

Кибер Радар 360

инструмент для достижения стратегических целей



Вы готовы ответить на сложные вопросы и вызовы?

Насколько эффективно мы тратим ИБ-бюджеты? Действительно ли наши усилия помогают снизить риски и на сколько?

Какова финансовая отдача от наших вложений в ИБ? Помогает ли ИБ бизнесу или является просто статьей затрат?

В условиях недостатка бюджета, насколько мы уверены, что финансируем действительно приоритетные направления развития ИБ?



Можете ли вы обосновать бюджет на усиление ИБ с цифрами в руках?



Что мы можем сделать, для максимальной готовности к кибер инцидентам?

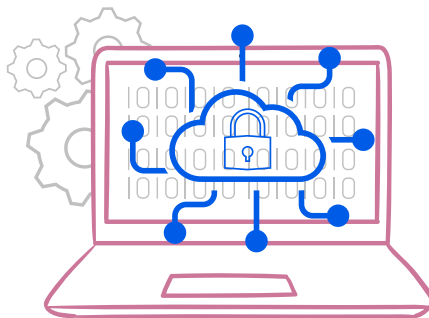


Насколько мы защищены от наиболее разрушительных сценариев киберинцидентов?

Достаточно ли зрел ваш процесс управления киберрисками?

Синхронизованное по риск-аппетиту управление киберрисками и стратегическими потребностями

Интегрированные в культуру организации и ее бизнес процессы требования кибербезопасности



Управление киберрисками используется в качестве движителя стратегии развития бизнеса, и управления доверием

Обеспечить доступ к качественной экспертизе и отчетности, необходимой для управления киберрисками

У нас есть ответ и мы всегда готовы прийти вам на помощь

Наш подход основан на реализации ключевых принципов, рекомендованных компанией PwC* директорам организаций, заинтересованных в построении зрелого процесса управления киберрисками.

Мы помогаем нашим клиентам сделать большой шаг от культурной модели «страх, неопределенность и сомнения», к связному и прозрачному восприятию профиля киберрисков Компании, позволяющему принимать финансово-оптимальные решения по управлению киберрисками.



Наша платформа по управлению киберрисками

- 1 Объединяет усилия ключевых игроков — советов директоров, владельцев рисков, менеджеров по ИБ и ИТ, для поддержки управления киберрисками.
- 2 Является единым центром отчетности и принятия решений по управлению киберрисками.
- 3 Обеспечивает переход к практике количественной оценки киберрисков, используя практичную и международно признанную методику количественной оценки, позволяющую учитывать финансовую отдачу от решений, принятых для минимизации киберриска.
- 4 Адаптирована к различным уровням зрелости и доступности необходимых данных.
- 5 Обладает возможностями, необходимыми для создания экосистемы управления рисками ИТ и непрерывности.
- 6 Гибкая — используется технология low-code (язык Power BI DAX), снижающая требования к навыкам программирования. Система может быть развернута локально или в виде SaaS-решения
- 7 Наполненная опытом и IP — мы не зависим от иностранного лицензирования и уже использовали нашу методику и инструментарий в нескольких крупных проектах
- 8 Прагматичная — наша модель данных подстраивается к уровню зрелости Клиента, связывает различные источники для достижения максимального результата



Мы реализуем современную и практичную методику

ОТОБРАТЬ

ОПИСАТЬ

РАССЧИТАТЬ

УПРАВЛЯТЬ

Критичные события риска

- Проанализировать контекст и бизнес-среду Компании
- Найти ИТ-зависимые компоненты бизнес-стратегии
- Выявить приоритетные кибер-события, способные нанести ущерб или нарушить стратегические планы

Сценарии инцидентов

- Определить степень агрессивности внешней среды
- Определить приоритетных агентов угрозы
- Определить приоритетные цели и пути атаки
- Определить способность контрольной среды противостоять приоритетным сценариям инцидентов

Симуляция и моделирование

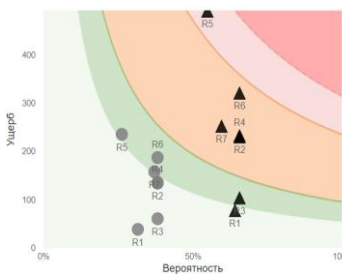
- Определить наиболее вероятные сценарии развития инцидентов
- Определить компоненты и размер ущерба
- Определить финансовые показатели и полный профиль риска

Решение и обработка

- Сравнить профиль риска с риск-аппетитом
- Определить снижаемые риски
- Сформировать программу по обработке рисков
- Детализировать инициативы по развитию контрольной среды
- Определить формат отчетности



Мы используем собственный инструментарий



Среднегодовой ожидаемый ущерб (ALE), млн. руб.	Риск-аппетит
76.95	✓
229.76	✗
103.06	✓
232.39	✗
491.27	✗
321.01	✗
252.22	✗

Имя	Категория	Риск	Важность	Степень	Степень	Степень	Степень	Степень	Степень	Степень	Степень
0001	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0002	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0003	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0004	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0005	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0006	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0007	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0008	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0009	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0010	Системное управление	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10

Инициатива	Процент выполнения	Степень	Степень	Степень	Степень	Степень	Степень	Степень	Степень	Степень	Степень
0001	64.1%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0002	63.6%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0003	61.1%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0004	61.8%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0005	54.9%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0006	54.5%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0007	59.6%	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10



Напишите нам, чтобы узнать о продукте и увидеть его демонстрацию



Дмитрий Шепелявый
Исполнительный директор направления «Цифровые продукты»

✉ dmitry.shepelyavy@tedo.ru



Михаил Толчельников
Руководитель направления «Управление киберрисками»

✉ mikhail.tolchelnikov@tedo.ru