

Риск-ориентированная стратегия и принципы управления стратегическими киберрисками

Июль 2022



О спикере



Михаил Толчельников

mikhail.tolchelnikov@tedo.ru

Старший менеджер практики анализа и контроля киберрисков с более чем 15 летним опытом работы. Занимал руководящие должности в международных компаниях из списка FTSE 100, сопровождая и поддерживая бизнес трансформации, цифровизацию и переходы на глобальный аутсорсинг.

В настоящий момент являюсь экспертом в областях:

- Методика и процесс количественной оценки киберрисков,
- Построение систем управления информационной безопасностью,
- Киберотчетность и измерение эффективности контрольной среды ИБ,
- Управление рисками в цепочке поставок.

Ключевые проекты:

- Построение процессов кибероперирования (СУИБ) для одного из мировых лидеров производства товаров бытовой химии и гигиены
- Подготовка к сертификации по требованиям ISO 27001 для одной из крупнейших металлургических компаний России и одного из лидеров энергогенерации
- Построение процесса количественной оценки киберриска в рамках рискориентированной стратегии развития ИБ для одного из Российских лидеров FMCG сегмента



SABSA Chartered Security Architect (SCF)

ISO/IEC 27001:2013 Lead Implementer

CISSP



Повестка



Увеличение стратегического значения киберрисков



Недостатки классических методов управления киберрисками



Принципы построения финансово эффективной стратегии управления киберрисками



Пять ключевых точек контроля



Киберриски способны оказывать стратегическое влияние



Стратегические Цели Компании

Увеличить EBITDA Компании на **20 млрд. руб.**

Расширить количество активных пользователей мобильных приложений до **30 млн.**

Увеличить **инвестиционную привлекательность** Компании



Киберриски

Операционная деятельность остановлена в ходе целенаправленной кибератаки

Сотрудник передал данные клиентов с целью поддержки хактивистов

Планы M&A и ранние отчеты о финансовых результатах украдены финансово мотивированным хакером



События операционного риска

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

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

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

Киберриски в структуре корпоративных рисков



Корпоративные риски



Нарушение контрактных обязательств



Введение регуляторных ограничений и штрафов



Увеличение санкционного давления



Изменение стоимости привлечения и удержания клиентов



Снижение финансовых показателей стратегических инициатив

Недопустимые бизнес события



Остановка непрерывного производственного процесса



Технологическая авария



Необходимость увеличить финансовые резервы



Необходимость увеличить финансовые резервы



Нанесение вреда здоровью



Снижение цифрового доверия

События киберриска



Массовая утечка персональных данных



Атака вируса-шифровальщика



Целенаправленная кибератака

Классический подход к управлению киберрисками



Направлены ли наши усилия на улучшение ключевых возможностей противодействия угрозам?

Тратим ли мы на нашу программу по снижению профиля киберрисков достаточные средства?

Можем ли мы показать ценность и финансовую эффективность нашей программы по снижению профиля киберриска?

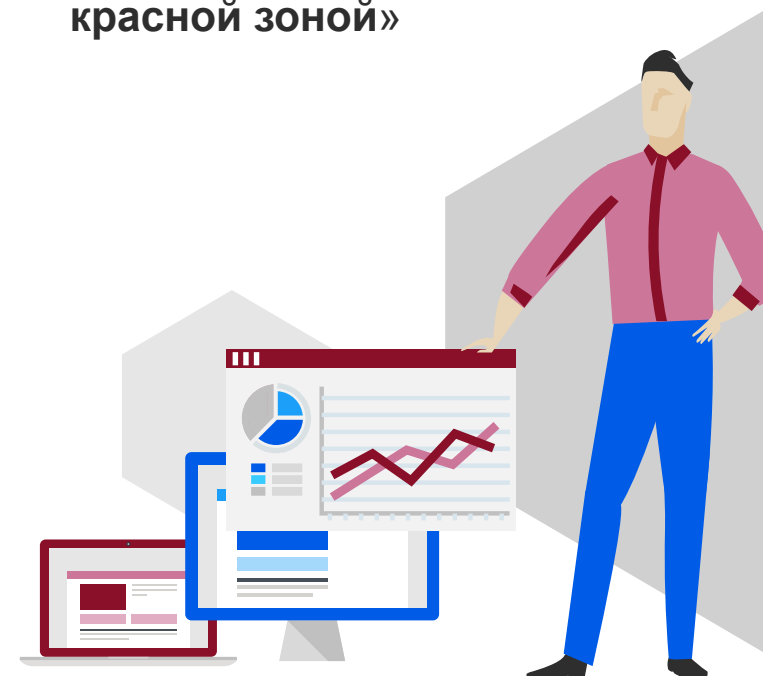
Какой уровень потерь мы можем прогнозировать, исходя из текущего уровня подверженности киберриску?

Насколько материален текущий уровень киберриска для нашей организации?

Достаточно ли усилий мы направляем на управление профилем киберриска?



«В текущем квартале **расходы на ИБ возросли на 500 тыс. руб.**, что позволило перевести два риска в зеленую зону, при этом, общий профиль рисков ИБ **остался на границе с красной зоной**»



Классические методы управления киберрисками перестали отвечать потребностям бизнеса



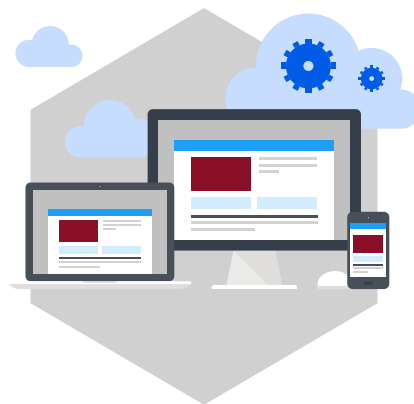
Отчетность

Большинство* Советов Директоров считают отчеты по профилю киберриска слишком техническими и имеющими слабый фокус на демонстрации количественного ущерба для бизнеса. Слабая поддержка отчетов финансовыми метриками также оказывает влияние на качество диалога и принятия решений.



Управление

В цифровой экономике невозможно снизить киберриск до нуля, поэтому критичную важность приобретает возможность управлять недопустимыми событиями, фокусируя усилия на снижение их материальности. Целью управления профилем киберриска становится поиск оптимального для организации соотношения затрат на ИБ и возможных потерь от киберинцидентов.



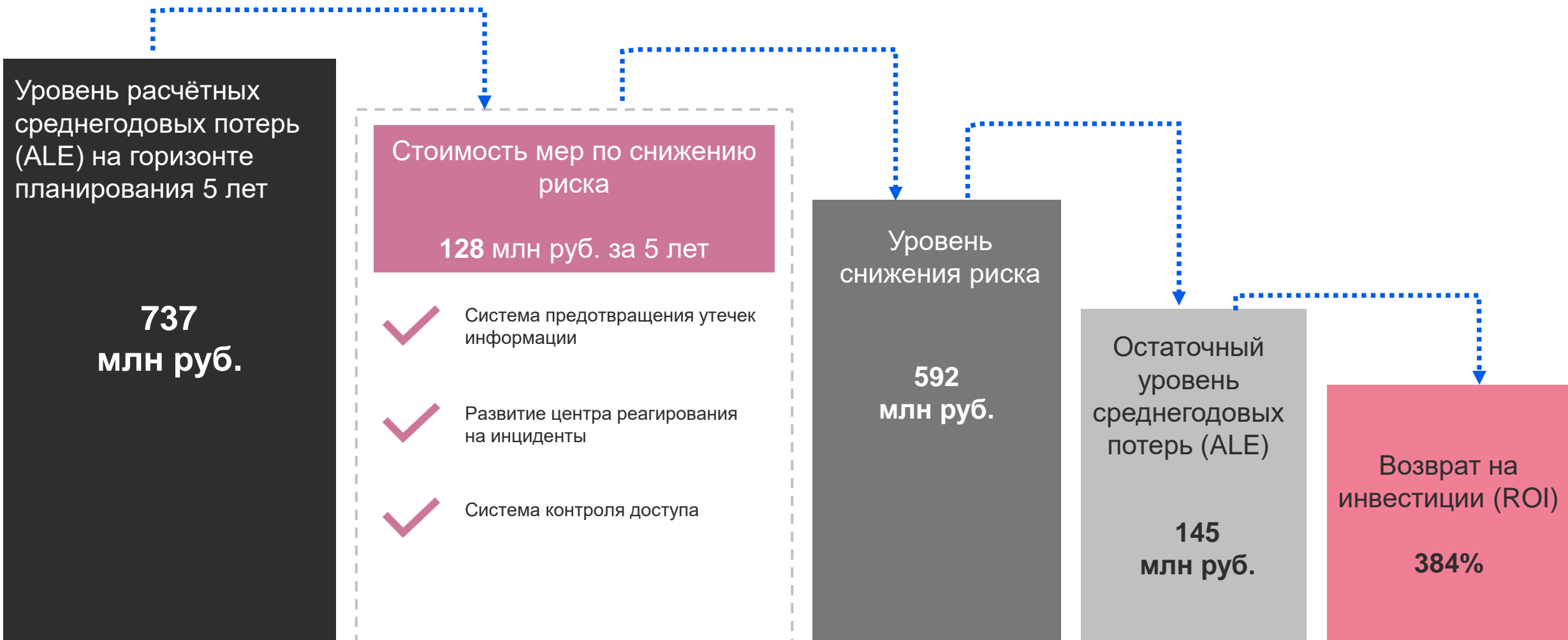
Эффективность

Бюджеты на кибербезопасность будут расти на 10% в год до 2027*, при этом, большинство финансовых директоров не получают прозрачной информации об эффективном их расходовании. Это не позволяет принимать информированные решения об изменении финансирования для поддержки стратегических инициатив по развитию бизнеса.



* Согласно опросам компании McKinsey

Количественный подход к управлению киберрисками



Риск ориентированная стратегия управления киберрисками



Компания А

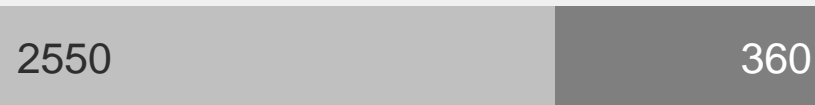
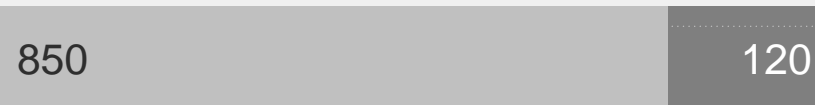
2015 год



2016 год



2017 год



Компания Б

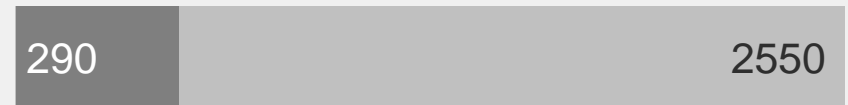
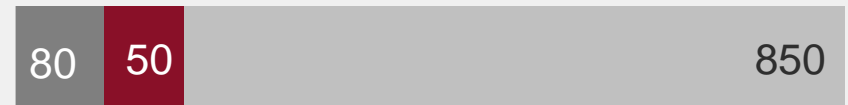
2015 год



2016 год



2017 год



Доход компании Затраты на ИБ Ущерб от инцидента

Шесть принципов управления киберрисками*

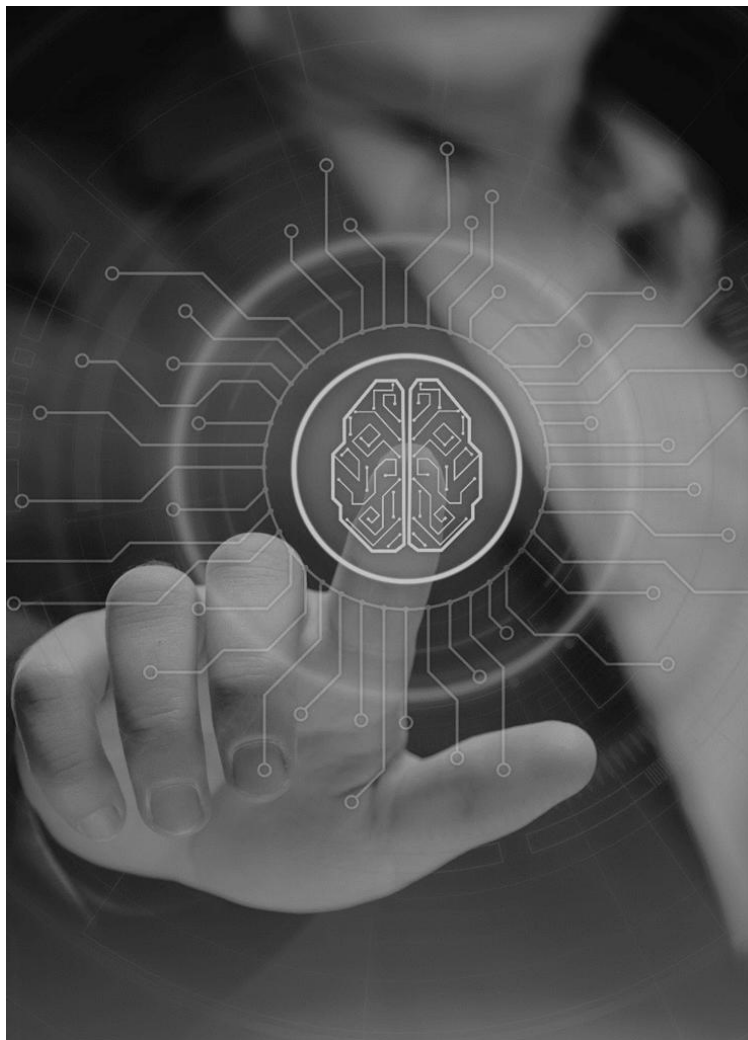


Принятие кибербезопасности в качестве движителя стратегии развития бизнеса

Понимание потерь и влияния киберрисков на экономику бизнеса, включая правовые последствия

Совет директоров имеет доступ к качественной экспертизе и выделяет достаточное время на обсуждение вопросов управления киберрисками

Интеграция требований кибербезопасности в организационную структуру и культуру организации



Синхронизация управления киберрисками с потребностями бизнеса

Адекватный фреймворк по управлению киберриском должен быть установлен на уровне предприятия и обеспечен достаточными ресурсами для функционирования

Приветствие и поддержка развития системной устойчивости и совместной работы

* National Association of Corporate Directors, Principles for Board Governance of Cyber Risk, MARCH 2021

Пять точек контроля зрелости



Аппетит к киберриску оценен количественно



Определены ключевые стратегические сценарии и события риска



Принят набор финансово эффективных мер, необходимых для оптимизации профиля киберрисков



Применяется зрелая методика количественной оценки, поддержанная инструментами автоматизации



Руководство открыто демонстрирует поддержку и доверие CISO

Передовые инструменты поддержки

Кибер Радар 360 - поддержка принятия финансово эффективных решений по управлению киберрисками

Профиль киберриска

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

Приборная панель демонстрирующая профиль киберриска и динамику его снижения для управляющего звена и директоров

Сценарный анализ

Интерактивная карта зависимостей рисков, агентов угрозы, элементов контрольной среды и метрик, позволяющая получить ценные инсайты

Площадь атаки

Комплексное представление о площади атаки и эффективности контрольной среды ИБ (метрики)

Анализ контрольной среды

Визуализация возможностей реализации различных сценариев событий риска для ключевых агентов угрозы

Проблематика

Измерение и описание профиля киберрисков непростая задача для большинства организаций. Особенно для тех, менеджмент которых имеет высокий интерес к той области и зрелые запросы:

- Какие еще усилия мы должны сделать для достижения нужного уровня защищенности?
- Насколько реальны направленные на нас угрозы?
- Защищены ли мы в достаточной для нас степени?
- Инвестиции в какие элементы контрольной среды приведут к наибольшему снижению риска?

Наше решение

Наш продукт создан прагматичным, позволяющим сфокусироваться на ключевых рисках и компонентах контрольной среды, реализуя при этом количественную оценку профиля киберриска.

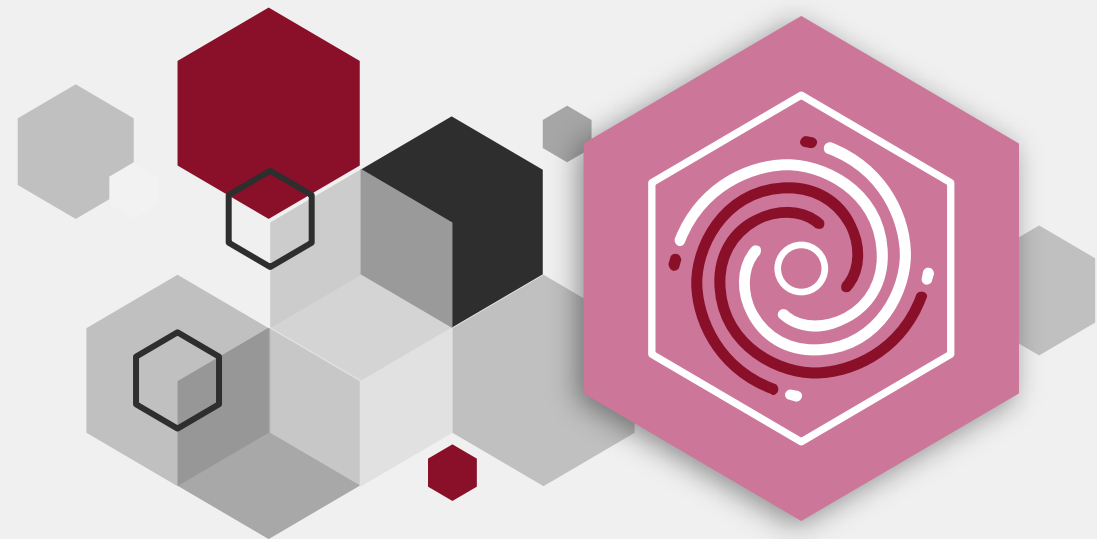
- Использовать проверенные прагматичные модели данных и каталоги
- Готовые приборные панели по рискам, реализованные в Power BI
- Возможность интеграции с существующими в компании инструментами отчетности по рискам
- Возможность облачного размещения сервиса

В нашем подходе мы используем стандартизированные элементы процесса, которые можно использовать без существенной доработки, построенные исходя из лучших практик и нашего опыта.

Наш продукт содержит полноценные каталоги агентов угроз, типов киберрисков, компонентов контрольной среды, а также метрики и готовые сценарии событий риска, дополненные прагматичным подходом по их оценке. Это позволяет собирать приборные доски по киберриску, детальность которых можно наращивать с ростом количества получаемых данных, дополняя их возможностями мониторинга в реальном времени. Мы используем Microsoft Power BI в качестве доступной платформы, позволяющей легко адаптировать продукт под нужды заказчика.

Вопросы?

tedo.ru



«Технологии Доверия» (www.tedo.ru) предоставляет аудиторские и консультационные услуги компаниям разных отраслей. В офисах «Технологий Доверия» в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже, Владикавказе, Перми и Нижнем Новгороде работают 3 700 специалистов. Мы используем свои знания, богатый опыт и творческий подход для разработки практических советов и решений, открывающих новые перспективы для бизнеса.

Драйверы перехода и цели проекта



Драйверы

Прямые требования руководства компании

Низкая зрелость методики выявления, оценки и управления киберрисками

Слабая интегрированность процесса управления киберрисками в процесс управления рисками операционной деятельности

Процесс моделирования финансовой эффективности мер по улучшению контрольной среды ИБ требует улучшения

Низкая зрелость отчетности о профиле киберрисков и эффективности контрольной среды

Сложность оценки реальности направленных на нас угроз и достаточности имеющегося уровня защиты

Отсутствие элементов автоматизации процесса управления профилем киберриска и создания отчетности



Цели и задачи проекта

Улучшение качества принятия решений по управлению профилем рисков кибербезопасности путем запуска процесса количественной оценки киберрисков на базе автоматизированной платформы по управлению киберрисками

Создание инструмента создания финансово оптимального набора инициатив для развития контрольной среды ИБ путем анализа финансовой эффективности внедрения отдельных средств защиты, для обеспечения оптимального баланса остаточных киберрисков и затрат на их минимизацию

Создание возможности для демонстрации материальной и контролируемой связи текущего уровня зрелости контрольной среды ИБ с вероятностью и масштабом наступления критичных событий киберриска

Создание платформы, позволяющей демонстрировать клиентам, партнерам и руководству организации высокую степень заботы о сохранности данных и защите технологических процессов от современных киберугроз

Ценность и факторы успеха проекта



Факторы успеха

Фокус на узкий набор недопустимых событий, способных повлиять на стратегические цели организации

Расширенное обучение методике и процессу количественной оценки киберрисков для ключевых заинтересованных сторон на первых стадиях проекта

Заинтересованность в результате при принятии факторов, ограничивающих методику

Вовлечение в процесс ключевых заинтересованных сторон (руководство, корпоративные риски, ИТ и ИБ)



Ресурсы и данные

Использование методов экспресс-оценки основных компонентов процесса (профиль компании, агенты угрозы, зрелость контрольной среды, компоненты ущерба) не потребует существенных усилий по исследованию, аудиту и сбору информации

Максимальное использование готовых каталогов и справочников облегчает запуск процесса

Для старта потребуется только минимальный, немедленно-доступный набор исторических и операционных данных

Проекту потребуется вовлеченность экспертов ИТ, ИБ, а также доступ к среднему менеджменту компании

Потребуется высокая вовлеченность владельца процесса (спонсор проекта)

Почему «Кибер Радар 360»?



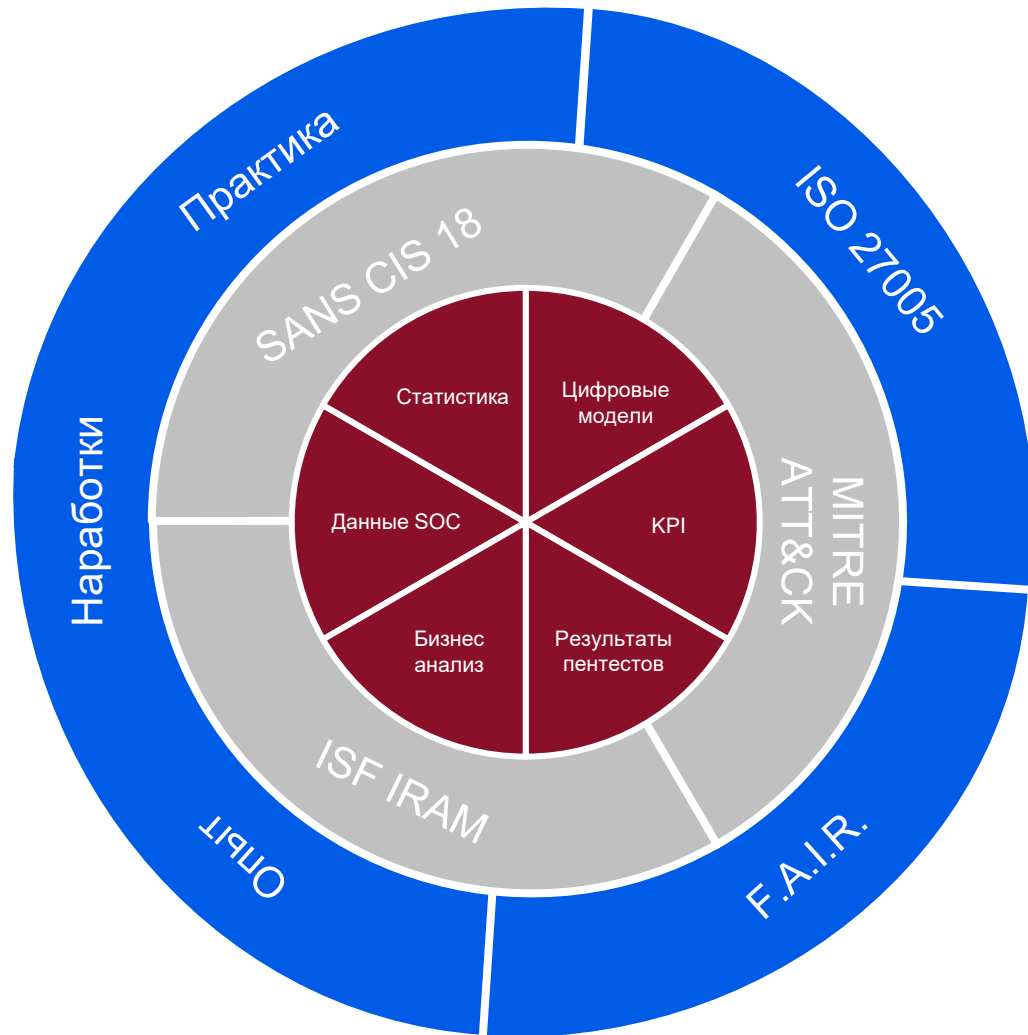
Преимущества

- Наш продукт создан прагматичным, позволяющим сфокусироваться на ключевых рисках и компонентах контрольной среды, реализуя при этом количественную оценку профиля киберриска
- Используем эволюционный подход к внедрению процесса, начиная с минимального набора абсолютно доступных данных
- Мы используем стандартизированные элементы процесса, построенные исходя из лучших практик и нашего опыта, которые можно использовать без существенной доработки
- Мы используем проверенные прагматичные модели данных и каталоги агентов угроз, типов киберрисков, компонентов контрольной среды, а также метрики и готовые сценарии событий риска, дополненные прагматичным подходом по их оценке
- Предоставляем готовый набор приборных панелей по рискам, реализованные в Power BI
- Использование Microsoft Power BI в связке с Excel позволяет быстро адаптировать продукт под нужды заказчика и оставляет заказчику возможность доработок платформы

Таксономия киберриска



Наш подход к количественной оценке киберрисков

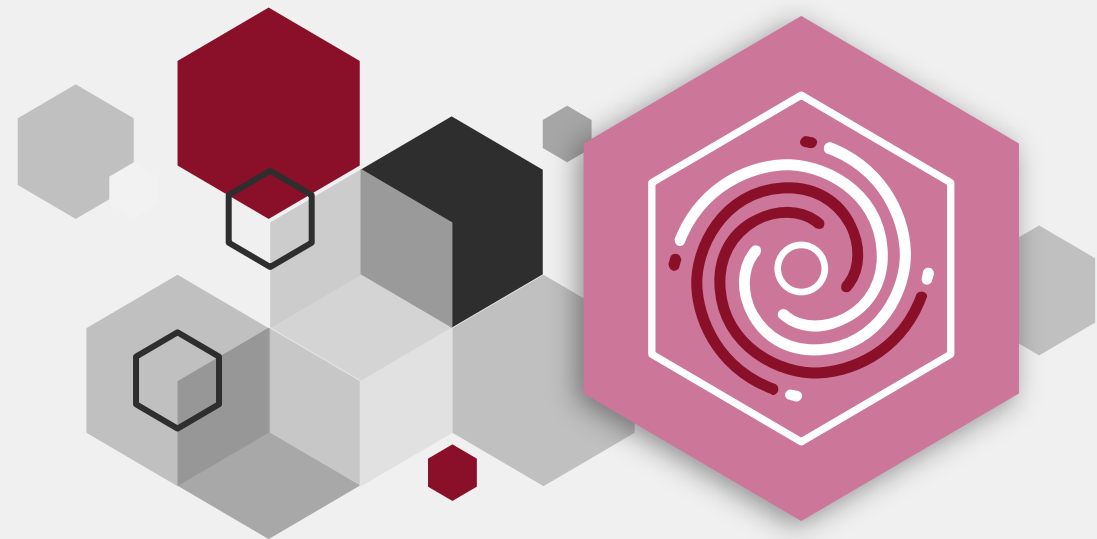


Использование международно признанных методик и стандартов позволяет построить надежный фундамент процесса, дополняя их наработанной практикой и опытом, применимым для российских условий.

- FAIR (Factor Analysis of Information Risk) – методика Value at Risk (VaR), применяемой для моделирования финансовых рисков, адаптированная FAIR Institute для процесса количественной оценки киберрисков. Методика формирует единый подход к управлению киберриском, подходящий как для управляющих менеджеров, так и для сотрудников ИТ и ИБ, позволяя измерять, управлять и создавать отчетность по профилю киберриска.
- ISO 27005 – ключевой компонент серии ISO27000, являющейся международным стандартом по построению СУИБ. Стандарт описывает лучшую практику дизайна, построения и применения процесса управления киберрисками в организациях любого масштаба.
- SANS CIS18 – методика, разработанная SANS Institute, позволяющая оценивать архитектуру и зрелость компонентов контрольной среды ИБ, выстраивая мост между управляющими фреймворками уровня ISO 27000 и NIST. CIS18 позволяет организациям оценивать киберустойчивость, выявляя наиболее слабые компоненты контрольной среды в триаде «люди, процессы, технологии».
- MITRE ATT&CK – регулярно обновляемый сборник техник и тактик, применяемых реальными агентами киберугрозы. ATT&CK применяется, как общепризнанная база знаний, для разработки моделей угроз и моделирования кибератак.

Вопросы?

tedo.ru



«Технологии Доверия» (www.tedo.ru) предоставляет аудиторские и консультационные услуги компаниям разных отраслей. В офисах «Технологий Доверия» в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже, Владикавказе, Перми и Нижнем Новгороде работают 3 700 специалистов. Мы используем свои знания, богатый опыт и творческий подход для разработки практических советов и решений, открывающих новые перспективы для бизнеса.