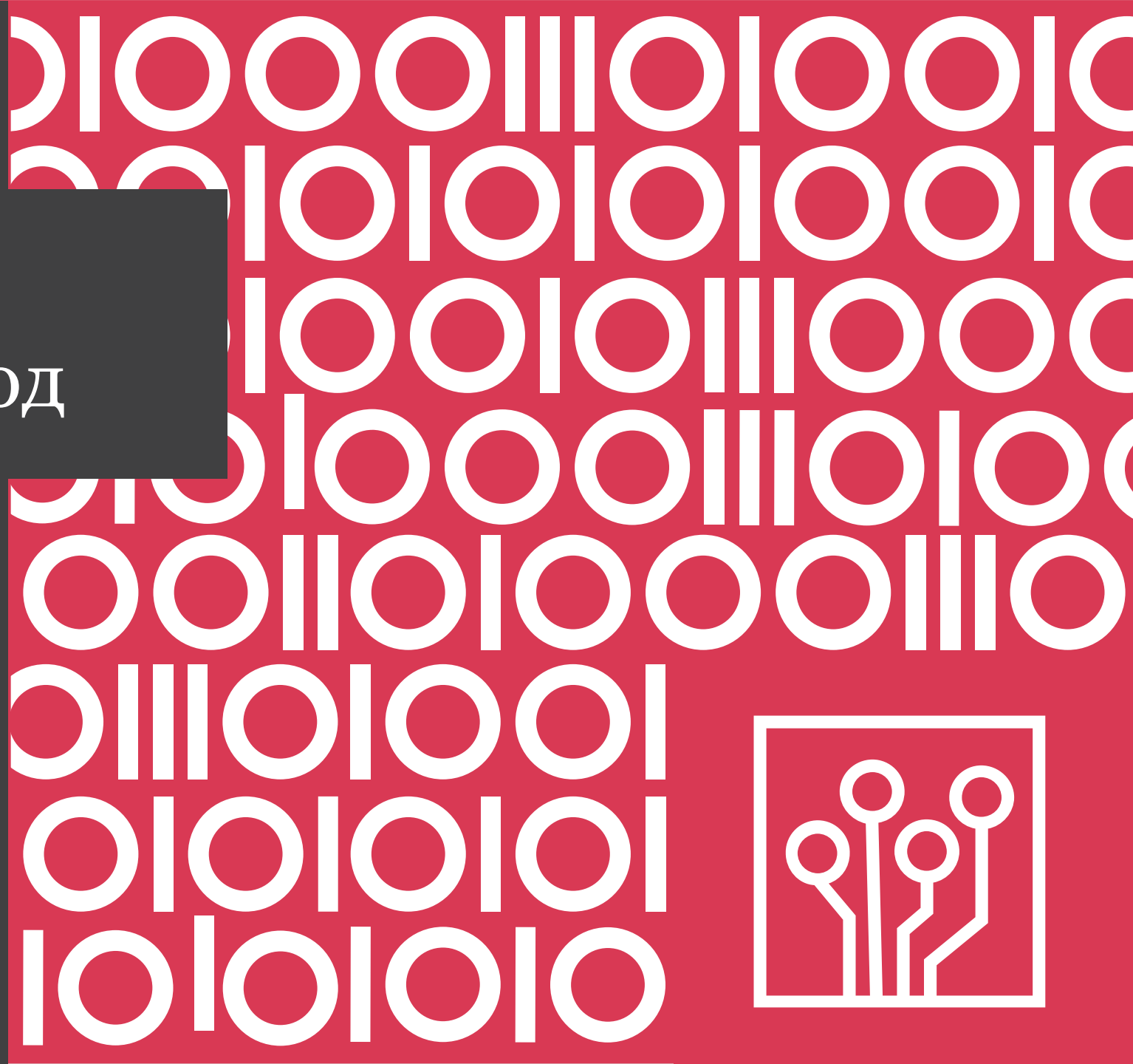
Количественная оценка рисков ИБ Принципы и подход

PwC, 2021



SABSA Chartered Security Architect (SCF)
ISO/IEC 27001:2013 Lead Implementer
CISSP

mikhail.tolchelnikov@pwc.ru

https://www.pwc.ru/cybersecurity

Михаил Толчельников

Менеджер практики анализа и контроля рисков с более чем 15 летним опытом работы в областях кибер оперирования, управления рисками, комплаенса и организации ответа на кибер инциденты.

Занимал руководящие должности в иностранных компаниях из списка FTSE 100, сопровождая и поддерживая бизнес трансформации, цифровизацию и переходы на глобальный аутсорсинг.

В настоящий момент являюсь экспертом в областях:

- Управление и количественная оценка кибер рисков,
- Построение систем управления информационной безопасностью,
- Отчетность и измерение эффективности контрольной среды ИБ,
- Управление рисками в цепочке поставок.

Риски и возможности

Устранение уязвимостей в цифровой платформе предприятия снизит профиль риска до планируемого уровня

Покупка нового средства защиты поможет снизить ущерб от события риска на 10%

Рост регуляторной зависимости и рисков, связанных с потерей IP может ухудшить показатели развития

Запуск нового цифрового продукта позволит увеличить клиентскую базу, достигнув стратегических показателей

Покупка новой линии производства позволит поднять прибыль на 5%

Выход на принципиально новый рынок позволит усилить портфель инноваций

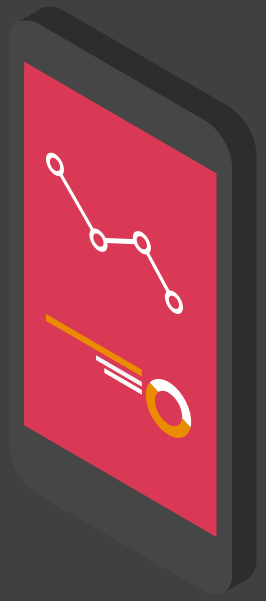
Управление рисками это не цель, это инструмент

Наша задача – дать бизнесу достаточно информации для принятия финансово-оптимального решения по инвестициям в минимизацию рисков

Мы можем по-разному реагировать на риски:

- принятие риска;
- отказ от риска;
- снижение риска;
- передача риска другой стороне;

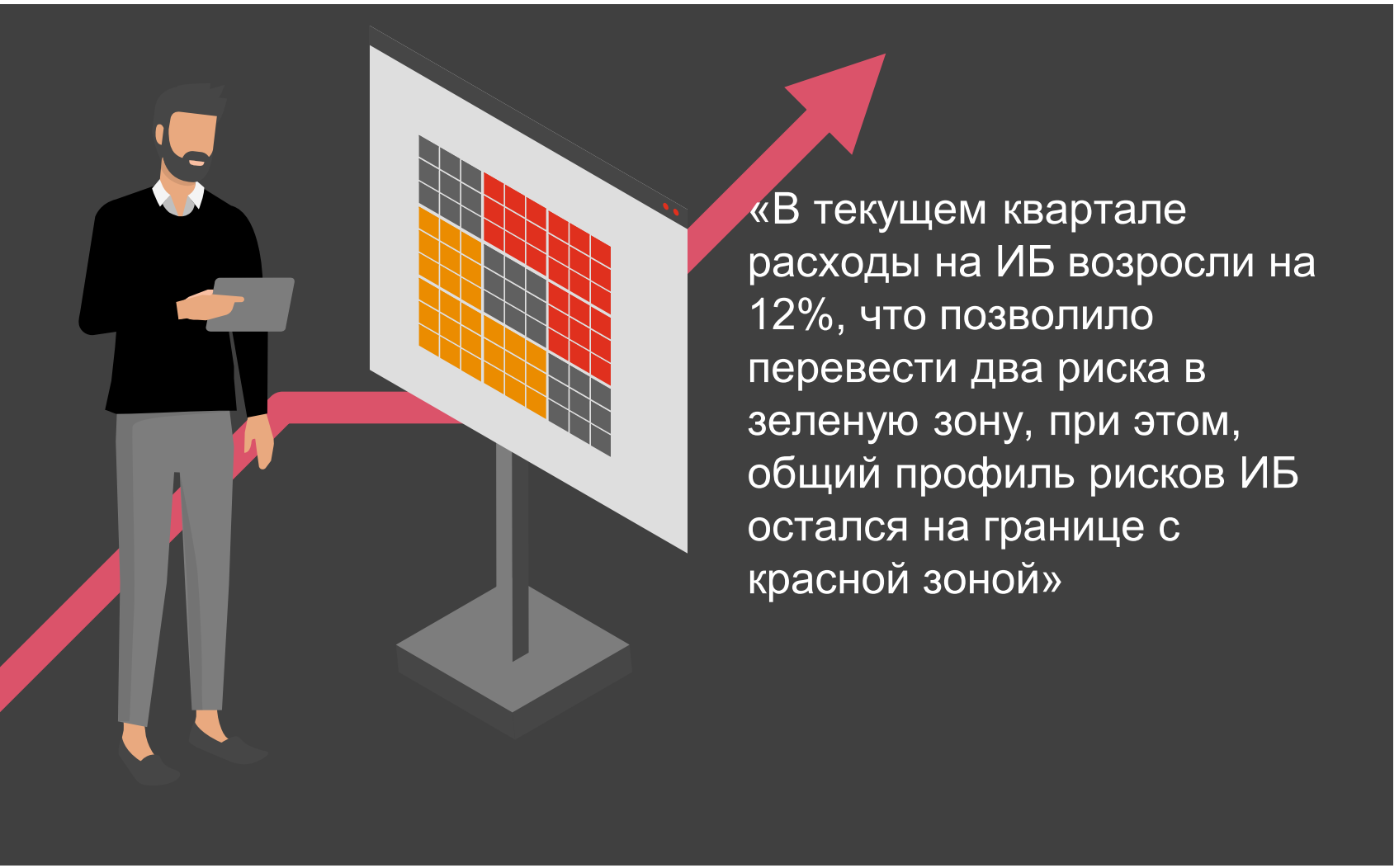
- увеличение риска



Мы можем по-разному финансировать риски:

- Отношение «Риск-Затраты» = 1000% для областей, где мы склонны к риску;
- Отношение «Риск-Затраты» = 100% там, где мы хотим избежать ощутимого ущерба;
- Отношение «Риск-Затраты» = 10% там где мы не имеем толерантности к риску;

Умножение красного на высокий



«В текущем квартале расходы на ИБ возросли на 12%, что позволило перевести два риска в зеленую зону, при этом, общий профиль рисков ИБ остался на границе с красной зоной»

Концентрируемся на значимом

Цели Компании

Увеличить EBITDA Компании на 20 млрд. руб.

Расширить количество активных пользователей мобильных приложений до 30 млн.

Увеличить инвестиционную привлекательность Компании

Риски информационной безопасности

Остановка операционной деятельности в ходе кибер атаки

Регулярные утечки пользовательских данных приводят к снижению рейтинга мобильных приложений и оттоку пользователей

Планы M&A и ранние отчеты о финансовых результатах стали доступны злоумышленникам

Влияние на цели

Длительный срок восстановления после атаки привел к снижению выручки на 65% на время инцидента

От 6% до 10% активных пользователей удалили мобильные приложения после новостей о взломе и краже данных

Изменение условий M&A привело к снижению привлекательности сделки.
Стоимость акций снизилась на фоне заявлений об инсайдерской торговле

Берем за основу работающую методику

Моделируем ущерб

РИСК
Вероятностные значения частоты наступления и величины будущих потерь

Масштаб потерь

Стоимость под Риском

Прямые финансовые потери	Расследование и ликвидация последствий	Репутация и лояльность клиентов	Расходы на кибербезопасность	Дополнительно
Снижение выручки	Внешние специалисты	Отток постоянных клиентов	Закупка новых инструментов	Увеличение страховой премии
Потери ФОТ	Сбор улик и расследование	Снижение параметра «компания первого выбора»	Сотрудники и ФОТ	Судебные издержки
		Снижение медиа рейтинга		

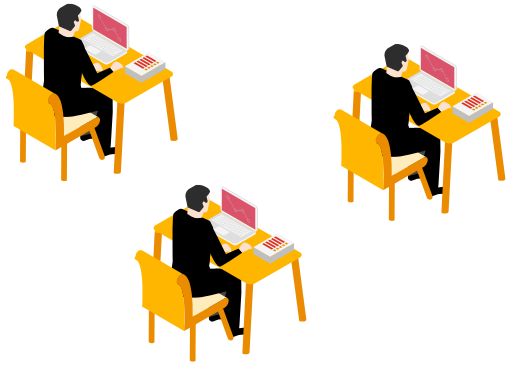
Моделируем вероятность событий риска

РИСК
Вероятностные значения частоты наступления и величины будущих потерь

Частота событий потерь

Постоянные попытки агентов угрозы

Агенты угрозы используют множество различных средств атаки: фишинг, вирусы-шифровальщики, DDoS и т.д.

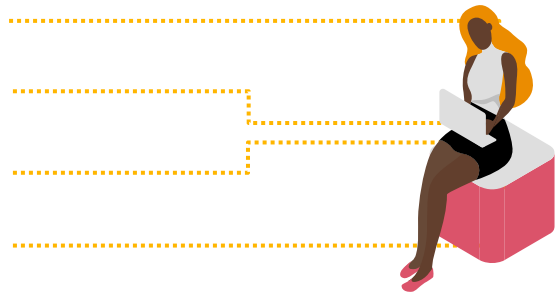


Защитные меры ИБ

Зрелость контролей и эффективность многоуровневой защиты снижает возможность успешной атаки

Некоторые атаки достигают цели и приводят к нанесению ущерба

Ущерб выражен в утечке, недоступности, краже средств, падении стоимости акций и т.д.

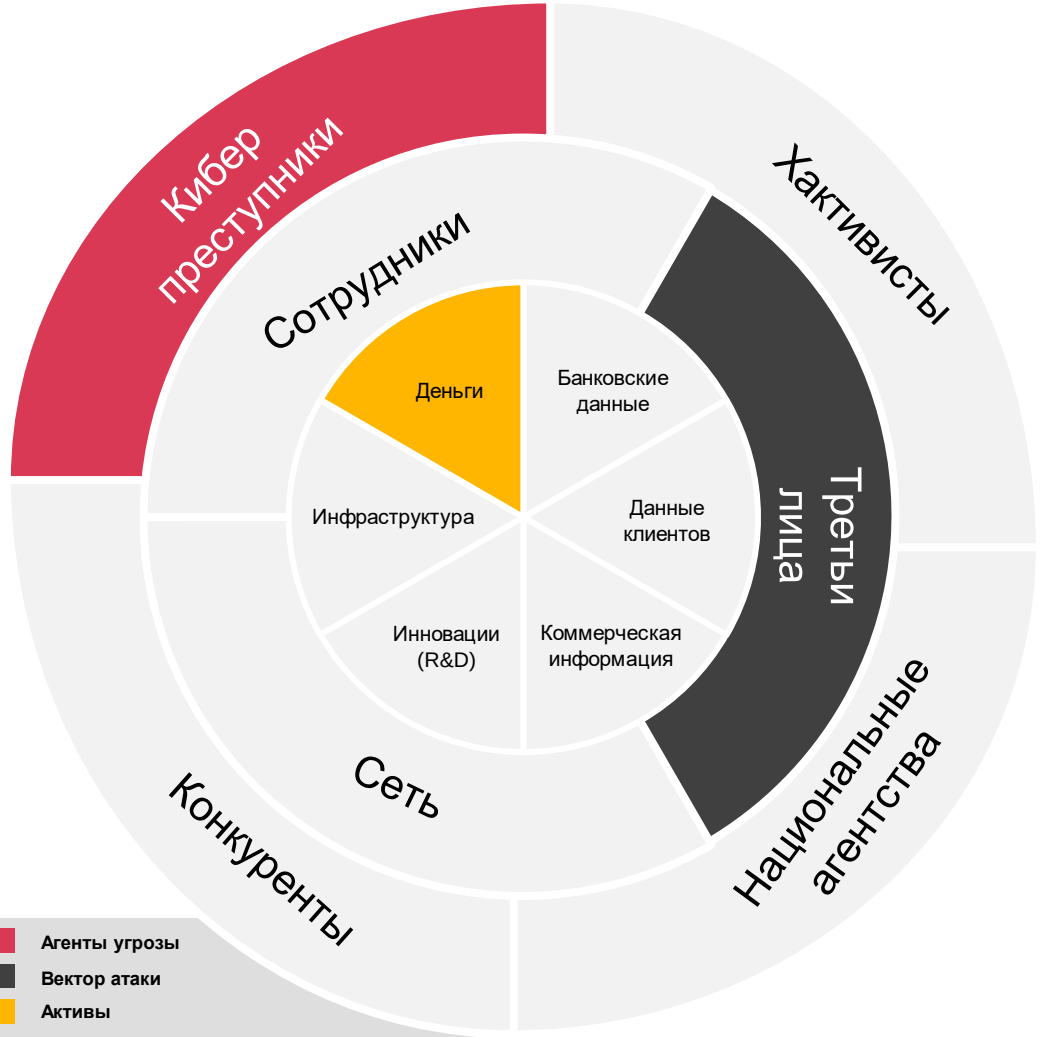


Вероятность атаки с целью получения выкупа (ВА)

Вероятность отражения атаки средствами защиты (ВЗ)

Вероятность нанесения ущерба для компании = (ВА) x (ВЗ)

Правильно расставляем приоритеты



Используем методы численного моделирования

Внутренняя статистика
по произошедшим инцидентами ИБ

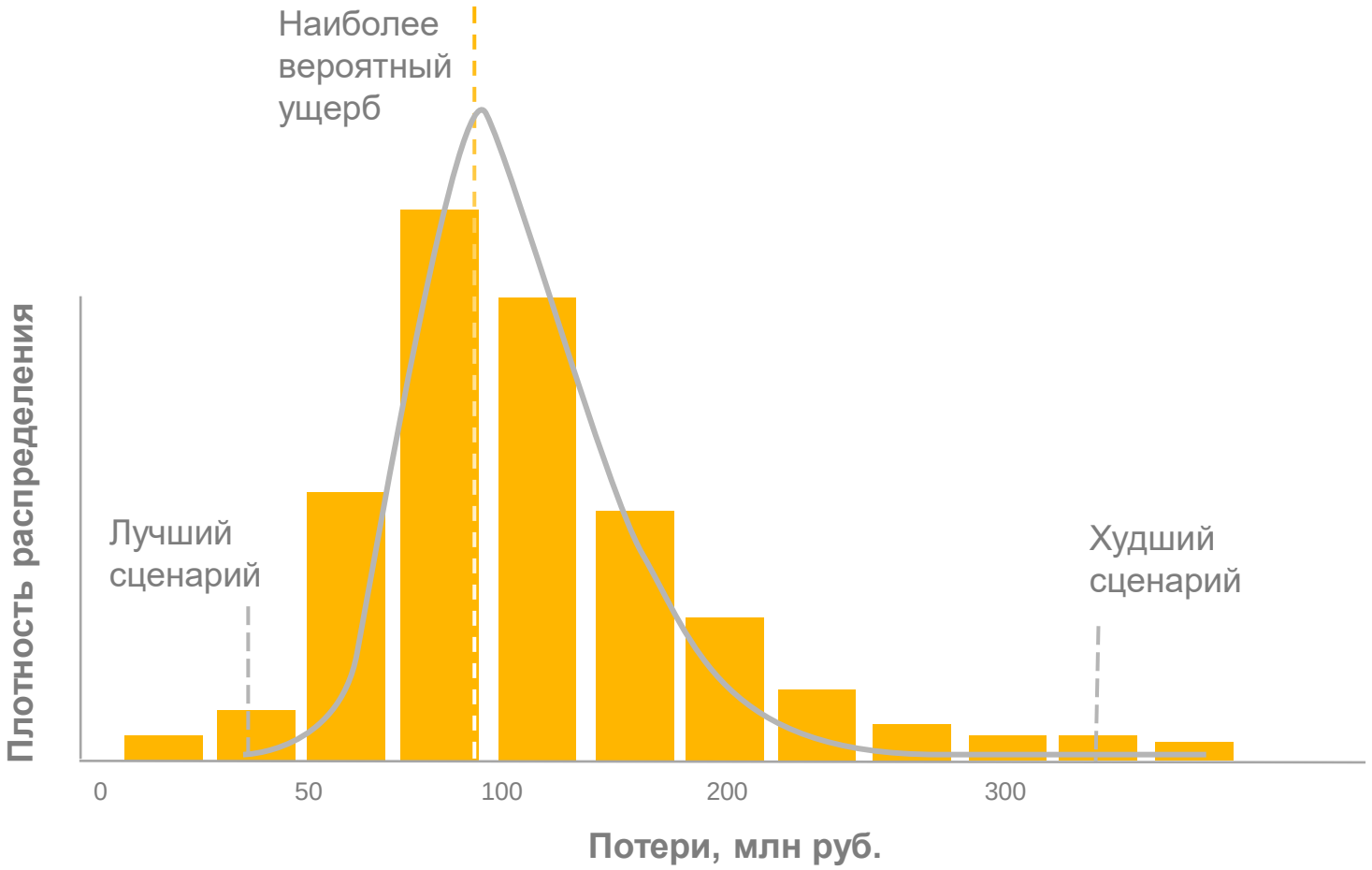
Внешние данные и статистика
по инцидентам и событиям ИБ

Моделирование по методу Монте-Карло

Логнормальное распределение

Теорема Байеса

Методы статистического анализа



Отражаем финансовую эффективность мер по снижению риска

Уровень расчётных среднегодовых потерь (ALE) на горизонте планирования 5 лет

737,0 млн руб.

Стоимость мер по снижению риска

128,0 млн руб. за 5 лет

Система DLP	**8,0**
Интеграция источников Threat Intelligence в SOC	**3,0**
Систем контроля привилегированного доступа	**5,0**

Уровень снижения риска

592,0 млн руб.

Остаточный уровень среднегодовых потерь (ALE)

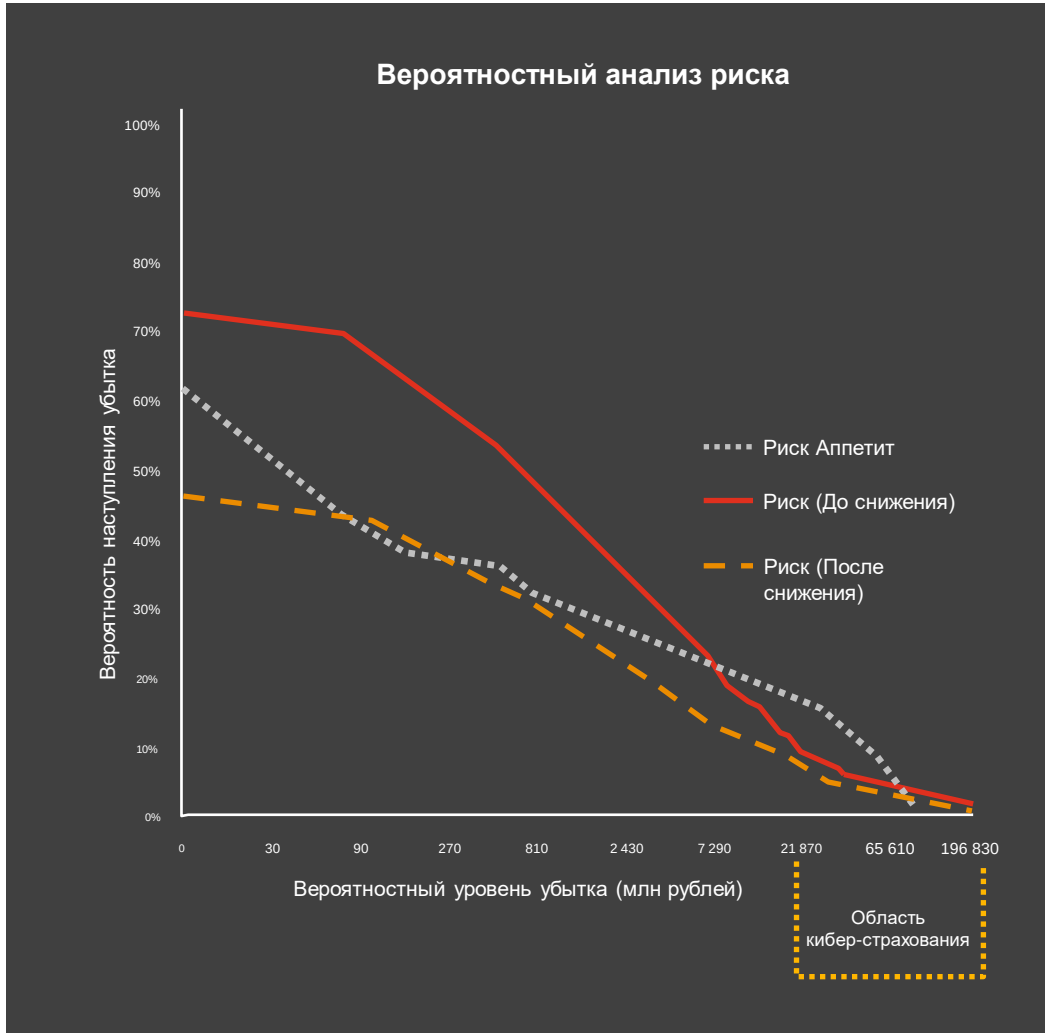
145,0 млн руб.

Возврат на инвестиции (ROSI)

592-128

128

= 362%



Цифровая панель управления киберрисками

Риски

Категория	Текущий уровень ALE (млн. руб.)*	Планируемый уровень ALE (млн. руб.)*	Изменение вероятности
Случайная утечка данных	45	36	-20%
Внешняя кибератака	180	104	-42%
Инсайдерская атака	180	83	-54%
Атака на цепочку поставок	80	72	-10%
DoS атака	120	108	-10%
Внешние манипуляции информацией	50	41	-18%
Атака на клиентов	110	35	-68%

*ALE (Annualised Loss Expectancy) – ожидаемый среднегодовой ущерб от события риска.

Ключевые контроли

Название	Тип*	Текущий	Планируемый	Цель
DevSecOps	P	2.0	3.8	4.0
Управление привилегированным доступом	P	2.0	2.3	4.0
Управление учетными записями	P	2.0	3.4	4.0
Аутентификация	P	2.0	2.6	3.5
Шифрование данных	P	2.0	3.2	4.0
Предотвращение потери данных	P	2.0	3.1	4.0
Культура безопасности и обучения	P	3.0	4.1	3.5
Непрерывный мониторинг	D	3.0	3.3	4.0
Анализ аномалий	D	4.0	4.1	4.5
Анализ угроз	D	3.0	2.9	3.5
Резервное копирование и восстановление данных	R	3.0	3.7	4.0
Управление кибер-кризисом	R	2.0	4.0	4.5
Реагирование на инцидент	R	4.0	4.4	4.5

*P - защита
D – обнаружение
R - восстановление

Завершен
По плану
Задержка
Проблемы
Не начат

Программа

Направление	Название	Статус*	Выгода	Стоимость
Управление доступом	Повторная сертификация доступа	●	11.2	£700K
Управление доступом	Надежная аутентификация	✓	9,0	£500K
Управление доступом	Управление привилегированным доступом	●	4.5	£100K
Управление доступом	Управление привилегиями на конечных точках	●	4.5	£800K
Безопасность данных	Надежный DPL электронной почты и фильтрация	●	1,6	£0K
Безопасность данных	Надежный веб-DPL и фильтрация	●	1,6	£150K
Управление доступом	Удаление учетных записей локальных администраторов	●	2.7	£20K
Безопасность данных	Минимизация данных	●	2.0	£100K
Безопасность данных	Предотвращение потери данных	●	18.0	£500K
Безоп. данных	Контроль доступа к сети	●	29.6	£800K
Безоп. данных	Сегментация сети	●	4.0	£800K
Безопасность конечного пользователя	Включение функции IDPS	●	1.6	£30K
Культура безопасности	Информационная кампания	●	0.8	£20K

Полученная выгода

7%

Выгода под риском

48%

Откуда берутся сложности?

У нас нет достаточного объема информации и статистических данных

У нас всегда больше данных, чем это необходимо для базовых вычислений

Это невозможно измерить и подсчитать

Если нечто имеет существенное значение для организации, его можно измерить и выразить в финансовых терминах

Мы не сможем подсчитать это с необходимой точностью

Точность вычислений не должна быть максимальной, ее должно быть достаточно для принятия решения

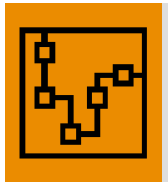
С чего начать?

Составить с владельцами ключевых бизнес процессов список недопустимых для бизнеса сценариев и оценить их ИТ и ИБ зависимость

Оценить степень интегрированности с процессом управления корпоративными рисками по методике, терминологии и таксономии риска

Выбрать фреймворк для оценки зрелости контролей ИБ, отвечающий контексту организации (ГОСТ, ISO 27000, ISF SoGP, NIST, CIS 20)

Составить план перехода на количественную оценку риска ИБ, оценив наличие необходимой поддержки, информации, ресурсов и знаний



Готовимся к поступательному развитию. Это не спринт, а марафон

Вопросы?

https://www.pwc.ru/cybersecurity

pwc.com