Московский государственный лингвистический университет
Факультет международной информационной безопасности

Анализ особенностей применения ключевых индикаторов риска в сфере информационной безопасности

Смолякова Елена Александровна
ФГБОУ ВО МГЛУ, ФИБ1-17-41
e.a.smolyak@gmail.com

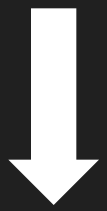
Москва, 2018

Понятие ключевых индикаторов риска

КИР – количественные показатели факторов риска.

Инструмент мониторинга; прогнозирования.

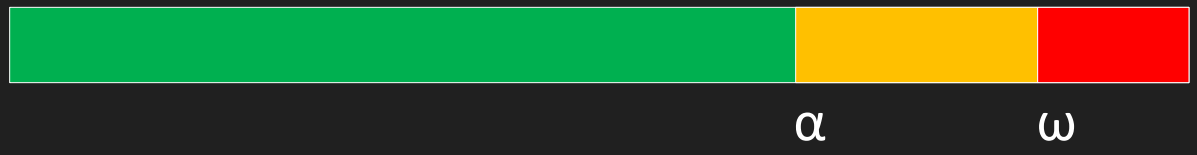
[Риск] = [Вероятность события] × [Размер ущерба]



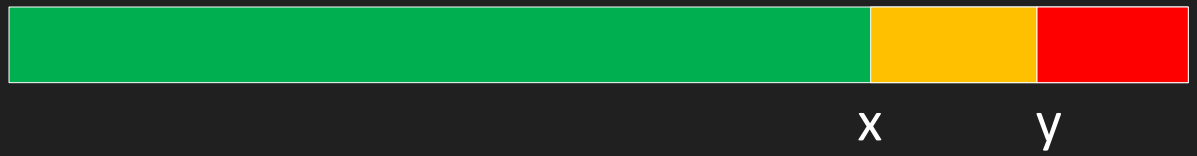
КИР

Пример использования

Сети



x 0,25 Число обнаруженных на АРМ вирусов



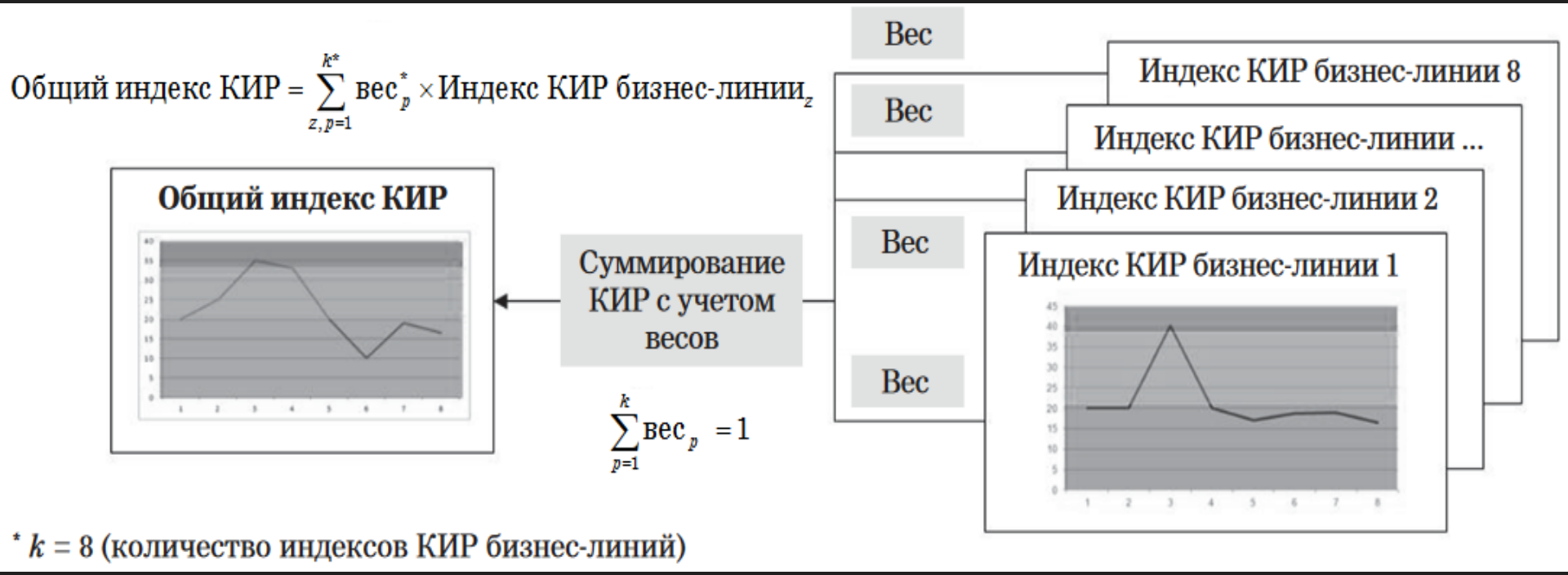
x 0,34 Время некорректной работы DNS-сервера



Различия в терминах

- KRI (Key Risk Indicator, ключевые индикаторы риска):
  «насколько вероятна реализация риска»;
- KPI (Key Performance Indicator, ключевые показатели эффективности):
  «насколько эффективна деятельность»;
- KCI (Key Control Indicator):
  «насколько эффективно управление деятельностью».

Методика с учетом бизнес-линий



Подход к оценке общего индекса КИР из статьи «Методика разработки системы индексов ключевых индикаторов риска» (В. Сизикова, В. Гаврилина, В. Битюцкий)

Ключевые элементы успешного внедрения КИР

- Содействие руководства;
- Налаженное взаимодействие между подразделениями;
- Достаточная информированность риск-менеджеров.

КИР;
\+ Системный подход;
Комплексный подход.

Наибольшая эффективность

Cyber Defense Matrix

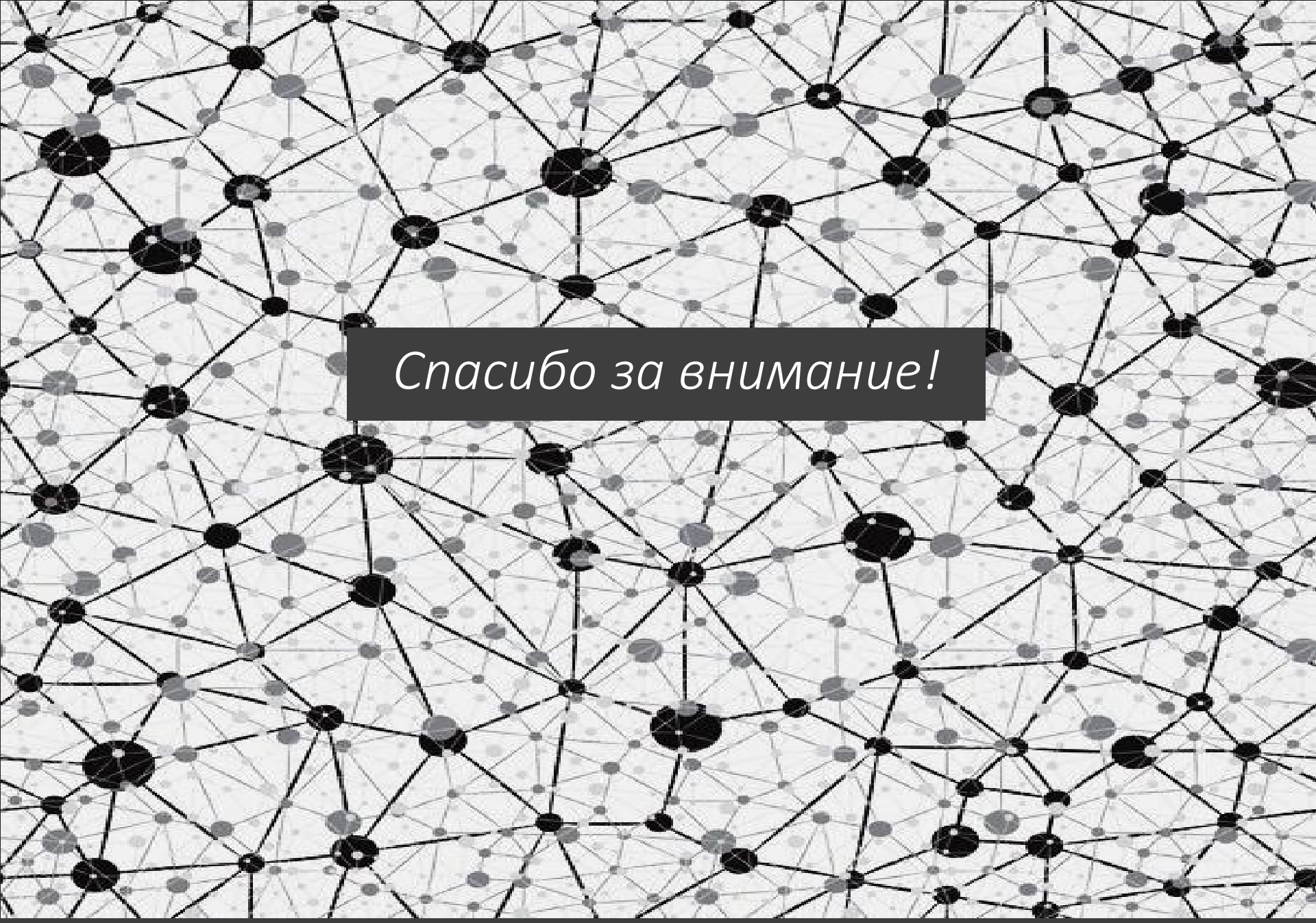
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Автор модели – Sounil Yu (Senior Vice President, Bank of America)

Элементы успешной разработки КИР в ИТ и ИБ

- Учет внешних факторов; → Включать соответствующие КИР.
- Наглядность и прозрачность КИР; → Разделять КИР на категории.
- Учет особенностей организации. → Не использовать стандартные наборы КИР.

1 Риск ≠ 1 КИР.


Спасибо за внимание!