# Принципы управления кибер рисками для стратегического руководства организации

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:

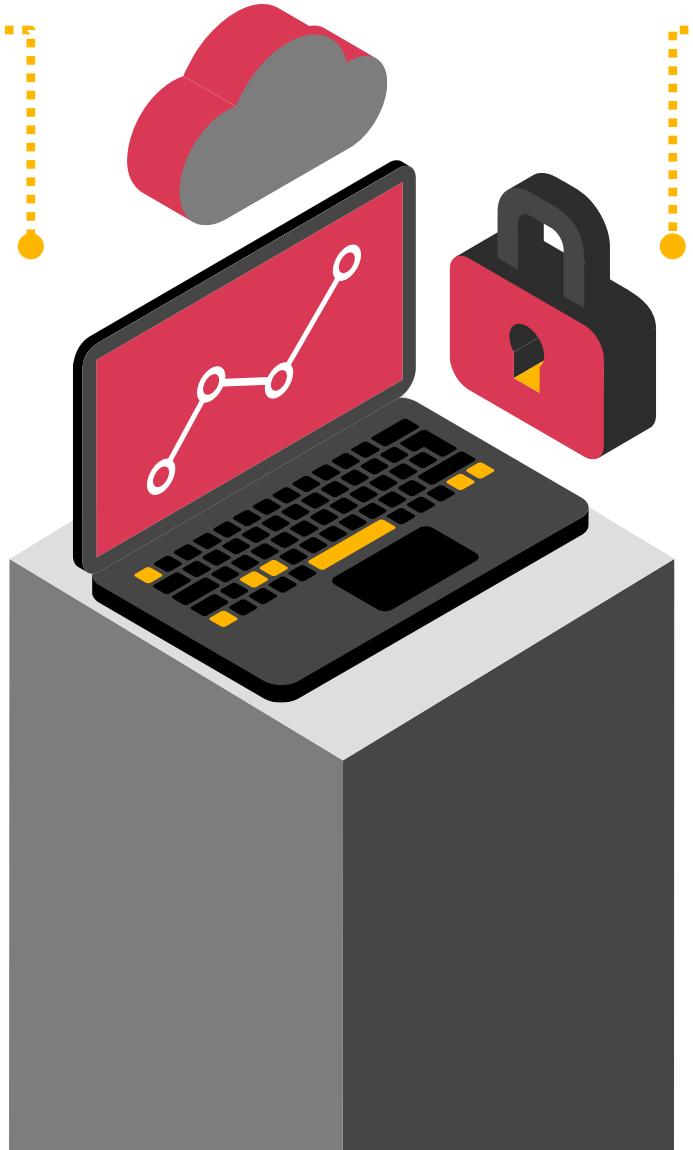
- Управление и количественная оценка кибер рисков,
- Построение систем управления информационной безопасностью,
- Отчетность и измерение эффективности контрольной среды ИБ,
- Управление рисками в цепочке поставок.

# Принципы управления киберрисками для Совета Директоров*

Принятие кибер безопасности в качестве движителя стратегии развития бизнеса
Понимание потерь и влияния кибер рисков на экономику бизнеса, включая правовые последствия

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

Интеграция требований кибер безопасности в организационную структуру и культуру организации



Синхронизация управления кибер рисками с потребностями бизнеса

Адекватный фреймворк по управлению кибер риском 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

# PwC - Global Digital Trust Insights 2022*

4 организации из 10 отмечают существенный прогресс, который они достигли за последние два года, в **ключевых областях кибер развития**:

- Построение культуры, основанной на принципах безопасности
- Управление кибер рисками
- Развитие коммуникации между менеджментом и советом директоров
- Выравнивание целей бизнеса и кибер безопасности

Управляющие директора считают, что они предоставляют «существенную» поддержку развития ИБ, при этом только 3 из 10 функционеров ИБ с ними согласны.

75% руководителей компаний оценивают организационную и структурную сложность как «тревожный» фактор роста кибер рисков и связанных с ними потенциальных потерь.

Службы ИБ в организациях, использующих наиболее продвинутые практики в построении экосистемы безопасности, обеспечении доверия к данным и вовлечению руководства, в два раза чаще достигали существенного прогресса в **ключевых областях кибер развития**.

Миссия кибер безопасности смещается в область развития доверия и обеспечения устойчивого развития бизнеса

Более половины компаний не имеют представления и не занимаются активным управлением кибер рисками, связанными с третьими лицами и цепочками поставок.

В 2022 году управляющие директора ожидают роста кибер атак и связанных с ними инцидентов.



* 2022 Global Digital Trust Insights проведенный компанией PwC в Августе 2021 опрос, в котором приняли участие 3,602 корпоративных управленцев высшего звена (CEOs, корпоративные директора, CFOs, CISOs, CIOs). Женщины составили 33% выборки.

# Понимание влияния кибер рисков на экономику бизнеса

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

# Кибер безопасности как движитель стратегии

| Стратегическая Цель | Кибер риск | Влияние на достижение цели |
|---|---|---|
| Увеличить EBITDA Компании на 20 млрд. руб. | Остановка операционной деятельности в ходе кибер атаки | Длительный срок восстановления после атаки привел к снижению выручки на 65% на время инцидента |
| Расширить количество активных пользователей мобильных приложений до 30 млн. | Регулярные утечки пользовательских данных приводят к снижению рейтинга мобильных приложений и оттоку пользователей | От 6% до 10% активных пользователей удалили мобильные приложения после новостей о взломе и краже данных |
| Увеличить инвестиционную привлекательность Компании | Планы M&A и ранние отчеты о финансовых результатах стали доступны злоумышленникам | Изменение условий M&A привело к снижению привлекательности сделки.<br>Стоимость акций снизилась на фоне заявлений об инсайдерской торговле |

# Развитие системной устойчивости и интегрированности

## Ключевые приоритеты бизнеса

- Технологическое лидерство
- Оптимизация затрат и повышение эффективности процессов
- Опора на данные, знания и доверие

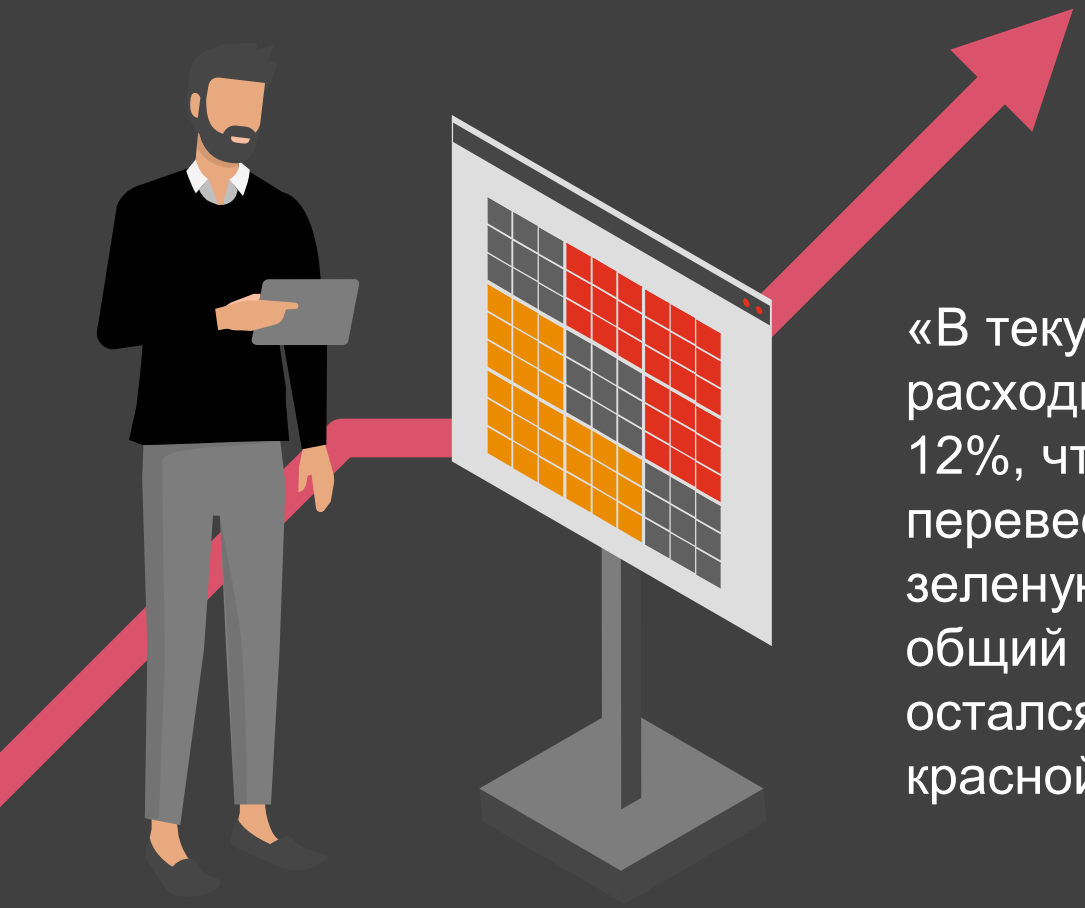
## Приоритеты развития ИТ

- Устранение инфраструктурных преград
- Автоматизация производственного процесса
- Создание лучшего клиентского опыта
- Инфраструктура как сервис (IaaS) и инфраструктурные платформы как сервис (PaaS)
- Повышение доступности ключевых информационных сервисов
- Глубокий анализ клиентских данных

## Приоритеты развития ИБ

- Снижение влияния ИБ на скорости изменения бизнеса
- Защита клиентских данных и цифровых активов
- Стандартизация и оптимизация контрольной среды
- Удержание кибер рисков на уровне риск-аппетита

# Совет директоров имеет доступ к качественной экспертизе



«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»

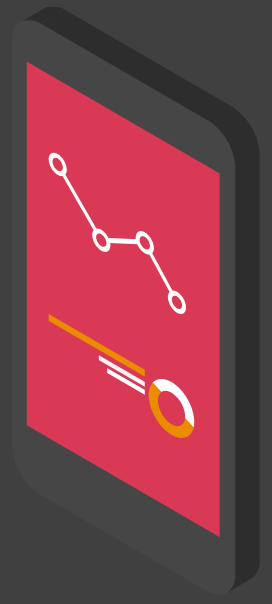
# Синхронизация рисков и потребностей бизнеса

**Оптимизируем реакцию под потенциальный ущерб и критичность бизнес инициативы:**

- Принятие риска;
- Отказ от риска;
- Снижение риска;
- Передача риска другой стороне;

---

- Увеличение риска

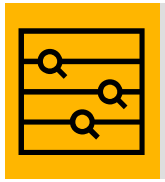


**Оптимизируем финансирование под риск-аппетит и контекст бизнес инициативы:**

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

# Что директор может сделать для улучшения ситуации

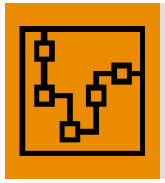
Определите ваш аппетит к кибер риску и начните оценивать его в количественных терминах



Определите ключевые риски, связанные с кибер угрозами и компромиссы «риск-ценность» в вашей стратегии цифрового развития

Признайте наличие кибер рисков и связанных с ними проблем, и принимайте необходимые для их минимизации решения

Обозначайте кибер безопасность как ключевое условие дельнейшего роста компании и улучшения доверия клиентов и инвесторов



Открыто демонстрируйте вашу поддержку и доверие CISO

# Вопросы?

https://www.pwc.ru/cybersecurity

pwc.com