УДК 681.3

В.А. Артамонов, Е.В. Артамонова

МЕТОДИЧЕСКИЕ АСПЕКТЫ ВЫБОРА ЗАТРАТ НА ОРГАНИЗАЦИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

ЧАСТЬ 2: МЕТОДИКА УЧЁТА ПРИОБРЕТЁННОЙ КОНКУРЕНТНОЙ ВЫГОДЫ

Рассмотренные в ***ч.1*** настоящей работы методические рекомендации предлагают при планировании защиты информации исчислять затраты на информационную безопасность (ИБ) пропорционально размерам возможных собственных потерь от утечки или утраты информации (нарушении политики безопасности).

Из постулатов рыночной теории оценки рисков и мер по снижению потерь финансовых ресурсов [1] следует, что в конкурентной среде собственные потери, как правило, сопровождаются получением выгод другими хозяйствующими субъектами. И эти выгоды способны обеспечить конкуренту долговременное закрепление на соответствующих товарных рынках.

Таким образом, рассмотренная методика ***Gartner Group*** не учитывает главного мотива промышленной разведки: потенциальной финансовой ценности информации для конкурента и его экономической выгоды от её получения. Поэтому, при защите информации важно учитывать не только свои убытки от утери или хищения информации, но и соотношение возможных собственных потерь с выгодой, получаемой конкурентами от завладения ею и использования. На данном принципе строятся некоторые методики «субоптимального» планирования бюджета на защиту информации в конкурентных условиях при условии наличия тотального промышленного шпионажа (коммерческой разведки) [2].

Проиллюстрируем одну такую методику на рассмотрении некоторого абстрактного примера. И так, руководством организации за планируемый период определены шесть угроз в виде возможных каналов утраты и/или утечки информации $\mathbf{I_1}$ ... $\mathbf{I_6}$ и с привлечением экспертов оценена вероятность осуществления каждой угрозы $\mathbf{P_1}$ **…** $\mathbf{P_6}$. Следует понимать, что вероятности не отражают величину потерь и им не пропорциональны. При определении значения вероятности угрозы следует учитывать возможности конкурентов по ведению коммерческой разведки (напоминает извечную «дуэль» военной разведки и контрразведки противоборствующих сторон). Требуется найти сумму финансовых средств, которая может быть выделена на защиту информации от всех угроз, и её распределение на мероприятия по защите от каждой угрозы, но уже в зависимости от собственных потерь и приобретений конкурентов при реализации каждой угрозы.

Первый этап: определение веса каждой угрозы (табл. 1).

1.Ранжируем угрозы в соответствии с иерархией звеньев организационной структуры предприятия, на которые они воздействуют, от $\mathbf{I_1}$ **(**угроза, существующая в нижнем звене) до $\mathbf{I_6}$ (угроза, существующая в верхнем

звене). Для простоты нижнее значение вероятности берём равным 0,5 (реализуется – не реализуется).

2. Оцениваем собственные потери (в виде неполученной прибыли) $\mathbf{D_{собі}}$ при реализации каждой угрозы.

3. Оцениваем выгоды конкурентов (полученную ими прибыль) $\mathbf{D_{коні}}$ при успешном осуществлении ими действий, ведущих к реализации угрозы.

4. Определяем показатель степени в формуле веса каждой угрозы как отношение величины собственных потерь к величине выгод конкурентов по каждой угрозе:

$$\alpha_i = D_{соб\ i} / D_{коні}. \quad (1)$$

5. Определяем вес каждой угрозы как показательную функцию вида: вероятность угрозы в степени, равной отношению собственных потерь к выгодам конкурентов по каждой угрозе:

$$P_{весі} = P_i^{\alpha i}. \quad (2)$$

Сущность веса угрозы заключается в следующем: рост потенциальной выгоды конкурента приводит к росту затрат на защиту от данной угрозы в сумме общих затрат на защиту при её постоянстве.

Таким образом, уже после определения веса порядок ранжирования изменился на $\mathbf{I_3, I_2, I_6, I_1, I_5, I_4}$. Угроза $\mathbf{I_6}$ с минимальной вероятностью переместилась с последнего места на третье и приобрела значительный вес, так как конкурент при её реализации получает существенные преимущества.

Таблица 1

Определение веса каждой угрозы								
№п/п	**Параметры**	$\mathbf{I_1}$	$\mathbf{I_2}$	$\mathbf{I_3}$	$\mathbf{I_4}$	$\mathbf{I_5}$	$\mathbf{I_6}$	**Суммы ∑**
1	**Вероятности угроз Pi**	**0,7**	**0,8**	**0,9**	**0,6**	**0,55**	**0,5**	–
2	**Потери ($ тыс.) Dсоб i**	**100**	**200**	**100**	**300**	**300**	**400**	**1400**
3	**Выгоды конкурентов ($тыс.) Dконі**	**100**	**400**	**200**	**200**	**500**	**1000**	**2400**
4	**Показатель степени αi в формуле веса**	**1**	**0.5**	**0.5**	**1.5**	**0.6**	**0.4**	–
5	**Вес угрозы $P_{весі} = P_i^{\alpha i}$**	**0,7**	**0,894**	**0,948**	**0,465**	**0,699**	**0,758**	–

Второй этап: определение значимости защиты от каждой угрозы (табл.2).

6. Определяем суммы собственных потерь $\mathbf{D_{собi}}$ и выгод конкурентов $\mathbf{D_{кон\,i}}$ по каждой угрозе и общую сумму по всем угрозам.

7. Определяем относительный вес потерь по каждой угрозе:

$$\mathbf{P_{отн\,i} = (D_{соб\,i} + D_{кон\,i})/(\sum D_{соб\,i} + \sum D_{кон\,i})}. \qquad (3)$$

Независимо от числа угроз сумма весов должна быть равна единице.

8. Определяем значимость защиты от каждой угрозы как произведение ее веса (вероятностный аргумент) на относительный вес (денежный вес):

$$\mathbf{P_{зн\,i} = P_{весi} \times P_{отн\,i}}. \qquad (4)$$

Сущность значимости защиты заключается в том, что её значение показывает долю отчисления от общей суммы, выделяемую на противодействие каждой угрозе.

Таким образом, после определения значимости защиты от угрозы порядок ранжирования изменился на $\mathbf{I_6, I_5, I_2, I_3, I_4, I_1}$. Мы видим, что хотя относительный вес потерь от разновероятностных угроз $\mathbf{I_2}$ и $\mathbf{I_5}$ отличается, но в списке значимости защиты они находятся рядом. Это определено соотношением значений собственных потерь и выгод конкурента: вес угрозы $\mathbf{I_5}$ возрастает за счёт того, что выгода конкурентов выше собственных потерь и значение суммы потерь и выгод больше, чем для угрозы $\mathbf{I_2}$. Последнее место угрозы $\mathbf{I_1}$ с не самой низкой вероятностью осуществления определено и малыми значениями потерь и выгод, и отсутствием превышения выгод конкурента над своими потерями. На первое же место вышла значимость защиты от угрозы $\mathbf{I_6}$ с минимальным значением вероятности. Это объясняется и самой большой суммой потерь и выгод, и большой разницей между этими величинами в пользу конкурента. Значимость защиты от угрозы с максимальной вероятность переместилась на четвёртое место, так как относительный вес потерь от её реализации не самый большой, и разница между собственными потерями и выгодами конкурента также не самая существенная.

Таблица 2

Определение значимости защиты от каждой угрозы								
№ п/п	**Параметры**	I_1	I_2	I_3	I_4	I_5	I_6	**Суммы ∑**
6	**Суммы($тыс.) собственных потерь и выгод конкурентов**	**200**	**600**	**300**	**500**	**800**	**1400**	**3800**
7	**Относительный вес потерь Ротні**	**0,052**	**0,158**	**0,079**	**0,132**	**0,211**	**0,368**	**∑Ротн =1**

8	**Значимость защиты от угрозы Рзн= Рвесі × Ротні**	**0,036**	**0,141**	**0,075**	**0,061**	**0,147**	**0,28**	**∑Рзні =0,74**

Третий этап: определение величины средств, необходимых и выделяемых на защиту информации от прогнозируемых угроз.

9. Научно обоснованных норм для определения инвестиций в ИБ не существует, для их выработки должна проводится соответствующая аналитическая работа, причём по каждой отрасли бизнеса, поэтому на практике в качестве финансовых баз, от которых задаются относительные величины потерь и отчислений на защиту информации, приводятся различные балансовые или экономические показатели, либо опираются на устоявшуюся по отрасли практику (best practice) [3]. Так в последнем случае эксперты – практики из некоторых авторитетных консалтинговых компаний в области защиты информации нашли некое оптимальное решение, при котором можно чувствовать себя относительно уверенно – стоимость системы ИБ должна составлять примерно 10-20% от стоимости корпоративной информационной системы (как видим весьма широкий диапазон и без учёта конкурентной среды бизнеса). Тем не менее, учитывая, что в примере в качестве базы для отчислений на защиту принята неполученная (потенциальная) прибыль, и ориентируясь на эти коэффициенты потерь, **норму отчисления** $\mathbf{D_{Н\ 0Т}}$ неполученной прибыли на защиту информации примем равной **0,3**. Тогда выделяемая сумма равна:

$$\mathbf{D_{Н.\ 0Т}} = 0{,}3 \sum \mathbf{D_{соб\ i}} = 0{,}3 \times 1400 \text{ тыс.} = 420 \text{ тыс.} \qquad (5)$$

Данная норма отчисления от сберегаемой прибыли предназначена для нейтрализации суммы значимостей всех угроз :

$$\mathbf{D_{Н.\ 0Т}} = \sum \mathbf{P_{зн\ i}}. \qquad (6)$$

Тогда на предотвращение каждой угрозы должна выделяться часть доли, пропорциональная значимости защиты от этой угрозы:

$$\mathbf{D_{Н\cdot 0Т}} = \sum \mathbf{P_{зн\ i}}. \qquad (7)$$

Распределение сумм находится применением следующего выражения:

$$\mathbf{D_{н.от\ i}} = \mathbf{D_{н.от}} \times \mathbf{P_{зн\ i}} / \sum \mathbf{P_{зн\ i}}. \qquad (8)$$

Пример расчёта для первой угрозы:

$$\mathbf{D_{н.от1}} = \$420\text{тыс.} \times 0{,}036/0{,}74 = \$20{,}43 \text{ тыс.} \qquad (9)$$

Просчитав суммы, необходимые для защиты информации от каждой угрозы, получим сводные результаты (см. табл. 3).

Таблица 3

Определение величины средств на защиту от каждой угрозы								
№п/п	**Параметры**	**I_1**	**I_2**	**I_3**	**I_4**	**I_5**	**I_6**	**Общая сумма (∑)**
9	**Сумма($тыс.) противодействия каждой угрозе Dн. от i**	**20,43**	**80**	**42,57**	**34,6**	**83,4**	**159**	**420**

Заключение.

Как видно, большую часть средств следует выделять не на защиту от тех угроз, вероятность которых больше, а от тех, где значимости защиты выше. В данном примере угроза $\mathbf{I_6}$ с вероятностью **0,5** и угроза $\mathbf{I_5}$ с вероятностью **0,55** могут нанести больший ущерб, так как, получив существенную выгоду, конкурент способен закрепиться на данном рынке, вытеснив с него ваше предприятие. Угроза с максимальной вероятностью по значимости защиты от нее оказалась на четвертом месте. Таким образом, значимость защиты от угрозы учитывает связь вероятности угрозы с вашими собственными потерями и получаемыми выгодами конкурентов, как по отдельным угрозам, так и по всей их совокупности. Эта связь проявляется только в том случае, когда норма отчисления на защиту берется не от упущенной выгоды или суммы потерь по отдельным угрозам, а от суммы упущенных выгод или потерь по всем угрозам. Это и есть основное отличие предлагаемой методики. Полученное с ее помощью распределение затрат учитывает вероятности событий и может считаться наиболее близким к оптимальному варианту.

Литература

1.Радиевский М.В. БИЗНЕС-ПЛАН. Технико-экономическое планирование и обоснование финансовой стратегии предприятия. Методика и практ. рек. – Мн.: Белпринт, 2000. – 264 с.

2. Провоторов В. Д. ЗАЩИТИТЬ, ЧТОБЫ НЕ ПРОИГРАТЬ.// Информационная безопасность, 2004, №5. – с. 18 – 20.

3.Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.: ил. - (Информационные технологии для инженеров).

МНОО «МАИТ», г. Минск