Количественная оценка кибер-рисков – неизбежное будущее современных компаний

PwC
ProfIT security day

Докладчик

Олег Прокудин

Менеджер отдела анализа и контроля рисков

Oleg.prokudin@pwc.com

Более чем 9 лет опыта работы по анализу бизнес-процессов, систем и контролей, включая проведение ИТ и ИБ аудитов и разработки ИТ и ИБ стратегий, а также проектов, связанных с обеспечением соответствия требованиям регуляторов.

Области наибольших компетенций:

Приведение процессов и систем компаний в соответствие ИТ и ИБ требованиям
Построения систем управления информационной безопасности на базе ISO27001
Разработка ИБ стратегий

Образование и профессиональные квалификации:

BSc in IT, KIMEP university.
Сертифицированный Профессионал в области Информационной Безопасности (CISSP)
Ведущий аудитор и специалист по внедрению (Lead Implementer/Lead Auditor) стандарта ISO27001.
Сертифицированный аудитор информационных систем (CISA)

Вопросы которые все чаще появляются в повестке дня

Насколько высок предполагаемый **уровень финансовых потерь** от кибер-инцидентов?

Как **рассказать Совету Директоров о кибер-рисках** языком, который будет им понятен?

Настолько **профиль наших кибер-рисков совпадает со стратегическими приоритетами** и соответствует риск аппетиту?

Как я могу измерить и **продемонстрировать эффективность инвестиций** в информационную безопасность в привязке к критичным кибер-рискам?

Эволюция процесса управления кибер рисками

1 Кибер безопасность не стоит на повестке

- Интуитивно понятные или общепринятые контроли
- Нет артикулированных потребностей

2 Процесс движимый зрелостью

- Фокус на приобретении новых возможностей
- Сравнение себя с другими
- Неуправляемый рост контроля и надзора
- Постоянный рост бюджета на ИБ без учета корпоративного риска

3 Процесс движимый требованиями соответствия

- Базовый риск-центрический подход
- Ограничения в области применения
- Стандартизированные наборы контролей
- Формальный фреймворк

4 Процесс движимый рисками

- Основная цель – снижение риска
- Приоритет инвестиций в программы, максимально воздействующие на риски
- Программа снижения кибер риска способствует достижениям корпоративным целям по рискам
- Оптимизация защитных мер по стоимости, гибкости и мере снижения риска

Начальная стадия
Упор на Страх-Неопределенность-Сомнения

Работоспособен на начальном этапе, при необходимости обеспечить базовый функционал СУИБ.

Переходный момент

- Сформулированные требования и задачи,
- необходимость повторяемого подхода,
- интеграция в корпоративные процесс и ISMS

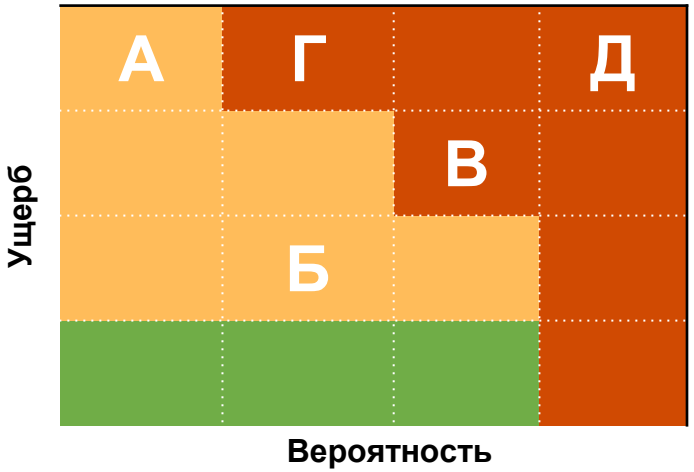
Целевое состояние

- полная интегрированность в корп. управление рисками
- низкая зависимость от экспертного мнения,
- инструменты автоматизации
- широкое использование данных и статистики для количественной оценки

“Качественная” и количественная оценка рисков

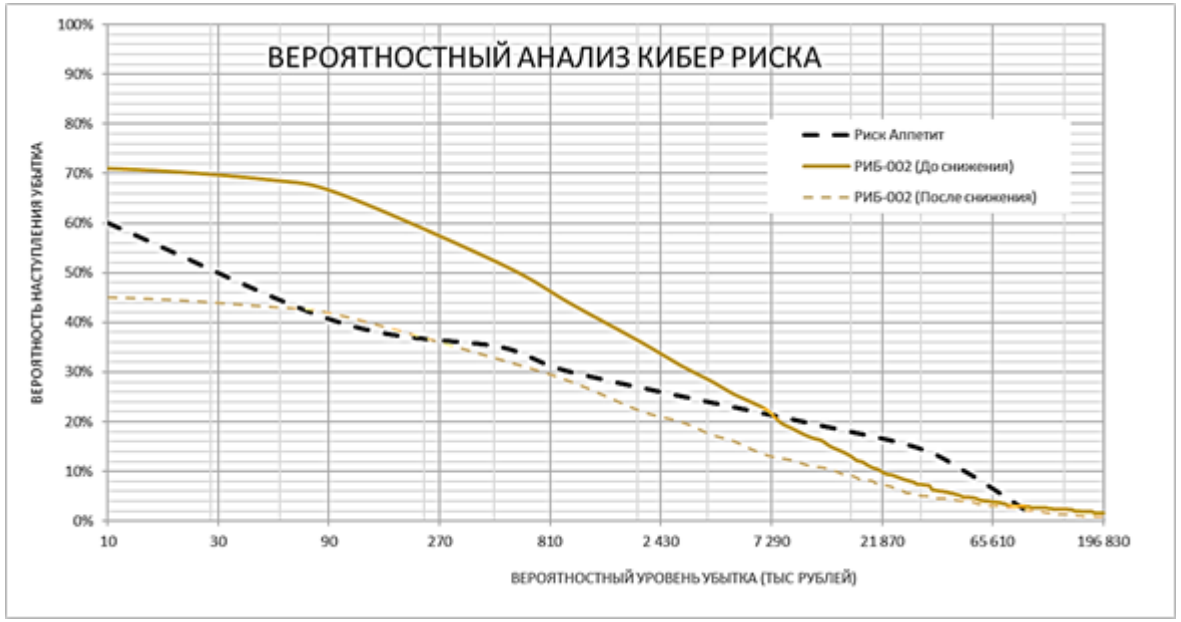
? **Вопрос - какая вероятность возникновения инцидента «Заражение вредоносным кодом» и какой ущерб он нанесет?**

Событие произойдет с **высокой** вероятностью и нанесет **средний** ущерб



- Экспертные предубеждения включены в оценку без корректировки.
- Шкала измерения запрещает математические действия.
- Вычисление финансовой эффективности качественно оцененных рисков затруднено.

Событие произойдет с вероятностью **от 0,5 до 1,5 %** в год и нанесет ущерб в объеме от **53 250 000 KZT** до **202 950 000 KZT**



Что мешает переходу к количественной оценке?

1	**Это невозможно измерить и подсчитать.**
2	**У нас нет достаточного объема информации и статистических данных.**
3	**Мы не можем подсчитать это с необходимой точностью.**

Давайте попробуем посчитать?

Вопрос: С какой вероятностью инцидент **«Заражение вредоносным кодом»** приведет к утечке интеллектуальной собственности и какой будет нанесен ущерб, если известно, что в компании работает **1000** сотрудников, **500** из которых имеют доступ к секретной информации?

Пример расчета вероятности

1 **Частота атаки** ((отправка зараженных вирусом писем, рассылка со ссылками на вредоносные сайты и т.д.))

10 000 случаев в год

2 **Количество регистрируемых инцидентов, связанных с заражением вирусам**

100 случаев в год

3 **Процент вирусов-шпионов в общей массе вирусов**

10 % - 30 %

1% - Вероятность единичного заражения

100 (заражения) ÷ 10100 (попытки + заражения) = 0,01 = 1 %

50% - Процент сотрудников, имеющих доступ к секретной информации

500 ÷ 1000 = 0,5 = 50%

От 0.5% до 1,5% - Базовая вероятность утечки секретных данных от единичного инцидента заражения вирусом

0,01 * 0,5 * 0,1 = 0,005 = 0,5%
0,01 * 0,5 * 0,3 = 0,015 = 1,5%

Пример расчета стоимости

		Верхний предел потерь (90%)	Нижний предел потерь (90%)
1	**Выручка (годовая)** Ожидаемое падение выручки находится в пределах от 0,7 до 0,1 процента от годового объема, приведенного к EBITDA	380 450 000 KZT	83 500 000 KZT
2	**Расследование инцидента и ликвидация последствий**	4 500 000 KZT	900 000 KZT
3	**Внеплановые совершенствования средств контроля кибербезопасности**	65 000 000 KZT	10 000 000 KZT
4	**Репутационный ущерб** (стоимость возврата репутации)	95 000 000 KZT	34 000 000 KZT
		202 950 000 KZT	**53 250 000 KZT**

Событие произойдет с вероятностью **от 0,5 до 1,5 %** в год и нанесет ущерб в объеме от **53 250 000 KZT** до **202 950 000 KZT**

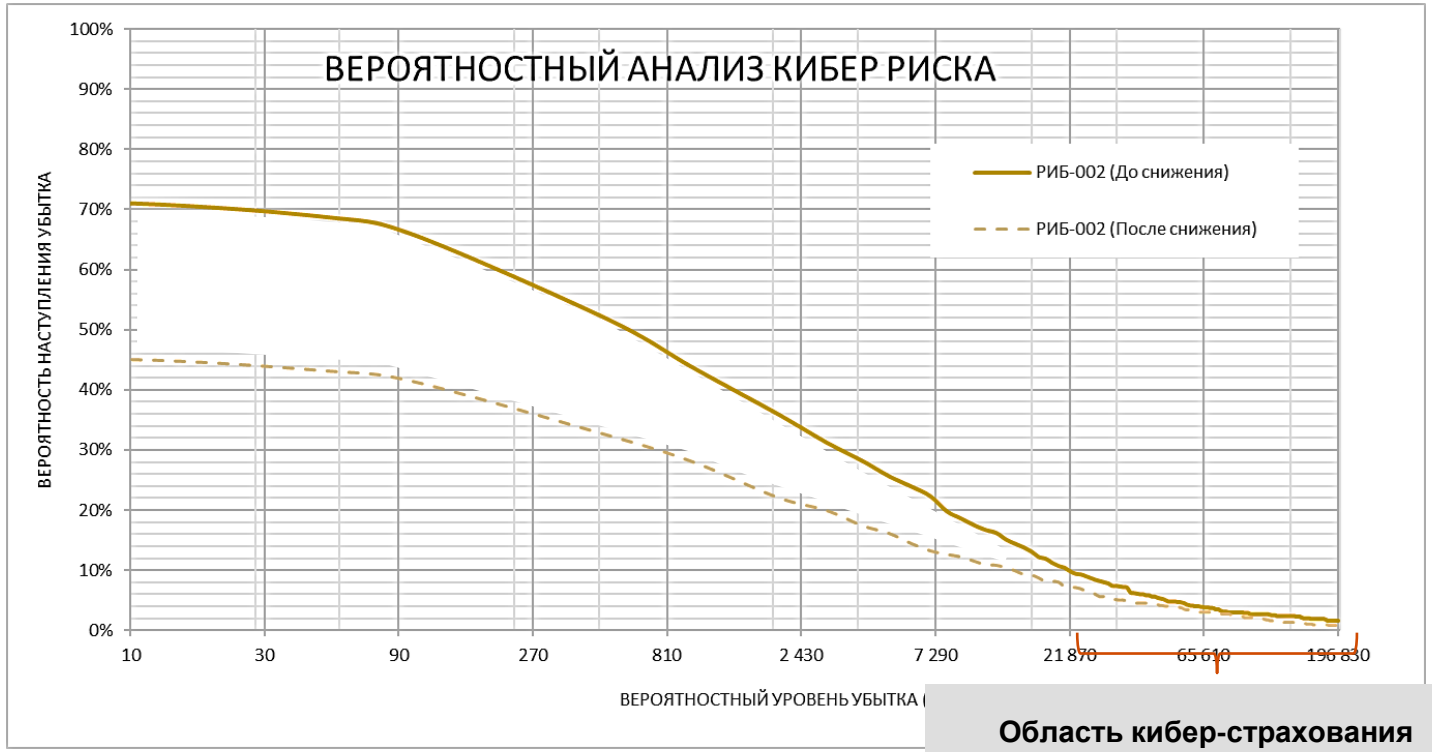
Один из возможных результатов

Уровень расчетных среднегодовых потерь (ALE)	**264,0 млн KZT. За 1 год**
Применение мер снижения риска	**- 119,0 млн KZT**
Остаточный среднегодовой ущерб	**145,0 млн KZT.**
Планируемые инвестиции в ИБ	**16 млн KZT.**

- Система DLP **8,0**
- Система контроля привилегированного доступа **9,0**
- Мониторинг событий ИБ **6,0**

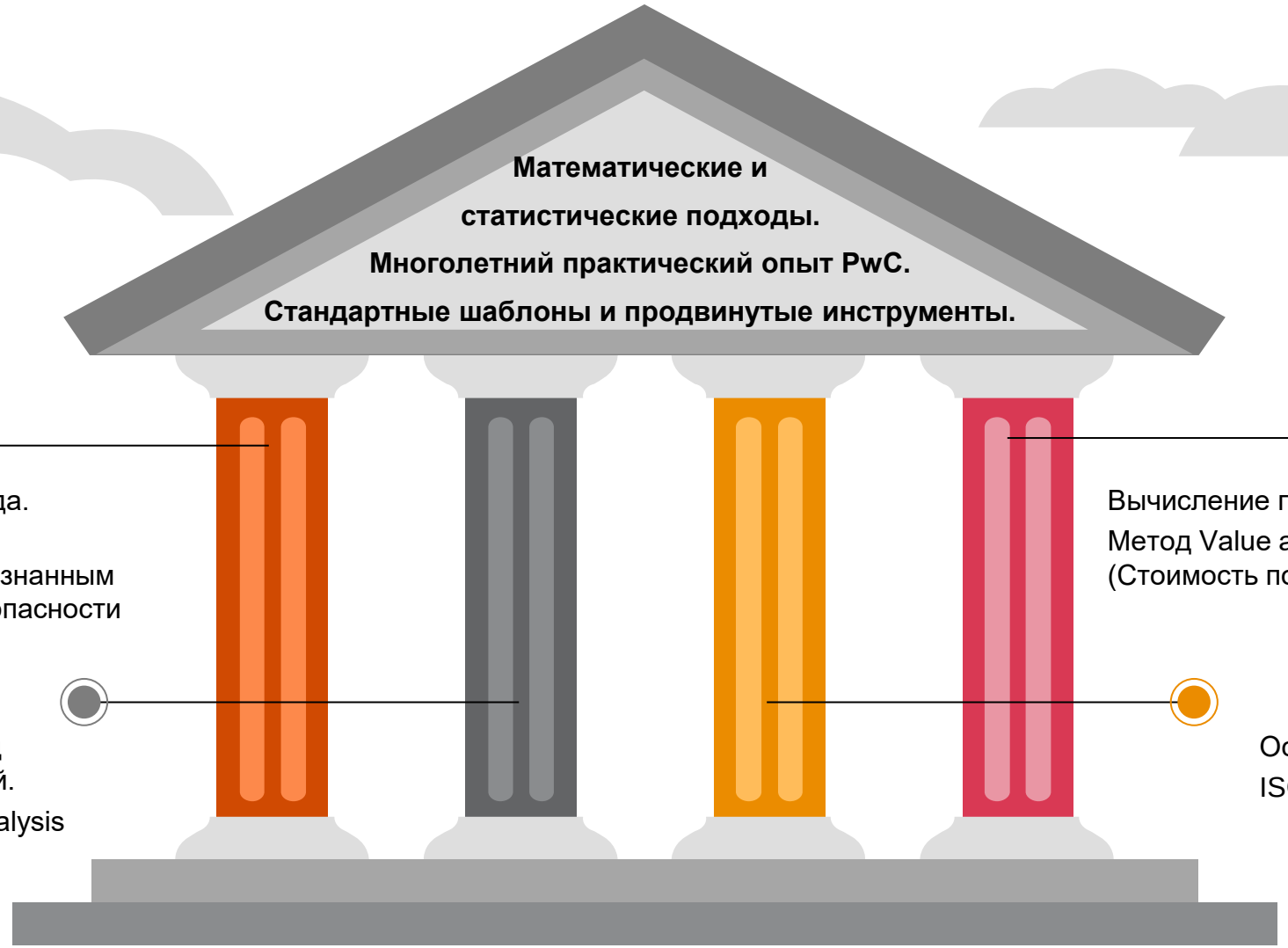
25,0 млн KZT За 1 год

Средний Ожидаемый Убыток после снижения:	109 млн KZT
Cyber TCO после снижения:	41 млн KZT
Бюджет на кибер контроли увеличится на (%)	161%
Риски ИБ сократятся на (%)	25%
ROI	225%



Область кибер-страхования

Подход PwC Cyber VaR



Модель риска и основа подхода.

Метод IRAM2, разработанный Information Security Forum, признанным лидером в области кибер безопасности и управления кибер рисками.

Таксономия риска, подход к моделированию событий.

Методика FAIR (Factor Analysis for Information Risks).

Вычисление предполагаемых потерь.

Метод Value at Risk (Стоимость под Риском).

Основа процесса.

ISO 27005.

Подведем итоги

1. Риски ИТ и ИБ можно и нужно считать в количественном выражении. В обозримом будущем количественная оценка рисков ИТ и ИБ может стать обязательной для ряда индустрий.

2. У большинства Компаний существует достаточно данных для того, чтобы начать считать риски ИТ и ИБ количественно

3. Количественная оценка рисков ИТ и ИБ дает прозрачный инструмент принятия решения для руководства Компании

4. Количественная оценка рисков может послужить отличным фундаментом для построения стратегии ИБ, а также внести свой вклад в стратегию развития бизнеса.

Вопросы?

pwc.com