ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056.53

МЕТОДЫ ОЦЕНКИ РИСКОВ, СВЯЗАННЫХ С НАРУШЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Д.В. Кутузов, В.Н. Белозеров, Р.О. Ларченко

Статья посвящена проблемам оценки рисков, связанных с нарушением информационной безопасности предприятия. В статье изложены наиболее популярные методы оценки рисков, такие как метод ALE, метод компании IBM, приложение метода анализа иерархий. Для представленных методов рассмотрены их достоинства и недостатки, возможность применения для организаций.

Ключевые слова: *информационная безопасность, оценка рисков, управление рисками, метод оценки рисков ALE, метод оценки рисков IBM, метод анализа иерархий*

Key words: *Information safety, estimation of risks, management of risks, the Annualized Loss Expectancy method (ALE), the IBM company method, the method of the analysis of hierarchies*

Практически для любой организации актуальной является проблема оценки рисков, связанных с нарушениями безопасности. Причем чем крупнее предприятие или организация, тем острее стоит проблема оценки рисков.

Оценка рисков и выражение их в денежной форме необходима, прежде всего, для принятия решения о целесообразности внедрения мер по обеспечению безопасности, их состава и направленности.

Как известно, риск за период времени (обычно за год) вычисляется по формуле:

$$M = \sum_{i=1}^{n} v_i p_i \qquad (1)$$

где M – математическое ожидание потерь за год по всем видам рисков, руб.; v_i – стоимость *i*-го ресурса или потери, связанные с утратой или временной недоступностью ресурса; p_i – вероятность реализации угрозы ресурсу в течение года.

Вероятность реализации той или иной угрозы может быть оценена по статистическим данным, если на предприятии ведется статистика по нарушениям информационной безопасности.

При отсутствии статистических данных зачастую трудно определить вероятности того или иного события. Большинство предприятий не ведет учета нарушений безопасности и не имеет данных, характеризующих эти нарушения. Поэтому при оценке вероятности нарушения безопасности, организации прибегают к косвенным методам оценки, к которым можно отнести разного рода экспертные оценки и автоматизированные системы, построенные на их основе.

Рассмотрим некоторые методы, предназначенные для оценки уровня и безопасности организаций и рисков, связанных с ее нарушением.

Метод ALE (Annualized Loss Expectancy). Этот подход базируется на вычислении потерь от нарушений политики безопасности, с которыми может столкнуться компания, и их сравнении с инвестициями в безопасность, направленными на предотвращение нарушений. Метод ожидаемых потерь основан на эмпирическом опыте организаций и сведений о вторжениях, о потерях от вирусов, об отражении сервисных нападений и т. д. Например, нарушения безопасности коммерческих организаций приводят к следующим финансовым потерям:

- при ведении электронной коммерции потери, связанные с простоем и выходом из строя сетевого оборудования;

• нанесение ущерба имиджу и репутации компании;

• оплата сверхурочной работы ИТ-персонала и/или оплата работ подрядчикам, которые занимались восстановлением корпоративной информационной системы;

• оплата консультаций внешних специалистов, которые осуществляли восстановление данных, выполняли ремонт и оказывали юридическую помощь;

• оплата ремонта физических повреждений от виртуальных атак;

• судебные издержки при подаче искового заявления о виртуальных преступлениях и нарушениях политики безопасности.

Чтобы «смягчить» ожидаемые потери, компания должна инвестировать средства в безопасность: сетевые экраны, системы обнаружения вторжений, антивирусы. Если компания решает установить систему информационной безопасности, то ее стоимость обобщенно будет складываться из единовременных и периодических затрат.

Единовременные затраты:

• покупка лицензий антивирусного программного обеспечения, средств firewall;

• приобретение аппаратных средств;

• возможно, оплата консультаций внешнего эксперта в области информационной безопасности.

Периодические затраты:

• техническая поддержка и сопровождение;

• заработная плата ИТ-персонала;

• затраты на найм необходимых специалистов;

• затраты на исследование угроз нарушений политики безопасности.

Финансовая выгода обеспечивается ежегодными сбережениями, которые получает компания при внедрении системы ИБ. Выгоды рассчитываются по следующей формуле:

$$AS=ALE\times E-AC \qquad (2)$$

где AS – ежегодные сбережения (Annual Saving); ALE – показатель ожидаемых потерь (Annualised Loss Expectancy); E – эффективность системы защиты (около 85 %); AC – ежегодные затраты на безопасность (Annual Cost).

Методика оценки рисков и их расчет, производятся по следующему алгоритму. Формула, используемая при расчете рисков, представляет собой произведение трех параметров:

1) ценность ресурса (Asset Value, AV). Указанная величина характеризует ценность ресурса. При оценке рисков ценность ресурса ранжируется в диапазоне от 1 до 3, где 1 – минимальная ценность ресурса, 2 – средняя ценность ресурса и 3 – максимальная ценность ресурса;

2) мера уязвимости ресурса к угрозе (Exposure Factor, EF). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. Данная величина также ранжируется в диапазоне от 1 до 3, где 1 – минимальная мера уязвимости, 2 – средняя, 3 –максимальная;

3) оценка вероятности реализации угрозы (Annual Rate of Occurrence, ARO) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь (уровень риска):

1) оценка ожидаемого возможного ущерба от единичной реализации определенной угрозы (Single Loss Exposure, SLE) рассчитывается по формуле:

$$SLE=AV\times EF \tag{3}$$

2) итоговые ожидаемые потери от конкретной угрозы за определенный период времени (Annual Loss Exposure, ALE) характеризуют величину риска и рассчитываются по формуле:

$$ALE=SLE\times ARO \tag{4}$$

Метод компании IBM. Специалистами компании IBM была предложена эмпирическая зависимость ожидаемых потерь от i-той угрозы безопасности [1]:

$$R_i = 10^{(S_i+V_i-4)} \tag{5}$$

Здесь S_i – коэффициент, характеризующий возможную частоту возникновения i-той угрозы; V_i – коэффициент, характеризующий значение возможного ущерба при ее возникновении.

Значения коэффициентов, которые следует использовать, представлены в табл. 1, 2.

Таблица 1

Рекомендуемые значения S_i

Ожидаемая частота появления угрозы	Рекомендуемое значение S_i
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (приблизительно 10 раз в год)	5
2 раза в неделю (100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 2

Рекомендуемые значения V_i

Значение возможного ущерба при реализации угрозы, долл. США	Рекомендуемое значение V_i
1	0
10	1
100	2
1000	3
10000	4

Тогда суммарная стоимость потерь определяется по формуле:

$$R=\sum_i R_i \tag{6}$$

Достоинством данного метода является его простота, недостатком – необходимость использования статистики, отражающей частоту возникновения тех или иных угроз.

Оценка рисков с помощью метода анализа иерархий. Метод анализа иерархий (МАИ) является систематической процедурой для иерархического представления элементов, определяющих суть проблемы [1]. Метод состоит в декомпозиции проблемы на все более простые составляющие части и дальнейшей обработке последовательности суждений лица, принимающего решения, по парным сравнениям. В результате может быть выражена отно-

сительная степень (интенсивность) взаимодействия элементов в иерархии. Эти суждения затем выражаются численно. МАИ включает в себя процедуры синтеза множественных суждений, получения приоритетности критериев и нахождения альтернативных решений. Такой подход к решению проблемы выбора исходит из естественной способности людей думать логически и творчески, определять события и устанавливать отношения между ними.

Метод анализа иерархий предполагает выполнение следующих этапов:

1. Очертить проблему и определить, что мы хотим.
2. Построить иерархию (цель, критерии, альтернативы).
3. Построить множество матриц парных сравнений для каждого из нижних уровней по одной матрице для каждого элемента, примыкающего сверху уровня.
4. Проверить индекс согласованности каждой матрицы.
5. Использовать иерархический синтез для взвешивания собственных векторов весами критериев и вычислить сумму по всем соответствующим взвешенным компонентам собственных векторов уровня иерархии, лежащего ниже.

Все методологии исследований различных рисков, в частности, информационных, расположены на границе между объективной, неоднозначной, расплывчатой информацией и применяемыми четкими, жесткими методами обработки.

В результате становится необходимым соответствующий язык для перевода изучаемых проблем рынка в вид, приемлемый для используемых методов обработки информации.

Роль подобного языка в МАИ выполняют различные иерархические структуры. Соответственно, в МАИ любая задача или проблема предварительно структурируются и представляются в виде иерархии (древовидной или сетевой).

Таким образом, в МАИ основная цель исследования и все факторы, в той или иной степени влияющие на достижение цели, распределяются по уровням в зависимости от степени и характера влияния.

На первом уровне иерархии всегда находится одна вершина – цель проводимого исследования.

Второй уровень иерархии составляют факторы, непосредственно влияющие на достижение цели. При этом каждый фактор представляется в строящейся иерархии вершиной, соединенной с вершиной 1-го уровня.

Третий уровень составляют факторы, от которых зависят вершины 2-го уровня.

По окончании построения иерархии для каждой материнской вершины проводится оценка весовых коэффициентов, определяющих степень ее зависимости от влияющих на нее вершин более низкого уровня. При этом используется метод попарных сравнений.

На рис. приведена иерархия возможностей реализации угроз для различных ресурсов компании ТАН (может использоваться и для других предприятий).

Если известна вероятность нарушения информационной безопасности предприятий в РФ или ее отдельных субъектах, то метод анализа иерархий позволит определить долю рисков, связанных с информационными, физическими и сервисными ресурсами на предприятии ТАН, а затем оценить возможный ущерб при их реализации.

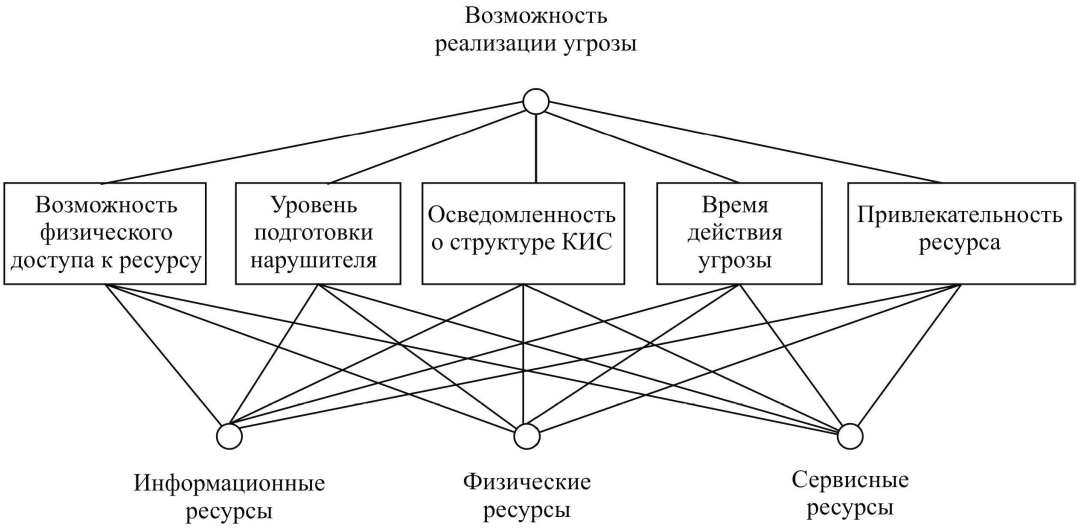

Рис. Иерархия возможностей реализации угроз для различных ресурсов компании ТАН

Пусть $A_1,...,A_n$ – множество из n элементов, в качестве которых будут выступать критерии сравнений или ресурсы.

Тогда $W_1,...,W_n$ – их взаимные оценки, которые соотносятся следующим образом:

$$W = \begin{array}{c} \\ A_1 \\ \dots \\ A_n \end{array} \begin{array}{c} \begin{array}{ccc} A_1 & \dots & A_n \end{array} \\ \begin{pmatrix} 1 & \dots & W_1/W_n \\ \dots & 1 & \dots \\ W_n/W_1 & \dots & 1 \end{pmatrix} \end{array} \tag{7}$$

Оценка компонент вектора приоритетов производится по формулам:

$$\begin{aligned} X_1 &= (1 \cdot (W_1/W_2) \cdot \dots \cdot (W_1/W_n))^{1/n} \\ &\dots \\ X_n &= ((W_n/W_1) \cdot \dots \cdot (W_n/W_{n-1}) \cdot 1)^{1/n} \end{aligned} \tag{8}$$

Веса по отдельным критериям рассчитываются по формуле:

$$W(A_i) = \frac{X_i}{\sum_i X_i} \tag{9}$$

Первым этапом является построение матрицы сравнений и расчет значений приоритетов критериев. В качестве критериев в данном случае выступают:

1) возможность физического доступа к ресурсу A_1;
2) уровень подготовки нарушителя A_2;
3) осведомленность о структуре КИС A_3;
4) время действия угрозы A_4;

5) привлекательность ресурса A_5.

Сравнения влияния основных критериев на возможность реализации угрозы тому или иному ресурсу, а значит, и на долю риска, приходящегося на тот или иной ресурс, производится по следующему принципу:

1 – равная важность;

3 – умеренное превосходство одного над другим;

5 – существенное превосходство одного над другим;

7 – значительное превосходство одного над другим;

9 – очень сильное превосходство одного над другим;

2, 4, 6, 8 – соответствующие промежуточные значения.

К преимуществам данного метода можно отнести следующие:

• иерархическое представление системы можно использовать для описания того, как влияют изменения приоритетов на верхних уровнях на приоритеты элементов нижних уровней;

• иерархии предоставляют более подробную информацию о структуре и функции системы на нижних уровнях и обеспечивают рассмотрение «акторов» и их целей на высших уровнях. Для удовлетворения ограничений на элементы уровня их лучше всего воспроизводить на следующем более высоком уровне;

• естественные системы, составленные иерархически, т.е. посредством модульного построения и затем сборки модулей, строятся намного эффективнее, чем системы, собранные в целом;

• иерархии устойчивы и гибки; они устойчивы в том смысле, что малые изменения вызывают малый эффект, а гибкие в том смысле, что добавления к хорошо структурированной иерархии не разрушают ее характеристик.

Основным и главным недостатком данного метода является его чрезмерная громоздкость и трудность в исправлении или модификации данных. Кроме того, при большом числе факторов затрудняется работа с методом из-за того, что лицо, принимающее решение, не в состоянии их соотносить друг с другом.

Методы оценки рисков, изложенные выше, могут быть использованы по отдельности или одновременно. В случае, если они используются одновременно, лицо, ответственное за безопасность предприятия или организации, может сравнить полученные результаты и в случае больших расхождений, проведя более детальный анализ, вновь выполнить оценку рисков. На основании оценки рисков должно быть принято решение о необходимости инвестиций в систему безопасности предприятия.

Библиографический список

1. ***Саати, Т.*** Принятие решений: метод анализа иерархий : пер. с англ. / Т. Саати. – М. : Радио и связь, 1993. – 278 с.

2. ***Семкин, С. Н.*** Основы организационного обеспечения информационной безопасности объектов информатизации / С. Н. Семкин, Э. В. Беляков, С. В. Гребенев, В. И. Казачок. – М. : Гелиос АРВ, 2005. – 186 с.