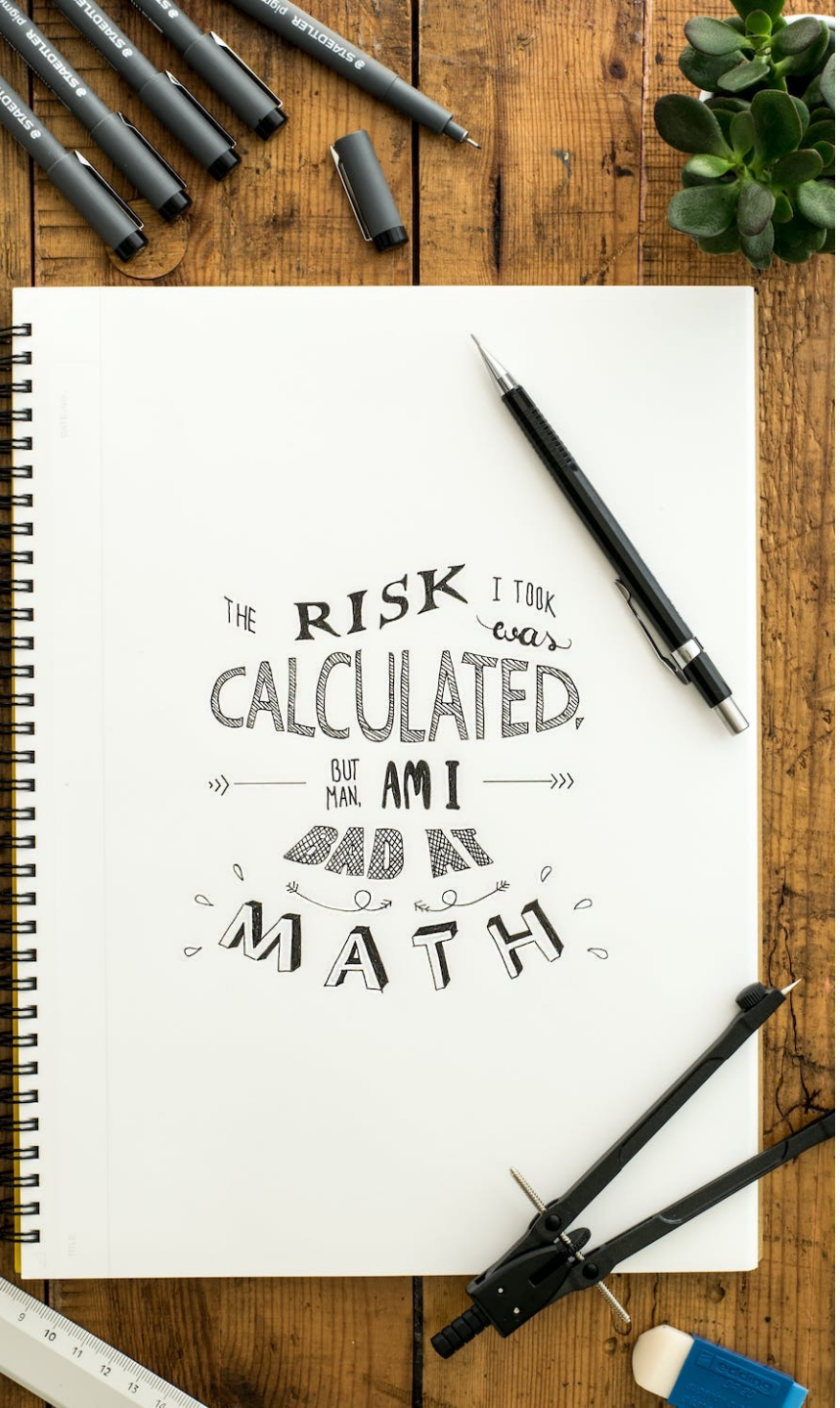
Алексей Лукацкий
Бизнес-консультант по безопасности

Риски ИБ

Методики оценки рисков ИБ, роль рисков ИБ в общей карте рисков организации, финансовая оценка рисков

Who am I?

- Бизнес-консультант по безопасности в Positive Technologies
- Автор проекта «Бизнес без опасности»
- Автор 5 книг и 30+ курсов по ИБ
- Программист, админ, аудитор, маркетолог, продавец, консультант, преподаватель, писатель, популяризатор
- 30+ лет в кибербезе



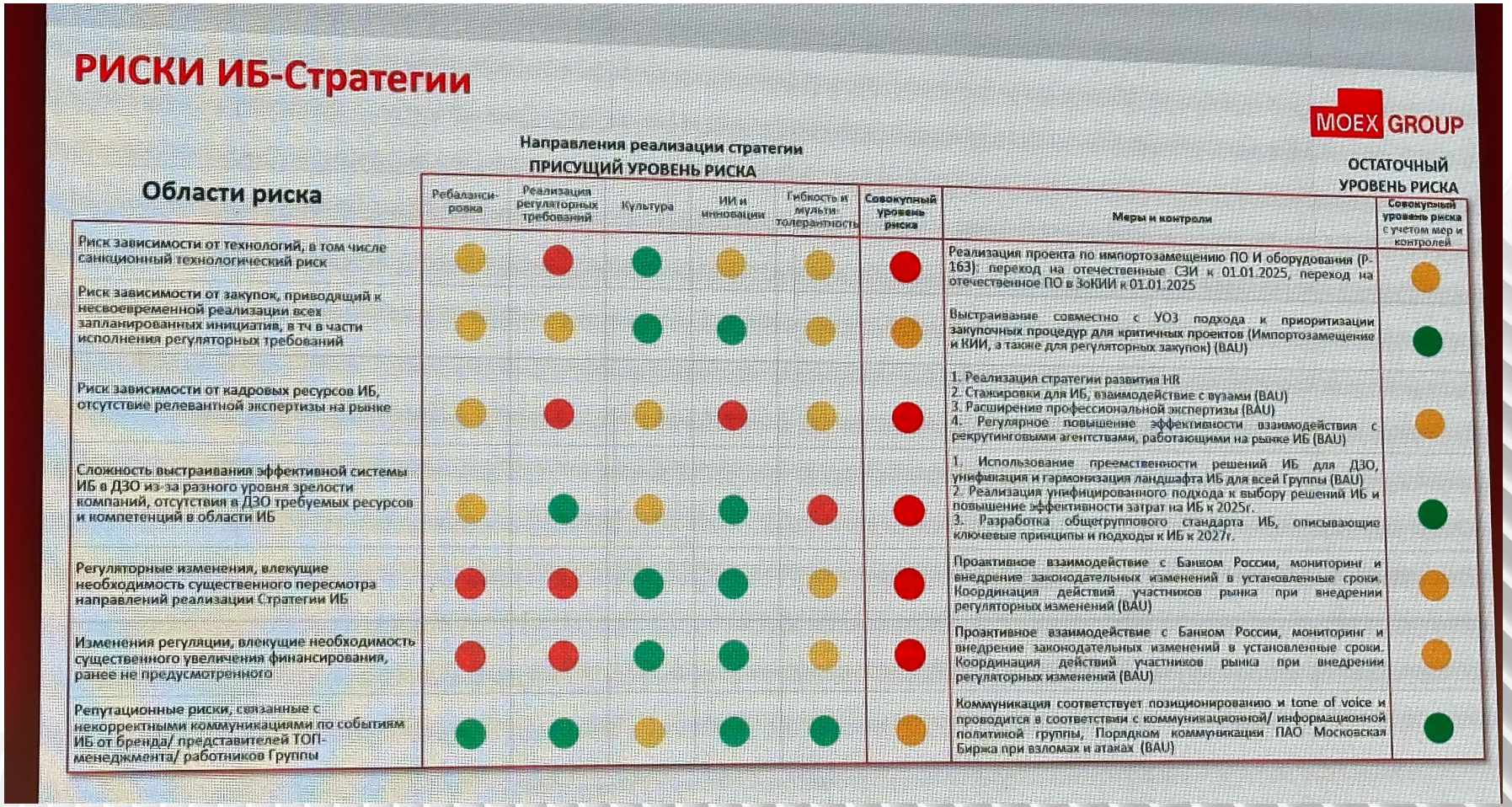
Риск = вероятность * ущерб

Как обычно измеряют риски/угрозы ИБ?

	Почти нереально	Маловероятно	Возможно	Вероятно	Очень вероятно
Катастрофически	6	7	8	9	10
Значительно	5	6	7	8	9
Умеренно	4	5	6	7	8
Незначительно	3	4	5	6	7
Несущественно	2	3	4	5	6
	Принять (уровень = 2,3)	Мониторить (уровень = 4,5)	Управлять (уровень = 6)	Избежать / разрулить (уровень = 7)	Немедленно избежать / разрулить (уровень = 8, 9, 10)

Оценка может быть и трех- и более факторной

Пример ММВБ



РИСКИ ИБ-Стратегии

MOEX GROUP

Области риска	Направления реализации стратегии: ПРИСУЩИЙ УРОВЕНЬ РИСКА: Ребалансировка	Реализация регуляторных требований	Культура	ИИ и инновации	Гибкость и мультитолерантность	Совокупный уровень риска	Меры и контроли	ОСТАТОЧНЫЙ УРОВЕНЬ РИСКА: Совокупный уровень риска с учетом мер и контролей
Риск зависимости от технологий, в том числе санкционный технологический риск	🟡	🔴	🟢	🟡	🟡	🔴	Реализация проекта по импортозамещению ПО И оборудования (Р-163); переход на отечественные СЗИ к 01.01.2025, переход на отечественное ПО в ЗоКИИ к 01.01.2025	🟡
Риск зависимости от закупок, приводящий к несвоевременной реализации всех запланированных инициатив, в тч в части исполнения регуляторных требований	🟡	🟡	🟢	🟢	🟡	🟡	Выстраивание совместно с УОЗ подхода к приоритизации закупочных процедур для критичных проектов (Импортозамещение и КИИ, а также для регуляторных закупок) (BAU)	🟢
Риск зависимости от кадровых ресурсов ИБ, отсутствие релевантной экспертизы на рынке	🟡	🔴	🟡	🔴	🟡	🔴	1. Реализация стратегии развития HR 2. Стажировки для ИБ, взаимодействие с вузами (BAU) 3. Расширение профессиональной экспертизы (BAU) 4. Регулярное повышение эффективности взаимодействия с рекрутинговыми агентствами, работающими на рынке ИБ (BAU)	🟡
Сложность выстраивания эффективной системы ИБ в ДЗО из-за разного уровня зрелости компаний, отсутствия в ДЗО требуемых ресурсов и компетенций в области ИБ	🟡	🟢	🟡	🟢	🔴	🔴	1. Использование преемственности решений ИБ для ДЗО, унификация и гармонизация ландшафта ИБ для всей Группы (BAU) 2. Реализация унифицированного подхода к выбору решений ИБ и повышение эффективности затрат на ИБ к 2025г. 3. Разработка общегруппового стандарта ИБ, описывающие ключевые принципы и подходы к ИБ к 2027г.	🟢
Регуляторные изменения, влекущие необходимость существенного пересмотра направлений реализации Стратегии ИБ	🔴	🔴	🟢	🟢	🟡	🔴	Проактивное взаимодействие с Банком России, мониторинг и внедрение законодательных изменений в установленные сроки. Координация действий участников рынка при внедрении регуляторных изменений (BAU)	🟡
Изменения регуляции, влекущие необходимость существенного увеличения финансирования, ранее не предусмотренного	🔴	🔴	🟢	🟢	🟡	🔴	Проактивное взаимодействие с Банком России, мониторинг и внедрение законодательных изменений в установленные сроки. Координация действий участников рынка при внедрении регуляторных изменений (BAU)	🟡
Репутационные риски, связанные с некорректными коммуникациями по событиям ИБ от бренда/ представителей ТОП-менеджмента/ работников Группы	🟢	🟢	🟡	🟢	🟢	🟡	Коммуникация соответствует позиционированию и tone of voice и проводится в соответствии с коммуникационной/ информационной политикой группы, Порядком коммуникации ПАО Московская Биржа при взломах и атаках (BAU)	🟢

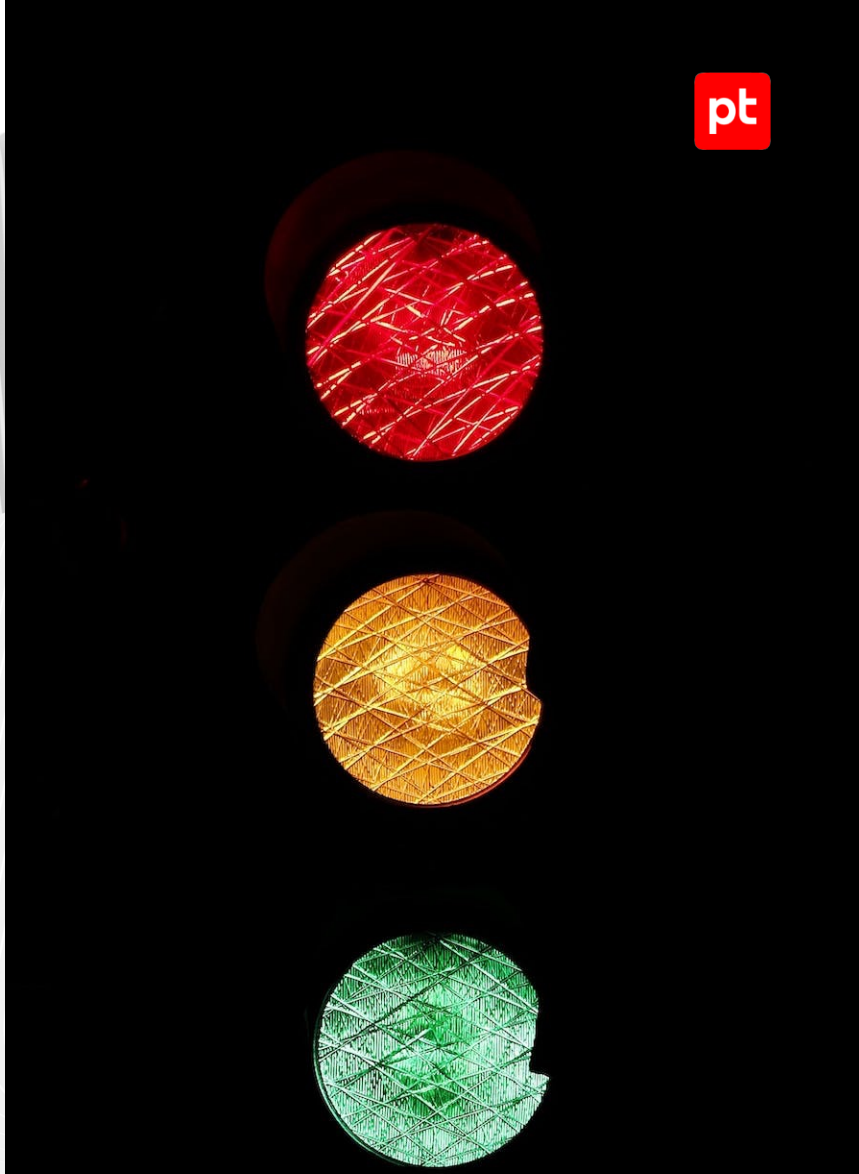
Шкала из 3-х уровней – это не количественная оценка

Недостатки «светофора»

- Зависимость от квалификации эксперта / экспертов
- Зависимость от доверия к эксперту
- Влияние на мнение экспертов заинтересованными лицами
- Невозможность провести оценку для редких событий
- Отсутствие достаточного числа экспертов
- Психология восприятия рисков (когнитивные искажения)

У специалистов по ИБ и топ-менеджеров разные шкалы оценки рисков

Вы уверены, что ваш «высокий» риск такой же, как и у CFO?



Основные подходу к оценке вероятности

- Историческая (статистическая) оценка, позволяющая на основании данных прошлых периодов прогнозировать будущее
- Опрос экспертов
  - Метод Дельфи, метод парных сопоставлений, метод классификации групп риска
- Прогнозирование с использованием таких приемов, как дерево неисправностей (граф атак), дерево событий и т.п.

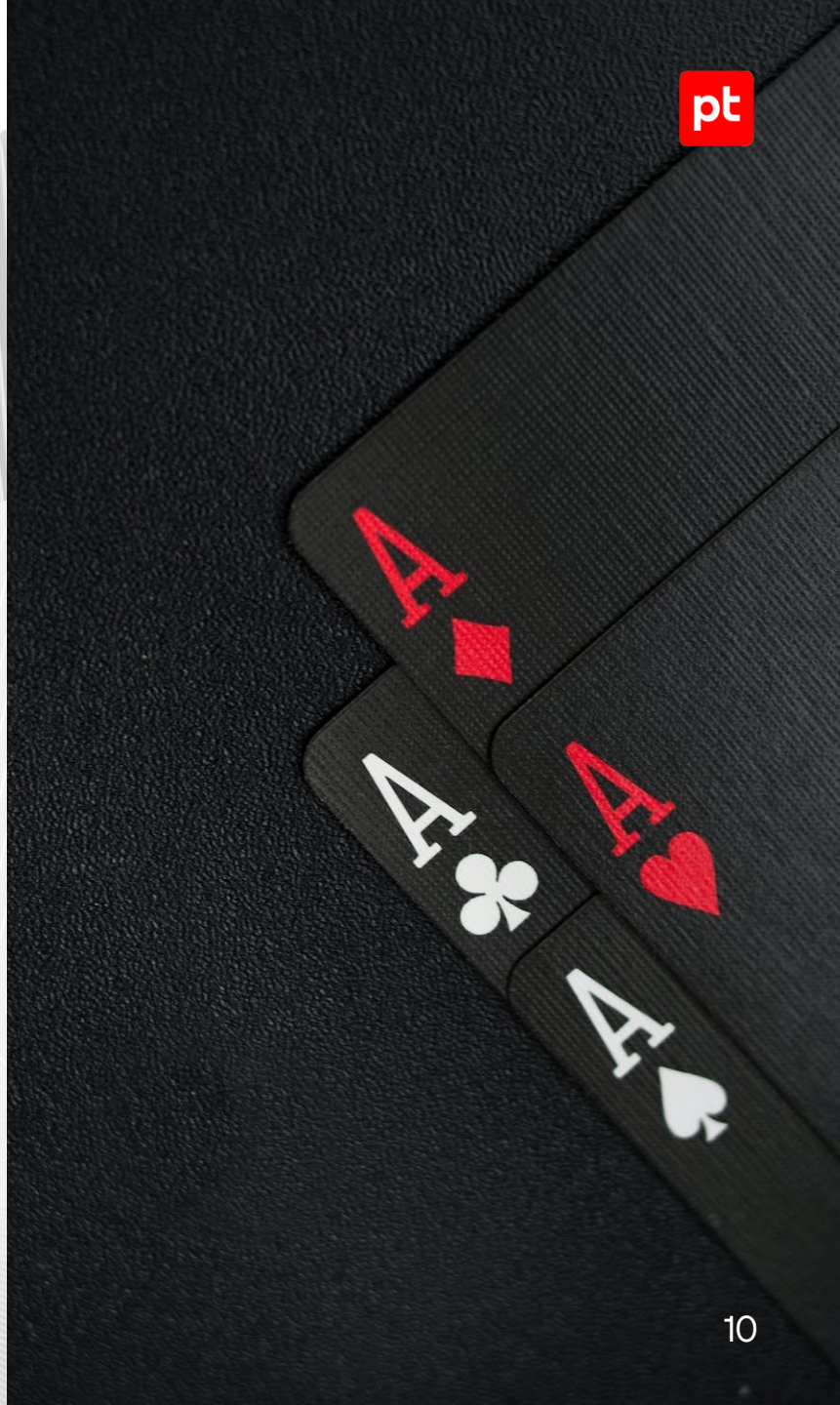
При каких условиях можно оценить вероятность?

- Одинаковое распределение событий
- События должны быть случайными
- События должны быть независимыми
- События должны составлять репрезентативную выборку

У вас есть массовые и однотипные события? Вам повезло – теория вероятностей для них применима. Вы оцениваете редкие или еще неслучившиеся с вами события? Вам не повезло ☹

Собственная статистика

- Историческая (статистическая) оценка позволяет на основании данных прошлых периодов прогнозировать будущее
- Один из эффективных методов
  - При условии неизменности среды оценки
- Необходимо наблюдение и сбор данных в течение нескольких лет
  - Без наличия адекватных инструментальных средств это непростая задача – сбор, нормализация, хранение и анализ данных



Аналитические методы

- Прогнозирование с использованием аналитических методов
  - «Дерево неисправностей» (Fault Tree Analysis) – диаграмма всех возможных последствий инцидента в системе (МЭК 61025)
  - «Дерево событий» (Event Tree Analysis) - диаграмма всех возможных последствий данного события
  - Имитационное моделирование отказов/инцидентов (метод Монте-Карло)

Экспертные методы

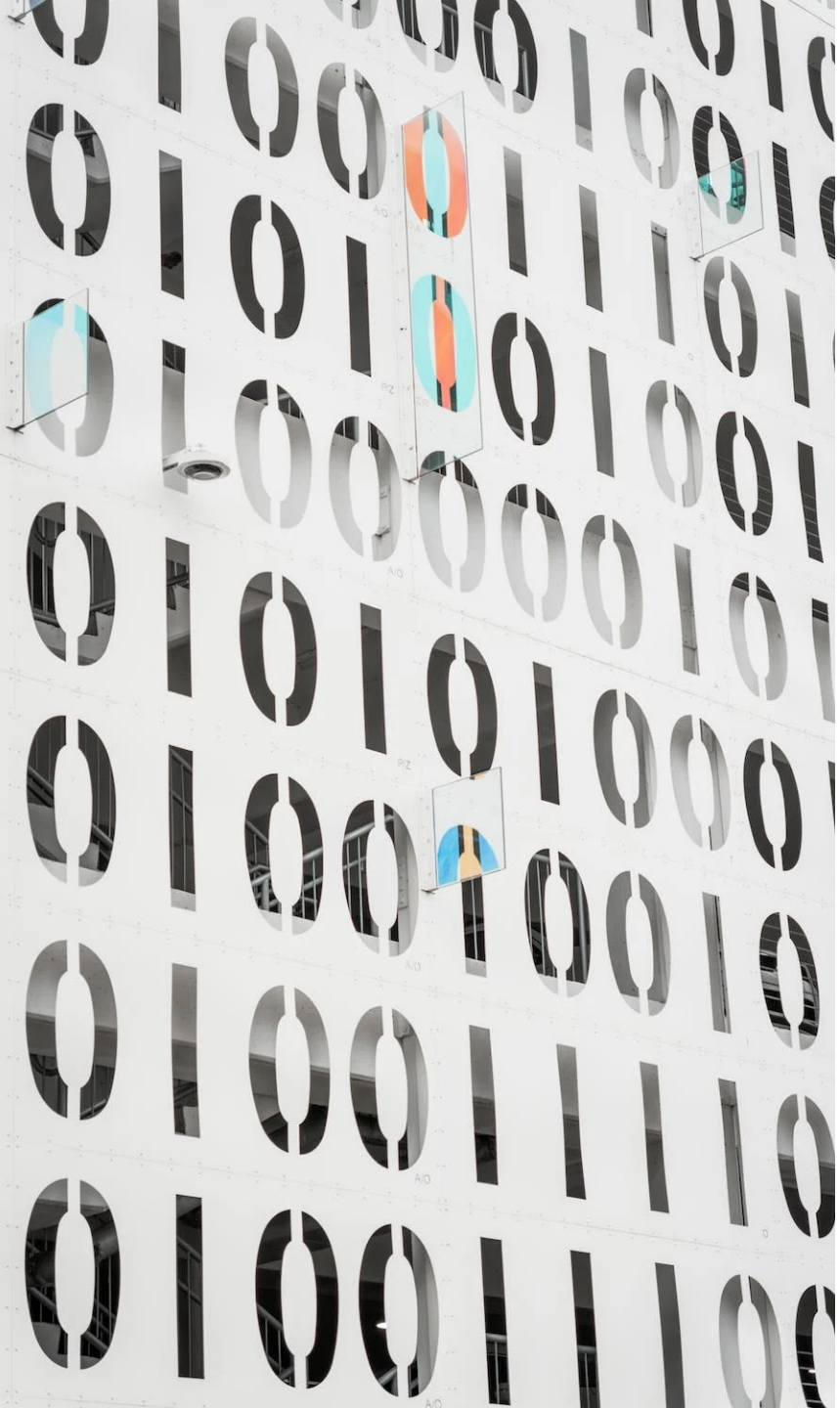
- Эксперты ранжируют вероятность наступления события исходя из своего опыта и знаний анализируемой системы
  - Зависимость от опыта
- Эксперты проверяют на практике возможность реализации риска (пентест, Bug Bounty)
  - Долго, дорого и невозможно для всех рисков

Когнитивные искажения

Вместо вероятности потенциал нападения

Название фактора	Диапазон	Значение при идентификации уязвимости	Значение при использовании уязвимости
Затрачиваемое время	< 0.5 часа	0	0
	< 1 день	2	3
	< 1месяц	3	5
	> 1месяц	5	8
	Не практично	*	*
Компетентность	Непрофессионал	0	0
	Профессионал	2	2
	Эксперт	5	4
Знание ОО	Отсутствие информа-ции	0	0
	Общедоступная ин-формация	2	2
	Чувствительная ин-формация	5	4
Доступ к ОО	< 0.5 часа или не обна-руживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	6
	> 1 месяц	4	9
	Не практично	*	*
Оборудование	Отсутствует	0	0
	Стандартное	1	2
	Специализированное	3	4
	Заказное	5	6

* Означает, что нападение невозможно в пределах тех временных рамок, которые были бы приемлемы для нарушителя. Любое значение «*» указывает на «высокий» рейтинг.



Бинарная вероятность

- Вероятность принимается равной единице, если угроза может быть осуществлена, и нулю – если нет
  - При отсутствии защитных мер
- Этот подход имеет право на жизнь, но только для небольшого количества систем и сценариев
  - В обычной жизни это слишком дорого
- ...или для угроз, которые являются очень распространенными
- Данный метод применяется в небольшом количестве различных методик
  - Методика оценки угроз – ФСТЭК
  - Security Architecture for Enterprise (SAFE) – Cisco
  - Методика ФСБ по персданным

Промежуточное резюме

Для редких событий ИБ, постоянно изменяющегося ландшафта угроз ИБ или еще не случавшихся событий посчитать вероятность количественно невозможно даже приблизительно

Либо это долго, дорого и никому не нужно!

Оценка потерь

- Оценка риска не имеет смысла, если мы не можем определить ценность актива, подверженного рискам
- Точная оценка невозможна по своей природе
  - Многие ее и не ждут, столкнувшись с потерями при инвестиционных, рыночных рисках...
- Worst-case (самый худший случай) не имеет отношения к анализу рисков, т.к. исчезает элемент вероятности
- Оценка пост-фактум возможна, но...

Уровни зрелости оценки ущерба от рисков ИБ

Как считаем потери?

- На базе чужой статистики (Verizon DBIR или Ponemon Institute)
- Пост-фактум - DAC (Detailed Attack Cost)
- Усредненно на базе прошлой статистики - ALE (Annual Loss Expectancy)
- От стоимости актива

Прямой и косвенный ущерб

$$U = U_p + A * U_k$$

- U - экономический ущерб от инцидента
- U_p - прямой экономический ущерб
- A - коэффициент приведения разновременных затрат (коэффициент дисконтирования), зависящий от длительности последствий
- U_k - косвенный экономический ущерб

прямого

Оценка ущерба от атак на сайт

- Цикл продаж, профиль пользователя, средний чек, график спроса и предложения...
- Сезонность продаж (цикл продаж)
- Время простоя за год * годовой размер доходов через сайт
- Сайт важен для бизнеса! Почему? А фиг знает!
- Я дерусь, потому что я дерусь (с) д'Артаньян

Что еще надо/можно учесть?

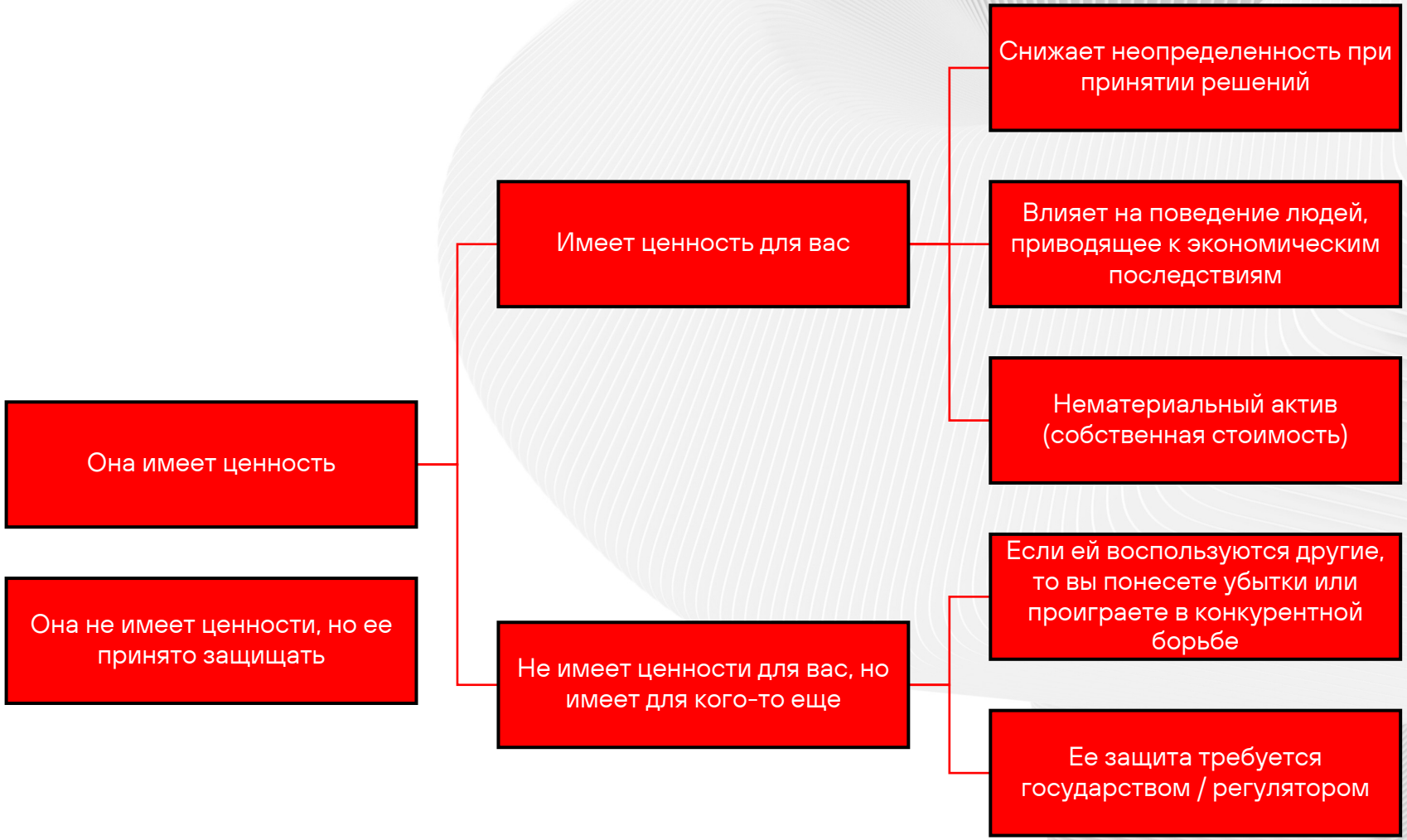
- Снижение доходов
- Потери интеллектуальной собственности
- Уменьшение резервов капитала
- Потеря работы, оплата медицинской терапии, отмененные планы, например, на каникулы и выходные и т.п.
- Компенсация персоналу
- Найм новых сотрудников
- Рост затрат на ИБ
- Рост затрат на страховку
- Снижение рейтинга
- Штрафы
- Расследование инцидента
- Уведомление пострадавших
- Компенсация
- Аренда центров обработки вызовов
- PR
- Выплаты вымогателям
- Судебные издержки
- Сдвиг сделок на следующие периоды
- Страхование киберрисков
- Отклоненные претензии по страховке
- Рост страховой премии
- Текучка клиентов
- Снижение стоимости акций
- Ухудшение условий по M&A
- Затраты на аудит ИБ

Итоговая оценка стоимости может отличаться от первичной на порядки

Оценка от актива

- Активы бывают материальные и нематериальные
- Материальные активы оцениваются обычно на основе стоимости их замены или восстановления
- Аналогичным образом часто оценивается и программное обеспечение
- Ценность информации и иных нематериальных активов определяется либо экспертным способом (метод Дельфи) или с помощью специальных методик

Ценность информационного актива



Виды стоимости НМА

Вид стоимости	Определение
Стоимость обмена	Вероятная цена продажи, когда условия обмена известны обеим сторонам и сделка считается взаимовыгодной
Обоснованная рыночная стоимость	Наиболее вероятная цена, по которой объект оценки переходит из рук одного продавца в руки другого на открытом рынке и добровольно
Стоимость использования	Стоимость объекта оценки в представлении конкретного пользователя и с учетом его ограничений
Ликвидационная стоимость	Стоимость объекта оценки при вынужденной продаже, банкротстве
Стоимость замещения	Наименьшая стоимость эквивалентного объекта оценки

Методы оценки НМА

Рыночный	Затратный	Доходный
• Метод сравнения продаж аналогичных объектов оценки	• Метод стоимости замещения • Метод восстановительной стоимости • Метод исходных затрат	• Метод расчета роялти • Метод исключения ставки роялти • Метод DCF • Метод прямой капитализации • Экспресс-оценка • Метод избыточной прибыли • Метод по правилу 25% • Экспертные методы

Стоимость информации?

- Информация стоит денег сама по себе
  - Самый простой метод
  - Множество стандартов оценки нематериальных активов
- Информация позволяет улучшить что-то
  - Стоимость информации равна разнице между стоимостью «до» и «после»
- Информация позволяет принимать решения
  - Самый сложный сценарий оценки стоимости
  - Методы AIE, iValue и другие

Но считать ущерб все равно необходимо

- Для учета в финансовой отчетности (если таковые требования есть)
- Для расчета страхового возмещения (если вы используете киберстрахование)
- Для оценки затрат на деятельность в области ИБ (если у вас не фиксированный бюджет)
- Для выплат компенсации клиентам (по требованиям законодательства или вашей политики)
- Для сравнения с… <много факторов>

Промежуточное резюме

Сложность и длительность расчета, отложенность многих потерь, разные формы потерь, отсутствие доступа к исходным бизнес-данным и недоверие к ИБ со стороны топ-менеджмента приводит к невозможности количественной оценки потерь от реализации рисков ИБ

Либо это долго, дорого и никому не нужно!

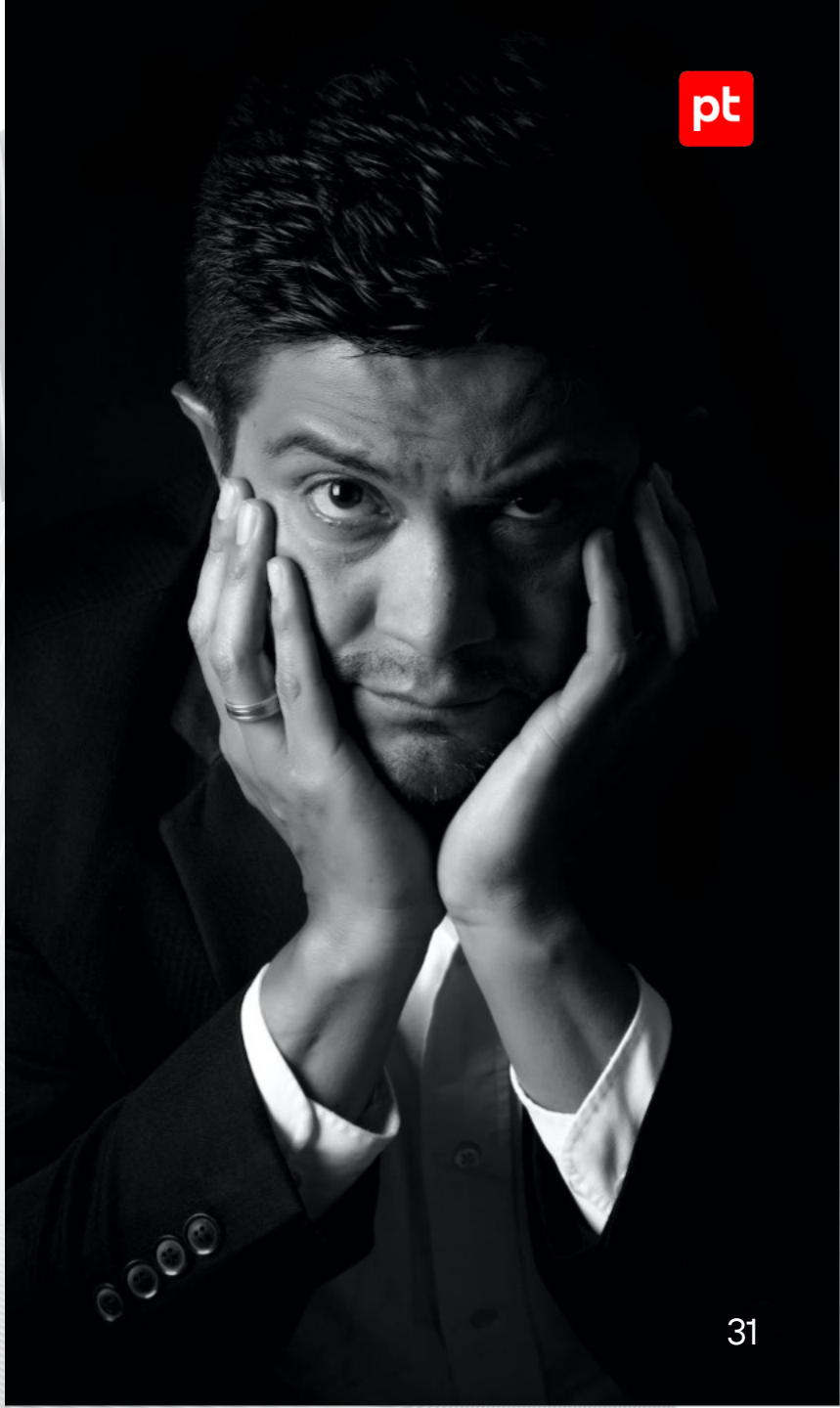
И куча «но» от самих ИБшников

- Нет, потому что мы не знаем, где взять данные
- Нет, потому что не дают данные
- Нет, потому что у нас нет квалификации для измерений
- Нет, потому что мы не верим в эффективность этих методов
- Нет, потому что мы боимся соваться в финансы
- Нет, потому что нет гарантии, что нам поверят
- Нет, потому что нам не верят
- Нет, потому что мы забыли математику
- Нет, потому что нет

Поэтому светофор!

Выводы

- Детальный количественный анализ частот и последствий от рисков ИБ при их большом количестве не всегда возможен и осуществим
- Предварительное ранжирование сценариев реализации рисков ИБ для последующего детального количественного анализа приоритетных рисков требует времени и экспертизы
- Во многих случаях к моменту завершения расчетов, они устаревают и становятся не нужны!



Если вас это не смущает, то для вас есть FAIR!

Все остальные методики – баловство и трата времени тех, для кого мы эту оценку действительно делаем. Хотя для первичной оценки, не выходящей за пределы ИБ, метод светофора вполне работает!

Но другие же считают...

Оценка бизнес-рисков

- Детальная оценки ущерба и вероятности на основе реальных бизнес-данных
- Дополнительная проверка с владельцем бизнес-юнита
- Потенциальное устаревание к моменту завершения оценки

Оценки киберрисков

- Экспертная оценка методов светофора (высокий /красный/, средний /желтый/ и низкий /зеленый/ ущерб или вероятность)
- Нехватка бизнес-знаний и данных для оценки ущерба
- Данных по вероятности нет

Как начальство думает о кибербезе

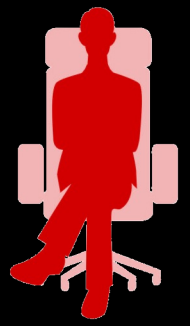
Чем выше статус, тем меньше мыслей о мелких проблемах

Топ-менеджер

- Как преумножить бизнес?
- Как не потерять бизнес?

→ Во внимание принимаются только события с катастрофическими последствиями, реализация которых недопустима

Оценка быстра, но субъективна



Рисковик

- Какие риски для бизнеса?
- Какой ущерб для бизнеса?
- Какова вероятность ущерба?

→ Оцениваются все риски для бизнеса с их оценкой по вероятности и степени ущерба с последующим занесением в реестр на сотни пунктов

Оценка объективна, но очень долга

Директор по ИБ

- Какие угрозы ИБ?
- Какие уязвимости?
- Какие инциденты ИБ?

→ В список включаются все опасности – из отчетов Threat Intelligence, СМИ, блогов вендоров, логов средств защиты без учета вреда для бизнеса

Приоритизация не с точки зрения бизнеса

Фокус на события, которые могут привести к катастрофическим последствиям

Мы называем их «недопустимыми событиями»

Примеры

- Природная катастрофа
- Банкротство
- Финансовые потери
- Отзыв лицензии
- Экологическая катастрофа
- Несчастный случай на производстве
- Останов производства
- ... и т.д.

Существуют ли такие события в результате ИБ?

Это все страшилки или реальность?

- Февраль 2015 года - хакерская атака на трейдинговую систему казанского Энергобанка, в результате которой курс рубля в течение 14 минут менялся на биржевых торгах более чем на 15%
  - Потери банка составили 244 миллиона рублей (по другим оценкам – 500 млн.)
- Вывод через банкоматы одного из банков нескольких сотен миллионов рублей (2015)
- Изменение рецептуры на пищевом производстве в ЦФО и отравление людей
- Отключение электричества в одной из областей РФ на 4 часа в 2022-м году
- Дипфейковый звонок личному бухгалтеру CEO московского рекламного агентства и потеря 200 тысяч евро

Источник: PT Standoff

В чем отличия?

Важные замечания

- Это субъективная оценка, но топ-менеджеров, понимающих бизнес
- Недопустимые события формулируются топ-менеджментом, а не специалистами по ИБ или рисками
- Достаточно быстрый процесс (~2-3 часа)
- Обычно формулируется 6-8 событий
- События определяются в рамках стратсессии
- У нас есть каталог с примерами недопустимых событий

Что дальше?

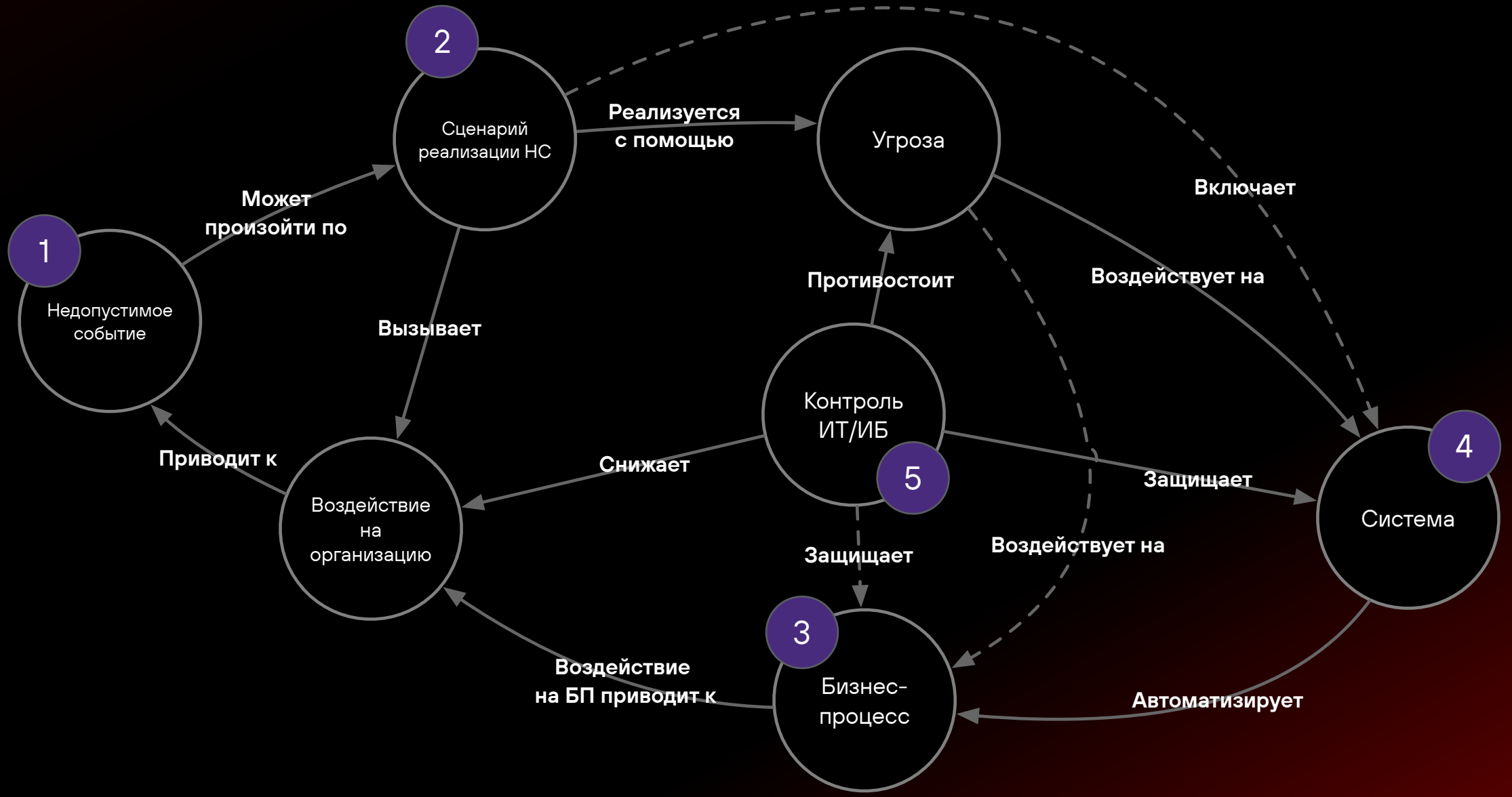
Маппинг событий на ИТ-инфраструктуру

Определили, что дальше?

	Что делается	Результат	Недели							
			1	2	3	4	5	6	7	8
Определение НС	Проведение стратегического семинара по формированию перечня недопустимых событий с их пороговыми значениями и определению ответственных за НС в компании	Перечень НС								
Декомпозиция НС	Проведение технических семинаров и интервью с целью определения сценариев реализации недопустимых событий, целевых и ключевых систем	Сценарии реализации НС								
Описание существующего ИТ-и ИБ-ландшафта	Проведение технических интервью о фреймворке исполнителя с целью определения текущего ИТ- и ИБ-ландшафта	Описание ИТ- и ИБ-ландшафта								
Определение условий и ограничений	Определение условий и ограничений кибертрансформации (например, ограничений по стоимости и максимальной длительности работ, по целевой архитектуре (in-house, outsourcing) и пр.)	Условия и ограничения кибер-трансформации								
Формирование требований	Формирование бизнес-требований для повышения киберустойчивости, адресованных функциональным подразделениям ИТ и ИБ, а также потенциальным исполнителям работ	Бизнес-требования для повышения киберустойчивости								

Итого: 7–8 недель

Приземляем на инфраструктуру



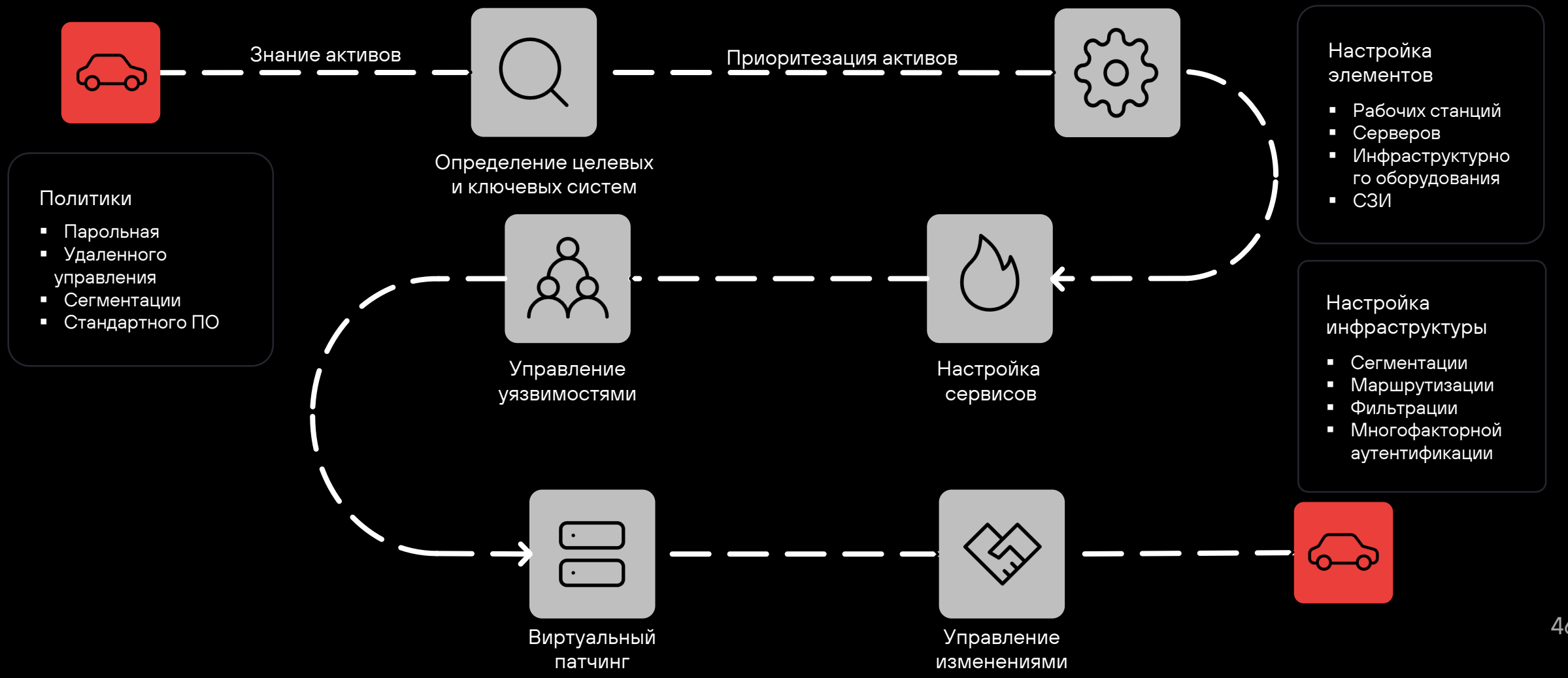
Затем вы идете традиционным путем

Усиление инфраструктуры, а также внедрение защитных мер и построение центра противодействия киберугрозам (ЦПК)

TTA > TTR

Харденинг ИТ-инфраструктуры никто не отменял и его постоянный контроль (например, с помощью PT Carbon)

Усиление ИТ-инфраструктуры для уменьшения площади атаки



А теперь можно хейтить!

Спасибо

alukatsky@ptsecurity.com