



Как добиться экономической эффективности при построении системы защиты АСУ ТП



Дмитрий Ильин

Директор по продажам Group-IB

ЭФФЕКТИВНАЯ ИБ ПОЗВОЛЯЕТ БИЗНЕСУ ЗАРАБАТЫВАТЬ БОЛЬШЕ

Грамотное управление киберрисками, эффективное расходование бюджета на ИБ сокращает недополученную прибыль и позволяет бизнесу получать больше денег. Больше денег у бизнеса – больше денег у ИБ, выше зрелость.

Этапы ИБ

Переход от деятельности организации к деньгам через киберриски осуществляется в несколько этапов

1 Проведение аудита

Объект защиты

2 Оценка рисков киберугроз

Что может нам грозить?

3 Определение контрмер

Что делать, чтобы минимизировать последствия

4 Оценка финансовой рентабельности

А не слишком ли это дорого?

5 Стратегия внедрения контрмер

В какой последовательности действовать

6 Политика управления рисками

Выстроить и поддерживать процесс

Этап 1. Проведение аудита

Что является скоупом?

- **Аудит** бизнес-процессов компании. Интервью с бизнес-подразделениями, вовлеченными в критичные бизнес-процессы.
- **Оценка** существующих мер ИБ.
- **Инвентаризация** активов, оценка их стоимости и бизнес-критичности.
- **Проведение** технического аудита на предмет наличия уязвимостей в процессах и автоматизированных системах.
- **Формирование** перечня инцидентов, приводящих к ущербу, определение вероятности их возникновения и величины последствий

Этап 2. Оценка рисков

Виды рисков и риск-сценарии



Оценка финансового
риска



Определение величины
допустимого риска для
компании



Оценка репутационного
риска



Определение сценариев
по управлению
выявленными рисками
(избегание, принятие,
передача, минимизация).



Оценка риска
невыполнения
требований
законодательства

Этап 3. Определение контрмер

Что конкретно сделать для реализации риск-сценариев?

- Изменение бизнес-процесса: изменение степени автоматизации, модификация технологического процесса обработки бизнес-критичной информации, внесение изменений в информационные системы (ex. добавить или удалить поля в 1С).
- Разработка, регламентация, внедрение процедуры ИБ. Сопровождение при внедрении процедуры, разработка механизмов контроля.
- Внесение изменений в инфраструктуру (перестройка/перераспределение сети).
- Перенастройка используемых в компании средств защиты информации.
- Внедрение ранее неиспользуемых технических средств защиты.

Этап 4. Оценка финансовой рентабельности

Сколько стоят контрмеры? Действительно ли они нужны, или правильнее будет рассмотреть другой сценарий?



Оценка затрат на покупку оборудования



Оценка внутренних затрат



Оценка затрат на покупку лицензий



Оценка стоимости владения техническим средством защиты в течении N лет



Оценка затрат подрядчиков

Этап 5. Стратегия внедрения контрмер

Что делать и в какой последовательности?

Какие контрмеры внедрять в первую очередь, а какие оставить «на потом»?

1

Разбить контрмеры
на проекты

2

Составить планы
проектов

3

Определить
очередность

4

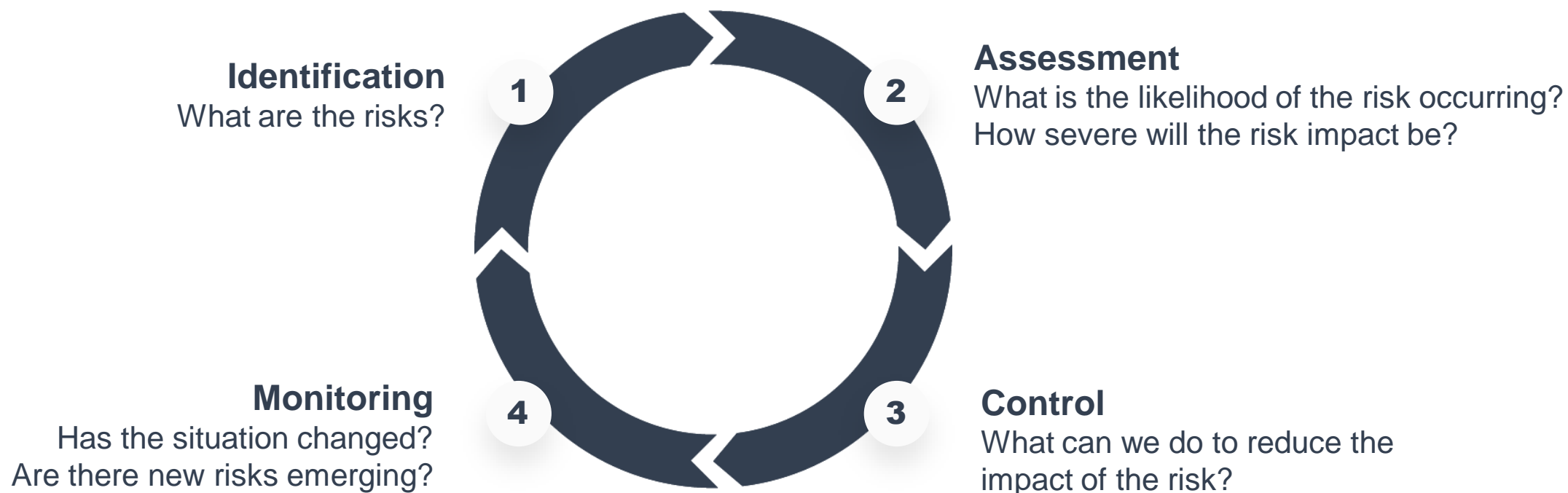
Показать, как
выполнение каждого
проекта приближает
к целевому состоянию

5

Объективно
корректировать
планы по ходу
исполнения

Этап 6. Политика управления киберрисками

Управление рисками – не одноразовая работа, работать с рисками нужно непрерывно!



Важно



Риск-менеджмент – процесс непрерывный

Должен быть регламентирован и строго выполняться



Правильно расставить приоритеты

Должен быть регламентирован и строго выполняться



Риск-сценарии

Рассматривать все, даже самые невероятные цепочки событий



Не переоценить контрамеру

Контрмера не должна быть дороже последствий



**Предотвращаем и расследуем
киберпреступления с 2003 года.**



Дмитрий Ильин

ilyin@group-ib.com

www.group-ib.ru

group-ib.ru/blog

info@group-ib.ru

+7 495 984 33 64

twitter.com/groupib

facebook.com/groupib

t.me/group_ib

instagram.com/group_ib