Применение инструментов качества для ранжирования рисков

Ненад Иняц,
PhD, профессор Дунайского университета г. Кремс (Австрия)

Слайд 1

1. Первым международным стандартом, полностью посвященным исключительно общим рискам, является ISO 31000:2000. В настоящее время действующая версия стандарта ISO 31000:2018 («Управление рисками - принципы и рекомендации» или на английском языке «Risk management - Principles and guidelines »). В стандарте приведено следующее определение риска:

- влияние неопределенности на цели. Когда в этом определении говорится о «неопределенности», имеется в виду вероятность возможного возникновения события в результате недостаточного знания или незнания всех необходимых данных, а также наличия возможного вмешательства (например, неоднозначность, помехи и т. д.). Существует математическая интерпретация риска как произведение вероятности возникновения (обычно нежелательного) события и его последствий, которые могут быть выражены в различных формах включая и финансовые.

Слайд 2

2. В качестве приложения или руководства к основному стандарту по менеджменту безопасности информационных систем ISO / IEC 27001:2013 «Информационные технологии - Методы безопасности - Системы менеджмента информационной безопасности - Требования» используется стандарт ISO/IEC 27005:2018 «Информационные технологии - Методы безопасности - Управление рисками информационной безопасности». В стандарте ISO / IEC 27000:2018 принято следующее определение риска:

- влияние неопределенности на цели. Сочетание последствий, которые могут возникнуть в результате возникновения нежелательного события, и вероятности его наступления. В стандарте ISO/IEC 27005:2018 указывает описание риска как продукта потенциальных угроз, уязвимостей и последствий для четко определенных активов любой организации. При этом опасности возникновения события и уязвимость принимается как вероятность его возникновения.

Слайд 3

Источник	Название стандарта
ISO/IEC	ISO/IEC 31000:2018 Risk Management – Principles and guidelines
ISO/IEC	ISO/IEC Guide 73:2002 Risk Management – Vocabulary – Guidelines fo use in standards
ISO/IEC	ISO/IEC Guide 51:1999 Information technology - Information security risk management
ISO/IEC	ISO/IEC 27005:2018 Information technology - Information security risk management
GOST - R	ГОСТ Р 51897-2011 Менеджмент риска. Термины и определения
AS/NZ	AS/NZ 4360:2004 Risk management
BS	BS 31100:2008 Code of praktice for risk management
DIN	DIN IEC 62198:2009 Risk management for projects

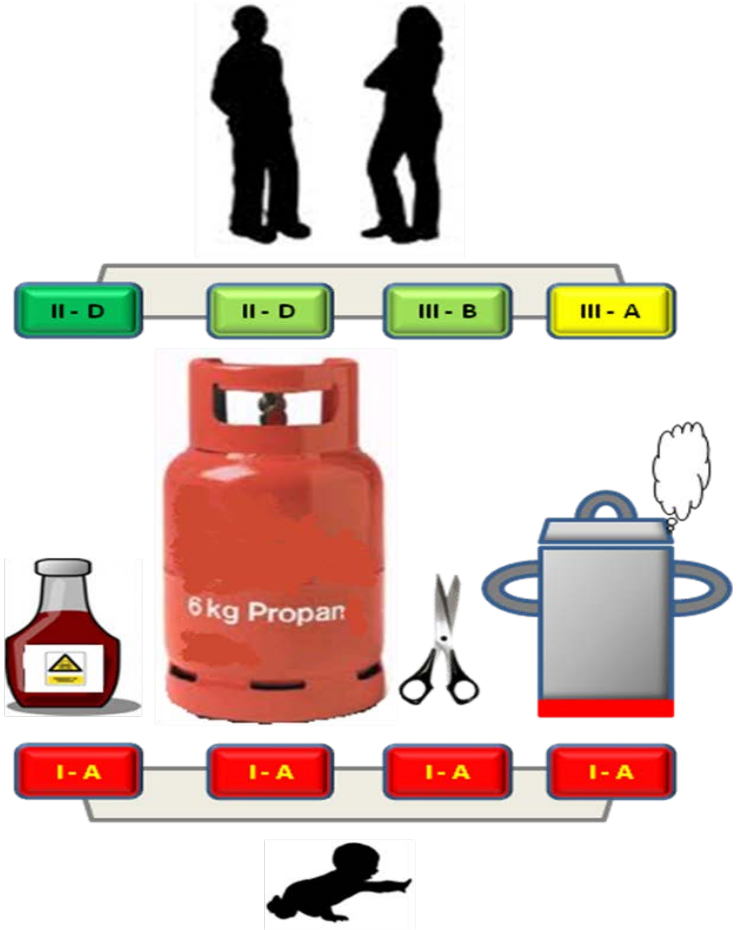
Слайд 4

Частота появления \ Уровень опасности	небольшой	средний	большой
высокая	*последствия (средние)*	*последствия (большие)*	*последствия (катастро-фические)*
средняя	*последствия (малы)*	*последствия (средние)*	*последствия (большие)*
маленькая	*последствия (незначительные)*	*последствия (малы)*	*последствия (средние)*

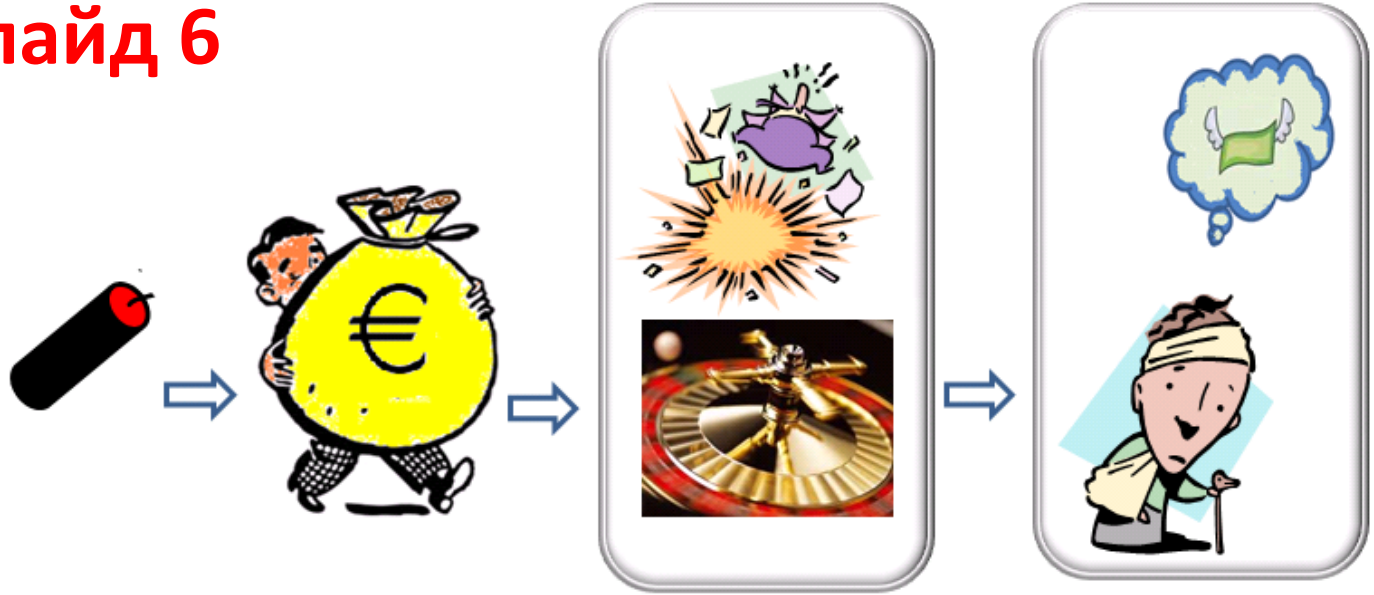
Слайд 4

Частота появления	Уровень опасностей			
	Незначительный VI	Малый III	Критический II	Катастрофи-ческий I
Постоянно/ большая	IV - A	III - A	II - A	I - A
Большая B	IV - B	III - B	II - B	I - A
Средняя C	IV - C	III - C	II - C	I - C
Малая D	IV - D	III - D	II - D	I - D
Маловероятная E	IV - E	III - E	II - E	I - E
Невероятная F	IV - F	III - F	II - F	I - F

Слайд 5



Слайд 6



Постоянная опасность

Имущество или ценности

Вероятность нападения, %

×

Последствия напа-дения (Евро)

Риск

Слайд 7


Mjere
Меры
безопасности
Приятный
Уязвимый
Ranjivost
Постоянная опасность
Имущество или ценности
Вероятность нападения, %
Последствия нападения (Евро)
Риск

Слайд 8

Последствия \ Вероятность	1	2	3
3	3	6	9
2	2	4	6
1	1	2	3

Результат	Угрозы	1			2			3		
	Уязвимость	1	2	3	1	2	3	1	2	3
	3	3	6	9	6	12	18	9	18	27
	2	2	4	6	4	8	12	6	12	18
	1	1	2	3	2	4	6	3	6	9

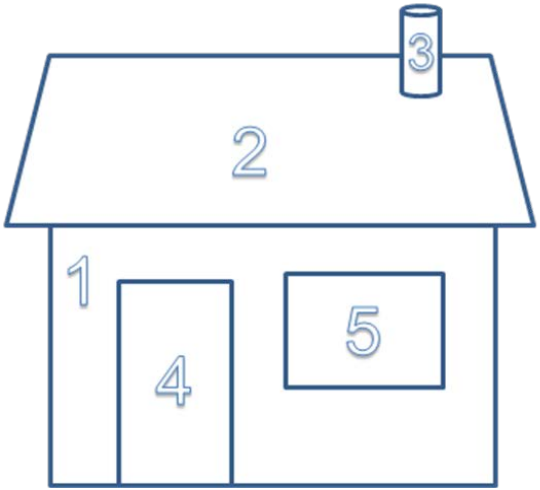
Слайд 9

(1) Обычная политика риска

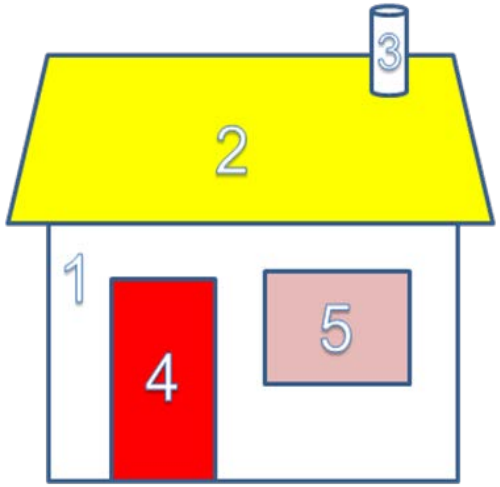
(2) Высокорисковая политика

(3) Низкорисковая политика

Слайд 10



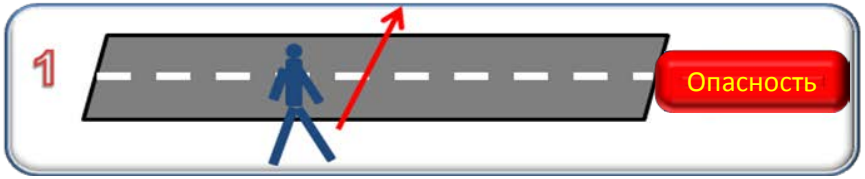
	Элементы дома
1	Стена
2	Крыша
3	Труба
4	Дверь
5	Окно

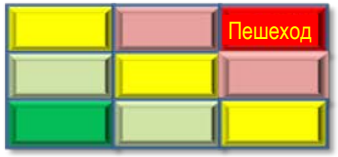


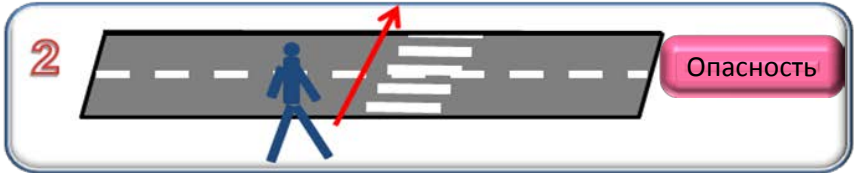
	Элементы дома
1	Стена
2	Крыша
3	Труба
4	Дверь
5	Окно

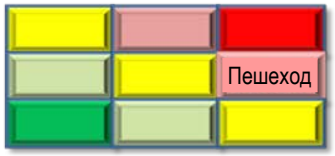
Частота \ Опасность (уровень)	1	2	3
3			4
2			5
1			2

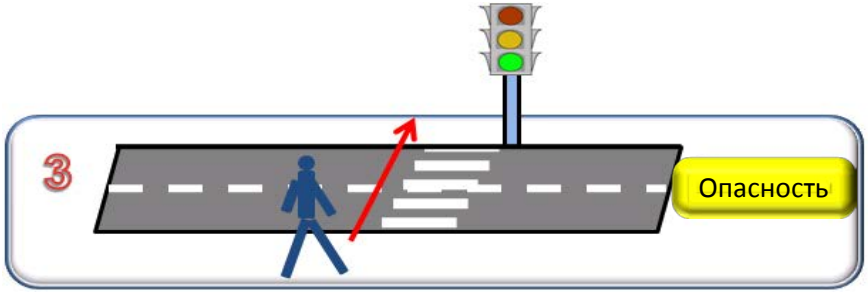
Слайд 11

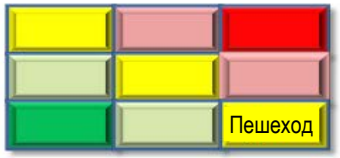

1
Опасность

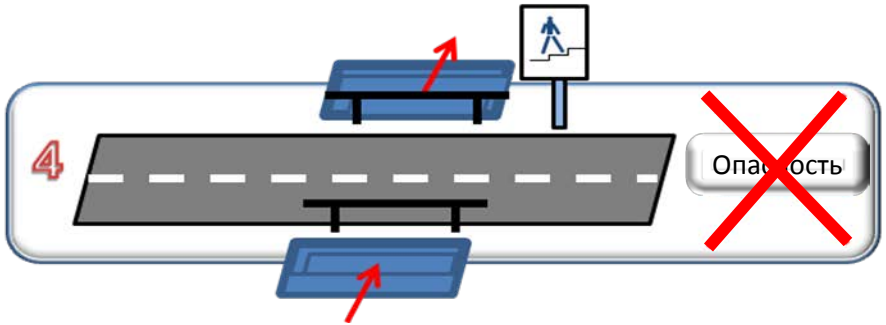

Пешеход

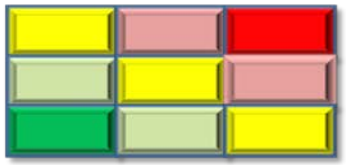

2
Опасность


Пешеход


3
Опасность


Пешеход

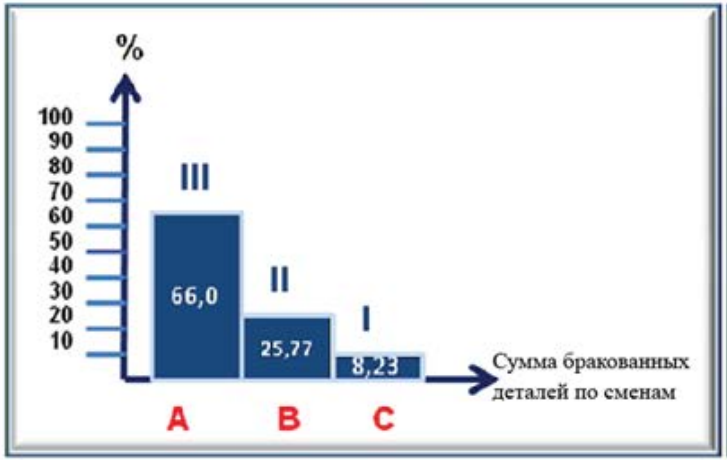

4
Опасность

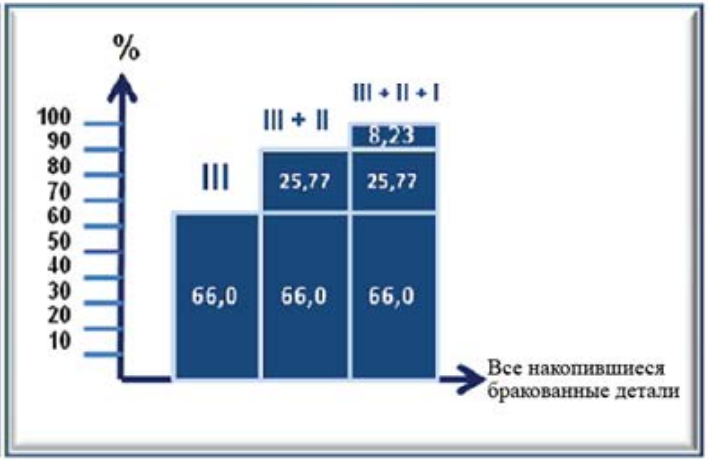


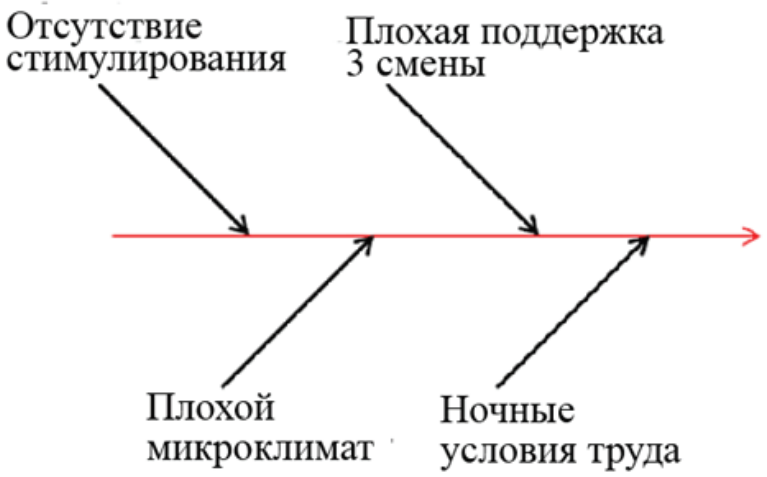
Слайд 12

	Понедельник	Вторник	Среда	Четверг	Пятница	Суббота	Σ
06: - 14:	1	1	2	2	3	3	8
14: - 22:	2	2	3	3	1	1	25
22: - 06:	3	3	1	1	2	2	64
Σ = 97	15	16	15	18	16	17	97

Слайд 12


%
100
90
80
70
60
50
40
30
20
10
III
II
I
66,0
25,77
8,23
A
B
C
Сумма бракованных деталей по сменам


%
100
90
80
70
60
50
40
30
20
10
III
III + II
III + II + I
66,0
66,0
66,0
25,77
25,77
8,23
Все накопившиеся бракованные детали


Отсутствие стимулирования
Плохая поддержка 3 смены
Плохой микроклимат
Ночные условия труда

Слайд 13

Фактор исследования: скорость

... быстрее чем					Σ
		1	2	0	3
	1		2	0	3
	0	0		0	0
	2	2	2		6

A : B → 1 : 1 Оба элемента имеют одинаковую скорость

A : B → 2 : 0 Элемент A значительно быстрее

A : B → 0 : 2 Элемент B значительно быстрее

Плохая поддержка
3 смены

Слайд 14

Взгляд вовнутрь

Взгляд в сторону окружения

SWOT	Преимущества (S): 1. Люди. 2. Мотивация. 3. ….	Недостатки (W): 1. Организация. 2. Обучение 3. ……
Шансы (O): 1. Инновации. 2. Креативность 3. …..	SO стратегия: 1. Новые продукты 2. Производительность. 3. …….	WO стратегия: 1. Реструктуризация. 2. Обучение
Угрозы (T) 1. Конкуренция. 2. Инфляция 3. ….	ST стратегия: 1. Бенчмаркинг. 2. Рационализация 3. …..	WT стратегия: 1.Инвестиции. 2. Реинженеринг 3. ….

Слайд 15

1.1. Принятие риска. Принятие риска считается отказом от любых действий в отношении риска, связанного с конкретным товаром или имуществом. Для этого может быть несколько причин: вероятность слишком мала (например, падение метеорита на человека или организацию), или последствия незначительны, или просто нет средств для вмешательства.

1.2. Передача риска. Когда мы говорим о передаче риска, мы обычно имеем в виду передачу риска и всех возможных последствий третьей стороне - например, страхование или привлечение специализированной компании для защиты объектов и людей. Эта форма передачи риска предполагает уплату страховых взносов и договоров об оказании услуг.

1.3. Избежание риска. Процедура (частичного или полного) избегания рисков в большинстве случаев выполняется путем управления опасностями - от снижения до полного устранения опасностей и, следовательно, рисков (например, с помощью новых технологий, замены опасных материалов и процессов, реинжиниринга). и т. д.).

1.4. Снижение рисков. Наиболее распространенным методом управления рисками в отношении определенных товаров или активов является снижение рисков. Затем, в соответствии с первым или вторым представлением риска, структурные компоненты сокращаются. В первом примере это снижение вероятности атак или последствий реализации последствий, а во втором - уменьшение угроз, уязвимостей и последствий.