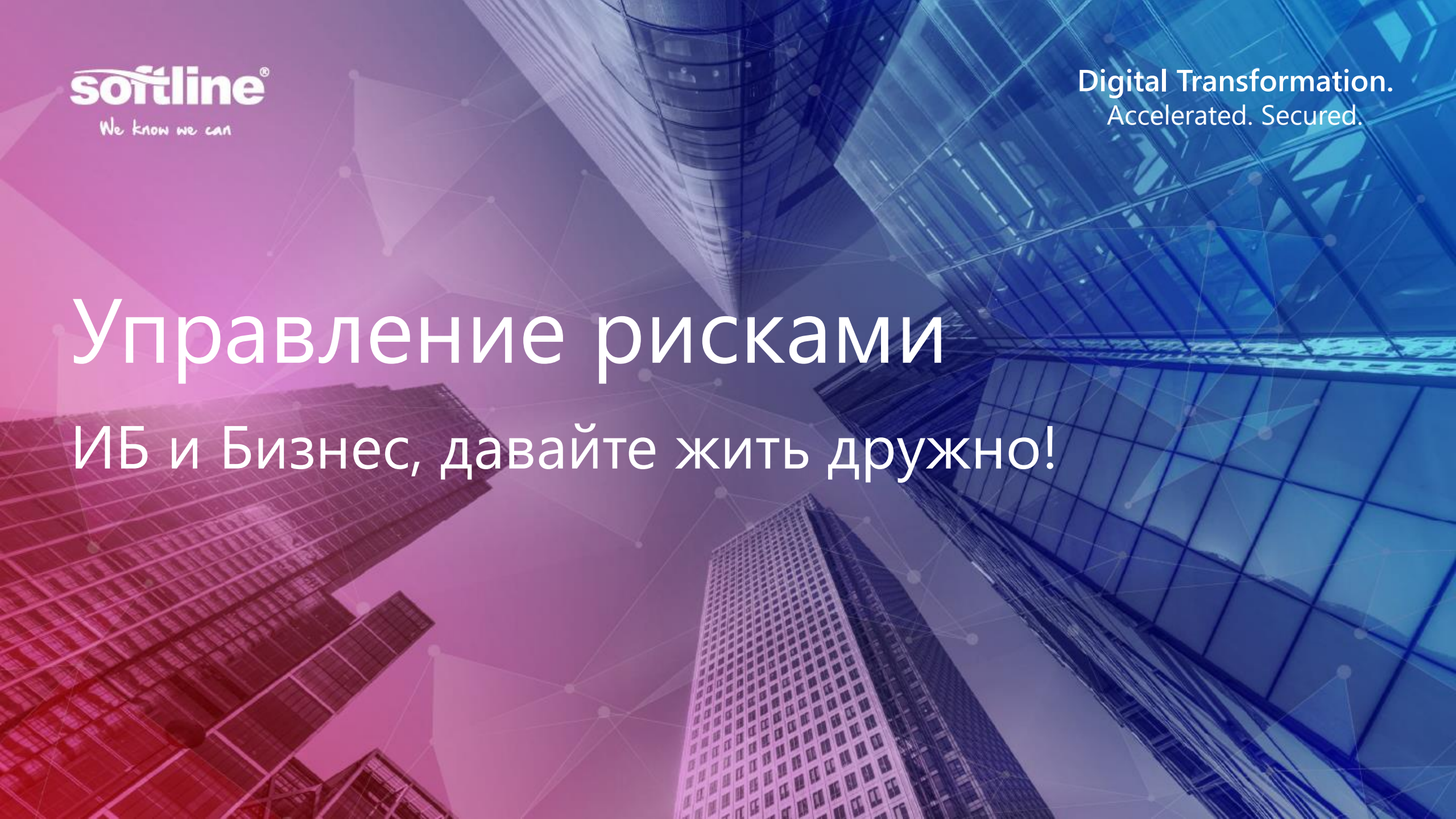
softline
We know we can
Digital Transformation.
Accelerated. Secured.
Управление рисками
ИБ и Бизнес, давайте жить дружно!

Тенденции кибербезопасности в России

Digital Transformation.
Accelerated. Secured.

98%
Составил рост хакерских атак на российские компании в 2022 г.

72%
Российских компаний не готовы увеличивать бюджет на ИБ в 2023 г.

56%
Средний показатель “защищенности” российских компаний

«Бережливая безопасность» - рациональное использование ресурсов для защиты действительно важных бизнес-активов

Зачем нужны эти ваши «риски»?

1. Определить ключевые ИТ-активы и защищать их в первую очередь

2. Учитывать изменения в бизнес-процессах и тренды в сфере кибербезопасности

3. Показать, сколько может стоить для бизнеса кибератака, если не инвестировать в ИБ

4. Обосновать траты на ИБ и разговаривать с бизнесом на понятном ему языке

Когда нужны эти ваши «риски»?

1. «Переросли» комплаенс, и нужно понять, что дальше делать?

2. CISO требуется обоснование бюджета.

3. Требование «сверху»: стейкхолдеры заинтересованы в управлении рисками (и риски ИБ как часть общих рисков Компании)

Почему «риски» важны?

Инцидент ИБ может «уничтожить» бизнес

Контекст меняется, ресурсы ограничены - что защищать в первую очередь?

Безопасность должна быть выгодна для Бизнеса

Как это в текущий момент?

Инцидент ИБ может «уничтожить» бизнес	→	Никогда не болело и не будет, а значит всё у нас и так нормально
Контекст меняется, ресурсы ограничены - что защищать в первую очередь?	→	Если (когда) заболит, тогда и будем лечить
Безопасность должна быть выгодна для Бизнеса	→	ИБ просит «много денег» – Бизнес дает «мало денег»

Как это должно быть?

Digital Transformation.
Accelerated. Secured.

Инцидент ИБ может «уничтожить» бизнес	Никогда не болело и не будет, а значит всё у нас и так нормально	Мы знаем, что «болит» у Бизнеса
Контекст меняется, ресурсы ограничены - что защищать в первую очередь?	Если (когда) заболит, тогда и будем лечить	Мы всегда знаем, что важно для Бизнеса
Безопасность должна быть выгодна для Бизнеса	ИБ просит «много денег» – Бизнес дает «мало денег»	Бизнес участвует в принятии решений по ключевым рискам

Везде «Бизнес»

А в чем коренная* причина?

Причина разногласий – недостаток коммуникаций!

*не «корневая»

А в чем коренная* причина?

Причина разногласий – недостаток коммуникаций!

*не «корневая»

Как считать риски?
Есть ровно «мильён» разных подходов

1. Риск считаем:
- 1.1 качественно
- 1.2 полуколичественно
- 1.3 количественно

2. Подход к рискам:
- 2.1 активоориентированный
- 2.2 рискоориентированный

3. Риск состоит из:
- 3.1 двух факторов *(вероятность, ущерб)*
- 3.2 трех факторов *(+эффективность)*
- 3.3 четверых факторов *(+уязвимость)*

4. Факторы определяются:
- 4.1 экспертно на верхнем уровне
- 4.2 декомпозицией на 2-4 уровня «вниз»
- 4.3 сложный математический аппарат

А еще есть умные книжки:

1. ISO 31010 «Risk management - Risk assessment techniques»
2. ISO/IEC 27005 «Information technology - Security techniques - Information security risk management»
3. Open FAIR™ Risk Analysis
4. NIST SP 800-30 Guide for Conducting Risk Assessments
5. ~~Методика оценки угроз ИБ ФСТЭК России~~

+ не забудьте требования от корпоративных рисков!

Практика оценки рисков – топ проблем

1. Перфекционизм
2. Самоуверенность
3. Вовлеченность
4. Масштабность

Практика оценки рисков: 1. Перфекционизм

«Если делать, то делать идеально» (с) CISO

а) сразу интегрируем «риски ИБ» с другими процессами;

б) оценим риски сразу для всего и вся;

в) и вообще будем планово риски пересматривать не раз в год, а раз в квартал;

г) а еще для всех рисков КИР(ы)* придумаем.

Выход: кушать слона по частям. Начать с «базы» и выстроить план развития на 2-3 года вперед.

*Ключевые индикаторы риска

Практика оценки рисков: 2. Самоуверенность

Digital Transformation.
Accelerated. Secured.

«Не надо никуда ходить, я сам вам всё расскажу» (с) CISO

а) про главные страхи Бизнеса;

б) про связанные ресурсы и их критичность;

в) про контрольные мероприятия;

г) про то, что нужно сделать с рисками.

Интернет-магазин:

№	ИБ	Бизнес
1	Утечка ПДн клиентов	Перебои в работе системы исполнения заказов
2	Утечка информации о себестоимости	Нарушение логистики
3	Нарушение работы сайта	Утечка ПДн клиентов

Выход: спросить «кого-то» еще. Например:

а, б, г – Бизнес
в – ИТ, юристов

Практика оценки рисков: 3. Вовлеченность

«Риски ИБ – это забота подразделения ИБ, зачем вы к нам пришли?» (с) Бизнес

а) мы тут деньги зарабатываем, а вы нас отвлекаете;

б) мы не понимаем, что вы хотите;

в) вы каждый год будете с этим приходить?

Выход: донести важность процесса, разложить задачи Бизнеса до атомарных действий, повторить минимум 2 раза.

Практика оценки рисков: 4. Масштабность

«Наши возможности ограничены возможностями экселя». При этом:

а) у нас существенное количество бизнес-процессов и активов;

б) необходимо встроить «риски» в операционную деятельность;

в) необходимо оперативно реагировать на изменения контекста Бизнеса;

г) хотим внедрить иные инструменты оценки рисков: самооценка, КИР;

д) необходимо рационально использовать ресурсы (помним про «бережливость»).

Выход: автоматизировать процессы управления (не только рисками и не только ИБ), например, с помощью систем класса SGRC*.

*Security Governance, Risk, Compliance

«Побочные эффекты» оценки рисков ИБ

Вы *ещё лучше* знаете, чем живет Бизнес и как именно Компания зарабатывает деньги

Бизнес вовлекается в принятие решений:

- поддерживает Вас при реализации мер ИБ и защите бюджета;
- принимает на себя часть ответственности.

Бизнес начинает догадываться, чем *на самом деле* занимается подразделение ИБ.

Оценка рисков – шаг в сторону зрелой стратегии ИБ.

Как мы проводим оценку рисков?

Digital Transformation.
Accelerated. Secured.

1 ОПРЕДЕЛЕНИЕ ОБЛАСТИ

0,5 месяца

Результат

1. Область оценки рисков ИБ - критичные направления бизнеса

2 ФОРМАЛИЗАЦИЯ ПРОЦЕССА

1-2 месяца

Результат

1. Методика оценки рисков ИБ, включая критерии оценки и порядок ее проведения (кто, что, как, в каком порядке)

3 ОБСЛЕДОВАНИЕ

1-2 месяца

Результат

1. Недопустимые события и связанные бизнес-метрики
2. Перечень защищаемых активов
3. Оценка процессов и мер обеспечения ИБ

4 ОЦЕНКА РИСКОВ

1-3 месяца

Результат

1. Сценарии реализации рисков и оценка последствий
2. Реестр рисков ИБ с указанием их величины и владельцев

5 ОБРАБОТКА РИСКОВ

1 месяц

Результат

1. Описание мероприятий по совершенствованию процессов и мер обеспечения ИБ
2. Дорожная карта реализации мероприятий

6 ИНФОРМИРОВАНИЕ

Результат

1. Отчет для руководства по результатам оценки рисков ИБ

We know we can

softline®

We know we can

Digital Transformation.

Accelerated. Secured.

Чуриков Алексей
Руководитель экспертной группы
АО «Технический центр «Инженер» ГК Softline
+7 (495) 761 71 46
info@tc-engineer.ru