ

Ущерб являющийся следствием инцидентов в большей своей части лежит именно в области инцидентов внутри бизнес-процессов. По отдельности каждый из инцидентов подобного рода выглядит незначительным, и скорее воспринимается как ошибка чем злонамеренное действие. Однако в общей своей массе, совокупный ущерб от подобного рода инцидентов – значителен. Что важно! Это не отложенные риски с прогнозируемой вероятностью наступления. Ущерб от инцидентов внутри бизнес-процессов, это фактически ежедневные потери имеющие прямую корреляцию с операционными показателями компании и качеством выпускаемого продукта.

Соотношение потерь от инцидентов в корпоративной среде

Безопасность 4.0

в контексте изменяющейся экономики и развития новых технологий возникает необходимость трансформации подхода построения систем безопасности

01

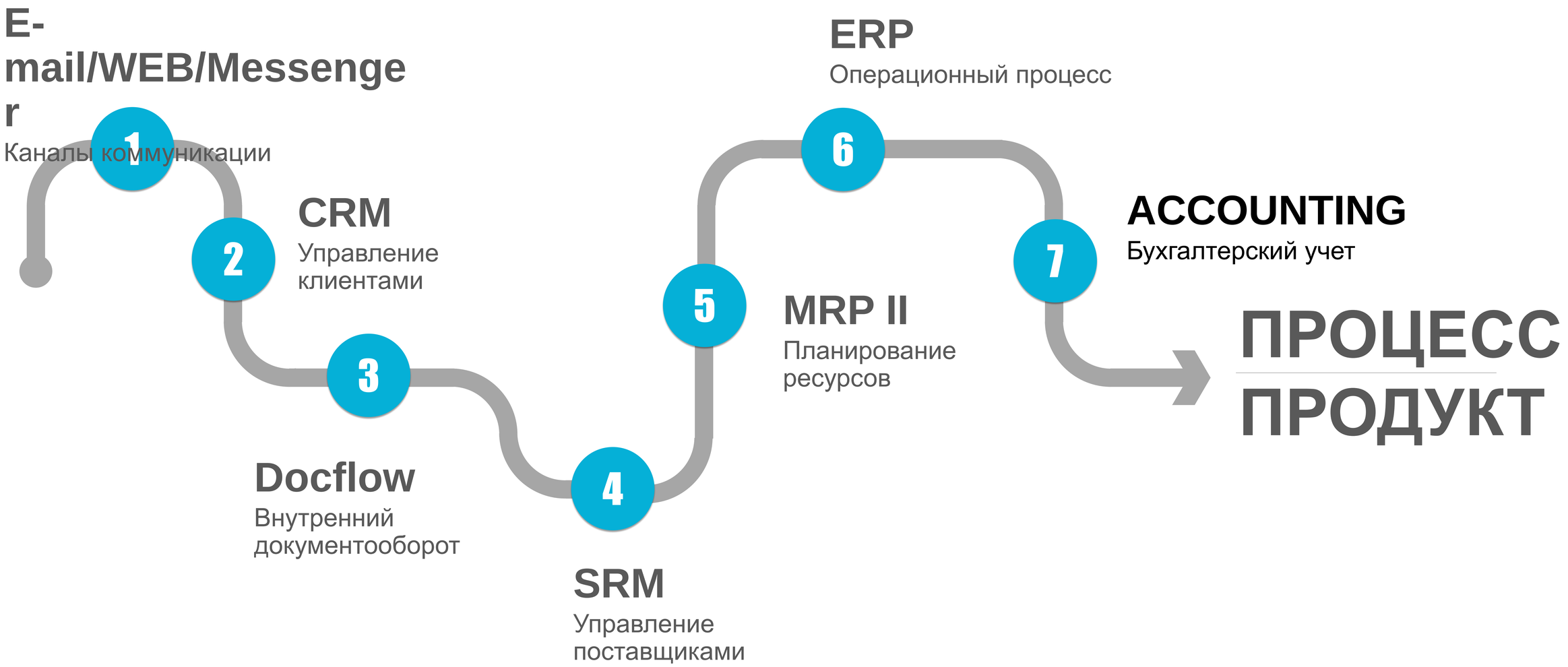
Комплексность подхода

Необходимо защищать именно цифровой продукт или бизнес-процесс, а не отдельные

02

Предиктивность

Системы защиты должны выявлять инцидент на этапе его подготовки не допуская реализации действий способных



Все существующие бизнес-процессы или создаваемые цифровые продукты могут быть представлены как совокупность артефактов (документов) или событий возникающих в различного рода информационных системах и сервисах. Для каждого процесса характерна корреляция возникающих событий, логика их возникновения, временные интервалы и т.д.

технологии

Big Data

как инструмент объединения разнородных данных из множества различных источников

Признаки инцидента

Все существующие системы безопасности или противодействия мошенничеству базируются на принципе описания паттерна негативного действия и последующем его выявлении.
Однако данная позиция является всегда отстающей и эффективна лишь когда мы снимаем пики высоких рисков. Когда мы говорим о бизнес-инцидентах, то создание подобных моделей нарушений экономически не целесообразно из-за высоких затрат по отношении к ущербу от каждой конкретной схемы инцидента.

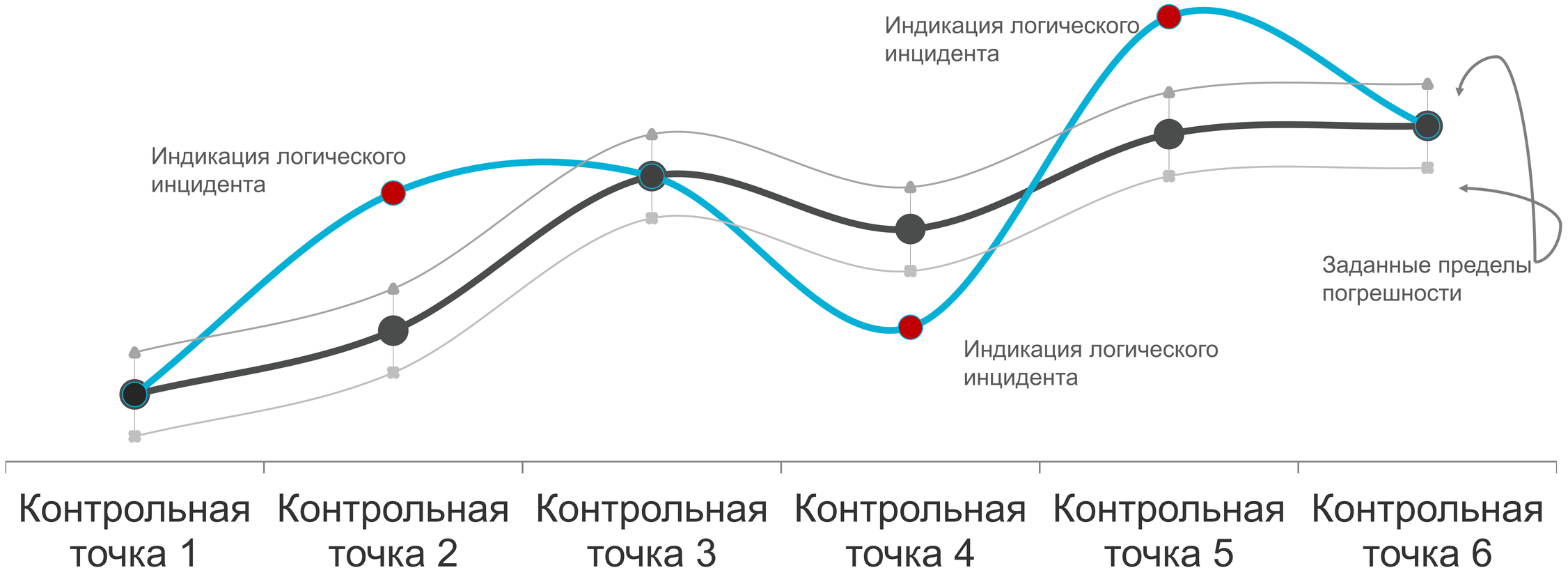
90%
80%
70%
60%
50%

Вероятность инцидента

Совокупность признаков определяющих инцидент

«- Мы проверяли. - Сказав, Деккер понял, как глупо это прозвучало. Да, они анализировали атмосферу, но как они могли обнаружить что-то, чего никогда не встречали? Опыт человеческий ограничен. Человек бережет себя от опасностей известных или воображаемых, но не может предвидеть непредвиденное»

Клиффорд Саймак. Ветер чужого мира



01

Даже если нет явной формализации процесса, его описания в какой либо из нотаций, то процесс все равно существует. На уровне инструкций или регламентов, или замысла владельца процесса. А значит мы его можем видеть на уровне событий информационных систем

02

Большую часть времени процесс происходит одинаково. В рамках единой логики. А значит все выявляемые отклонения будут являться инцидентами, влекущие за собой изменение качества этого процесса

Паттерны нормы

Выстраивание контрольной среды не требует создания моделей нарушения. Поскольку бизнес-инцидентом является любое отклонение от заданной и утверждённой модели процесса, то мы можем выявлять их сравнивая существующую логику процесса с описанной моделью. Данные модели как правило уже формализованы в той или иной степени когда мы говорим о объектах (как о базовой форме) или процессах, при этом так же справедливо будет говорить и о том, что они в смою очередь создают и третий уровень – паттерны пользователей, которые так же поддаются нормализации.

Object BA

Process BA

User BA

Machine Learning

Для оптимизации процесса разбора инцидентов могут быть использованы инструменты машинного обучения. Используемые как «очистки» инцидентов и обучающиеся на признаках false positive

Так же возможно построение прогнозных моделей в рамках выявление девиаций на ранних стадиях, когда момент наступления ущерба еще не известен.

Формирование «иммунитета»

01 Определение «цифрового» отпечатка существующего бизнес-процесса

02 Выявление контрольных точек. Изменение которых влияет на качество продукта\процесса

03 «Нормализация» процесса через постоянное сличение паттерна с событиями в реальном времени.

04 Запуск автоматизированной контрольной среды на существующем бизнес-процессе

dmitriy.manannikov

dmitriy.manannikov
@gmail.com

Спасибо за внимание