Разработка методик оценки затрат на ИБ

Рассмотрим, как можно определить прямые и косвенные затраты на ИБ с учетом специфики российских компаний.

Предположим, что руководство компании проводит работы по внедрению на предприятии системы защиты информации (СЗИ). Определены объекты и цели защиты, угрозы информационной безопасности и меры по противодействию им, приобретены и установлены необходимые средства защиты информации. Для того, чтобы требуемый уровень защиты ресурсов реально достигался и соответствовал ожиданиям руководства предприятия, необходимо ответить на следующие основные вопросы:

- Что такое затраты на информационную безопасность?
- Неизбежны ли затраты на информационную безопасность?
- Какова зависимость между затратами на информационную безопасность и достигаемым уровнем информационной безопасности?
- Представляют ли затраты на информационную безопасность существенную часть от оборота компании?
- Какую пользу можно извлечь из анализа затрат на информационную безопасность?

Затраты на информационную безопасность подразделяются на следующие категории:

- Затраты на формирование и поддержание звена управления системой защиты информации **(организационные затраты).**
- **Затраты на контроль**, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия.
- **Внутренние затраты** на ликвидацию последствий нарушения политики информационной безопасности (НПБ) - затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут.
- **Внешние затраты** на ликвидацию последствий нарушения политики информационной безопасности - компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т. п.
- **Затраты на техническое обслуживание системы защиты** информации и мероприятия по предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

Единовременные и систематические затраты

- Выделяют единовременные и систематические затраты.
- К единовременным относятся затраты на формирование политики безопасности предприятия: организационные затраты и затраты на приобретение и установку средств защиты.
- Классификация затрат условна, так как сбор, классификация и анализ затрат на информационную безопасность - внутренняя деятельность предприятий, и детальная разработка перечня зависят от особенностей конкретной организации.

- Невозможно полностью исключить затраты на безопасность, однако они могут быть приведены к приемлемому уровню. Некоторые виды затрат на безопасность являются абсолютно необходимыми, а некоторые могут быть существенно уменьшены или исключены. *Последние - это те, которые могут исчезнуть при отсутствии нарушений политики безопасности или сократятся, если количество и разрушающее воздействие нарушений уменьшатся.*

- Невозможно полностью исключить затраты на безопасность, однако они могут быть приведены к приемлемому уровню. Некоторые виды затрат на безопасность являются абсолютно необходимыми, а некоторые могут быть существенно уменьшены или исключены. Последние - это те, которые могут исчезнуть при отсутствии нарушений политики безопасности или сократятся, если количество и разрушающее воздействие нарушений уменьшатся.

При соблюдении политики безопасности и проведении профилактики нарушений можно существенно уменьшить следующие затраты:

- На восстановление системы безопасности до соответствия требованиям политики безопасности.
- На восстановление ресурсов информационной среды предприятия.
- На переделки внутри системы безопасности.
- На юридические споры и выплаты компенсаций.
- На выявление причин нарушения политики безопасности.

Неизбежные затраты могут включать:

- Обслуживание технических средств защиты.
- Конфиденциальное делопроизводство.
- Функционирование и аудит системы безопасности.
- Минимальный уровень проверок и контроля с привлечением специализированных организаций.
- Обучение персонала методам информационной безопасности.

Взаимосвязь между всеми затратами на безопасность, общими затратами на безопасность и уровнем защищенности информационной среды предприятия обычно имеет вид функции (Рис. 1).

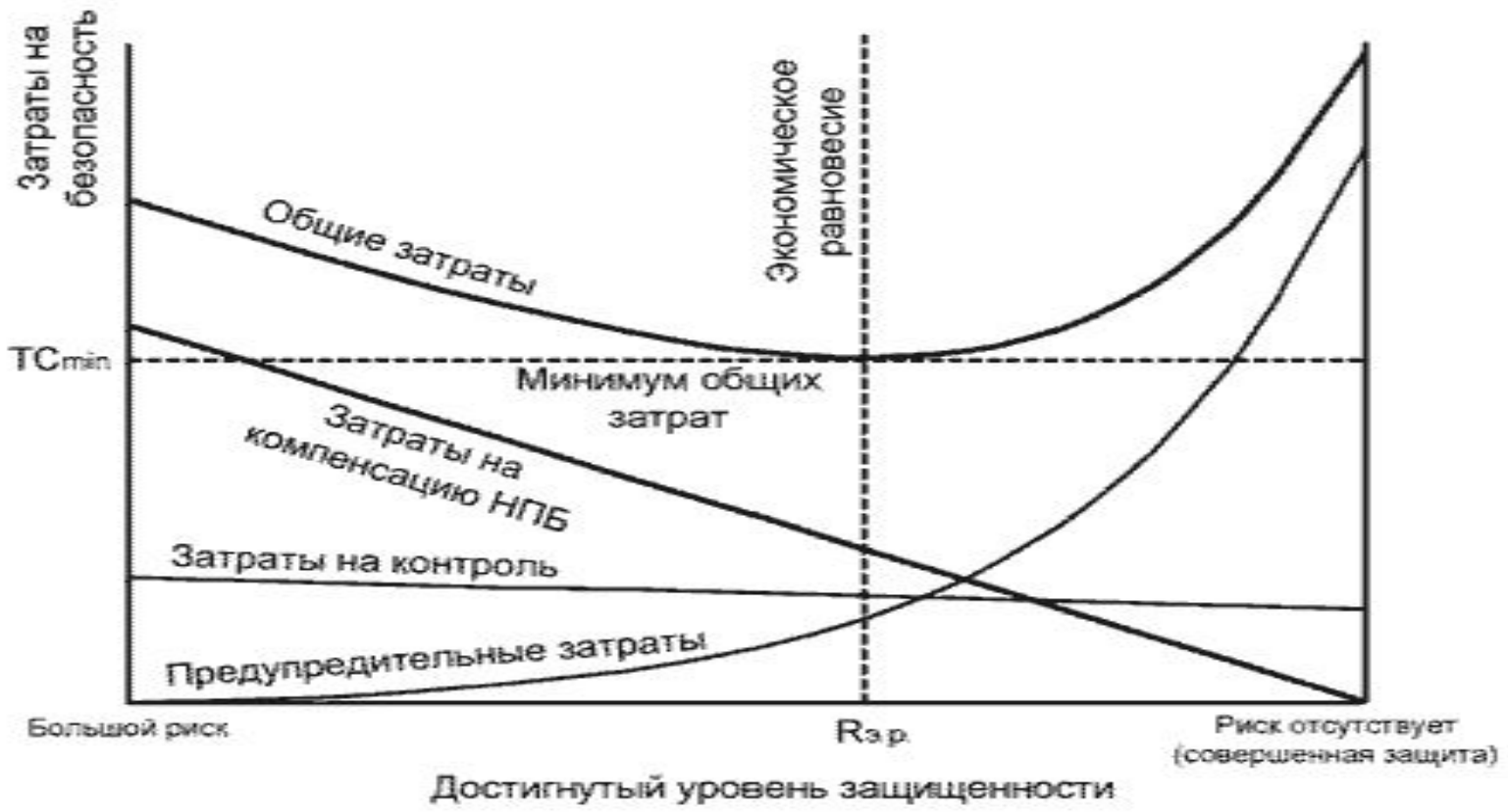

Рис.1. Взаимосвязь между затратами на безопасность и достигаемым уровнем защищенности

Общие затраты на безопасность складываются из затрат на предупредительные мероприятия, затрат на контроль и восполнение потерь (внешних и внутренних). С изменением уровня защищенности информационной среды изменяются величины составляющих общих затрат и, соответственно, их сумма - общие затраты на безопасность. Мы не включаем в данном случае единовременные затраты на формирование политики информационной безопасности предприятия, так как предполагаем, что такая политика уже выработана.

Как оценить долю затрат на ИБ в обороте компании?

Из опыта работы российских компаний, специализирующихся в области защиты информации на основе анализа состояния защищенности информационной среды предприятий металлургической отрасли и отрасли связи

Таблица 1. Типичное разделение затрат, связанных с ИБ

Затраты на потери (внешние и внутренние)	=	**70 % от общих затрат на безопасность**
Затраты на контроль	=	25 % от общих затрат на безопасность
Затраты на предупредительные мероприятия	=	5 % от общих затрат на безопасность

Таблица 2. Пример распределения общих затрат на безопасность

Затраты на потери (внешние и внутренние)	=	**50 % от новой величины общих затрат на безопасность**
Затраты на контроль	=	25 % от новой величины общих затрат на безопасность
Затраты на предупредительные мероприятия	=	25 % от новой величины общих затрат на безопасность

Таблица 3. Пример соотношения распределения общих затрат на ИБ

Затраты на потери (внешние и внутренние)	=	**30 % от начальной величины общих затрат на безопасность**
Затраты на контроль	=	25 % от начальной величины общих затрат на безопасность
Затраты на предупредительные мероприятия	=	25 % от начальной величины общих затрат на безопасность
Экономия	=	40 % от начальной величины общих затрат на безопасность