УДК 004.056

О.Т. Данилова, Е.В. Широков

Анализ результатов аудита системы защиты информации с применением комплексной сравнительной оценки

Предлагается способ анализа результатов системы защиты информации (СЗИ) на базе метода комплексной сравнительной оценки. Преимущества рассматриваемого способа состоят в том, что, во-первых, анализ базируется на комплексном многомерном подходе в оценке такого сложного явления, как структурные изменения, происходящие в системе защиты; во-вторых, логика способа позволяет избежать субъективизма отдельных показателей; в-третьих, метод отличается простотой и универсальностью.

Ключевые слова: информационная безопасность, комплексная оценка, методика оценки.

Анализ системы информационной безопасности (СЗИ) ключевых систем информационной инфраструктуры должен позволить получить полную и объективную оценку защищенности информационных процессов, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации. К сожалению, существуют препятствия как методологического, так и организационного характера тому, чтобы комплексная оценка удовлетворяла этим требованиям. Поэтому нередко возникают ситуации, когда полученные тем или иным способом обобщающие оценки СЗИ ключевых систем не соответствуют действительности или на практике не оправдывают усилий, затраченных на сбор и обработку данных [1].

Для получения адекватного анализа комплекса применяемых мер защиты на объекте без привлечения сторонних экспертов и значительных финансовых затрат в данной работе представляется методика комплексной оценки результатов анализа защищенности, основанная на применении общеизвестных подходов оценивания рисков и методов, являющихся основой для расчета различных рейтингов [2]. К методам многомерного анализа (комплексной сравнительной оценки) относятся следующие:

1. Метод суммирования показателей – используют в случае одинаковой направленности исходных показателей и их общей сопоставимости. Наилучшим результатом по данному методу считается тот, который представляет собой максимальную сумму показателей-стимуляторов или минимальную сумму показателей-дестимуляторов.

2. Метод суммы мест – здесь анализируемые объекты ранжируются по показателям-стимуляторам в порядке возрастания и по показателям-дестимуляторам в порядке убывания. Наилучшим результатам соответствуют значения минимальной суммы мест. Метод прост и позволяет быстро получить необходимую оценку, но при этом является грубым и приблизительным, не учитывает значимость различных показателей.

3. Метод расстояний – преимущество метода расстояний перед другими методами обусловлено использованием приема нормирования, когда значения показателя всех сравниваемых объектов делятся на так называемое эталонное (другими словами, оптимальное) значение показателя.

4. Таксонометрический метод – не только учитывает абсолютные значения показателей, но и позволяет элиминировать их различную вариацию и является обобщением метода расстояний.

5. Метод суммы баллов с заданной непрерывной шкалой на выбранном отрезке – при оценке всех показателей по одинаковой шкале не учитываются их коэффициенты значимости, поэтому необходимо строить для каждого показателя свою шкалу с учетом его значимости**.**

Кроме исходных данных о значениях показателей, задаются шкалы для оценки каждого показателя. Этот метод требует разработки большого числа шкальных оценок, которые необходимо согласовывать между собой. Наиболее распространенными являются непрерывные шкалы и дискретные шкалы [3, 4].

Дискретная шкала задает определенное число уровней оценок (баллов), с помощью которых оценивается показатель. Как правило, в этом случае выбирают целочисленные балльные оценки: 0,

1, 2, 3 и т.д. или 0, 5, 10 и т.д. Обычно балльная оценка в этом случае исчисляется путем задания интервалов изменения показателя и соответствующих балльных оценок.

При применении непрерывной шкалы оценки могут принадлежать любой точке отрезка, который определяет шкалу данного показателя. Как правило, способ исчисления балльной оценки для непрерывной шкалы – непрерывное отображение отрезка, в пределах которого изменяется данный показатель, на заданную шкалу.

Ядро методики представляет собой классический подход к формированию режима безопасности и проектированию системы защиты объекта информатизации, включающий в себя три основных ключевых этапа:

1) идентификация, анализ и оценка рисков, охватывающих все активы организации;

2) оценка возможности уменьшения рисков;

3) оценка остаточных рисков и проведение комплексной оценки с выдачей заключения о достаточности принятых мер по защите.

Анализ качества оценки объектов СЗИ состоит из следующих этапов:

Этап 1. Определяются цели и условия функционирования организации – владельца информационных ресурсов, поскольку уровень информационной безопасности организации является одной из характеристик его жизнеспособности. При анализе СЗИ организации некоторые положения комплексной оценки соответственно будут пересекаться с определенными видами деятельности организации. В основном это затрагивает формирование стратегических интересов организации и соответственно их количественного толкования.

Этап 2. Здесь формируются данные об информационной системе организации, необходимая база системного анализа и выбирается исходная система показателей.

Этап 3. На этом этапе выбираются группы показателей или отдельного критерия, определенного как мера для сравнения количественных показателей исследуемой операции в отношении затрачиваемых усилий и получаемых результатов. Критерий должен отвечать следующим основным требованиям: иметь ясный физический смысл; быть определяющим и соответствовать основной цели функционирования системы, подсистемы или элемента; учитывать основные детерминированные и стохастические факторы, определяющие уровень безопасности системы; быть критичным к анализируемым параметрам и достаточно чувствительным к ним.

Необходимое условие: все показатели должны иметь одинаковую направленность – либо на увеличение, либо на уменьшение, т.е. увеличение любого частного показателя рассматривается как улучшение результатов деятельности и наоборот. Если имеются разнонаправленные показатели, то их приводят к одинаковой направленности путем ввода обратных чисел.

Оценка уровня защищенности определяется по каждому семейству на отрезке [0;1]. Так как все компоненты доверия, содержащиеся в конкретном семействе, имеют иерархическую последовательность, то оценка «1» выставляется, если объект соответствует максимальному компоненту доверия, а оценка «0» – если не выполняются требования самого низкого компонента. Объекты оценки соотносятся к соответствующим компонентам доверия на основе соответствующей анкеты.

Этап 4. По исходным данным строится вспомогательная матрица **P** по следующим правилам:

а) если показатель является стимулятором ($s_j = +1$), то элементы j-го столбца матрицы упорядочиваются по убыванию и элементу p_{ij} придается значение, соответствующее месту элемента x_{ij} среди упорядоченных элементов j-го столбца, элементам с одинаковыми значениями присваиваются одинаковые места;

б) если показатель является дестимулятором ($s_j = 1$), то элементы j-го столбца матрицы упорядочиваются по возрастанию и элементу p_{ij} придается значение, соответствующее месту элемента x_{ij} среди упорядоченных элементов j-го столбца.

Для расчета балльной оценки при использовании непрерывной шкалы можно задействовать следующие формулы:

– для показателей-стимуляторов: $b_{ij} = b_{\min j} + \dfrac{(b_{\max j} - b_{\min j})(x_{ij} - x_{\min j})}{(x_{\max j} - x_{\min j})}$;

– для показателей-дестимуляторов: $b_{ij} = b_{\max j} + \dfrac{(b_{\max j} - b_{\min j})(x_{ij} - x_{\min j})}{(x_{\max j} - x_{\min j})}$.

Здесь $b_{\max j}$ и $b_{\min j}$ – максимально и минимально возможные балльные оценки для j-го показателя по принятой для него шкале; $x_{\max j}$ и $x_{\min j}$ – соответственно максимальное и минимальное значения j-го показателя.

Этап 5. На этом этапе проводится операция стандартизации признаков (показателей), поскольку разные признаки могут иметь различную размерность.

Этап 6. Производится расчет точки-эталона P_0, обусловленный тем, что в одномерном пространстве происходит попарное сравнение показателей. Эталоном будет точка (вектор), образованная по правилу: среди признаков-стимуляторов отбираются признаки с максимальными значениями, а среди признаков-дестимуляторов – с минимальными.

Этап 7. Осуществляется ранжирование объектов по степени убывания характеристик. Этот этап занимает важное место в системе комплексного анализа в двух случаях:

1) когда требуется сопоставить состояния нескольких объектов на основе единой системы показателей;

2) когда нужно сопоставить результаты функционирования какого-либо объекта во времени.

Ранговое место служит обобщающим показателем, представляя собой «равнодействующую» всех признаков, что позволяет линейно упорядочить анализируемые объекты. Проведение оценки рангового места заключается в следующем:

– определяется расстояние C_{i0} между точками, характеризующими исследуемые объекты, и эталонной точкой P_0;

– формируется вектор значения расстояний $C = (C_{10} C_{20} ... C_{m0})$;

– определяется среднее арифметическое расстояний между i-м объектом и точкой P_0:

$$\overline{C}_0 = \frac{1}{m} \sum_{i=1}^{m} C_{i0};$$

– вычисляется среднеквадратическое отклонение σ_0 от точки P_0;

– рассчитывается показатель качества оценки i-го объекта $C_0 = \overline{C}_0 + 2\sigma_0$.

По расстоянию между i-м элементом C_{i0} и точкой P_0 можно сделать предварительные выводы о ранговом месте объекта при оценке качества системы. Чем меньше расстояние между C_{i0} и P_0, тем выше качество защиты объекта по данному признаку.

Этап 8. Расчеты уточняются через определение оценки $D = 1 - \dfrac{C_{i0}}{C_0}$, которая интерпретируется следующим образом: качество объекта тем выше, чем ближе значение показателя к единице.

Точность каждого применяемого метода в комплексе можно характеризовать соответствием средних удельных весов всех показателей в комплексной оценке (вкладов показателей в оценку) их коэффициентам значимости [5]. Количественно точность метода можно оценить как квадрат расстояния между двумя точками в n-мерном пространстве. Координаты одной точки – это значения средних удельных весов каждого показателя в комплексной оценке (w_j), координаты второй – коэффициенты значимости показателей (k_j). Отклонение, характеризующее точность применяемого метода комплексной сравнительной оценки, рассчитывается по формуле

$$O = \sum_{j=1}^{n} (k_j - w_j)^2,$$

где w_j – средний удельный вес каждого показателя.

Чем меньше значение отклонения, тем ближе значения средних удельных весов и коэффициентов значимости, тем точнее метод.

Полученные результаты позволяют сделать вывод о приемлемости использования методики комплексной сравнительной оценки для анализа результатов аудита системы обеспечения информационной безопасности организации. Однако следует учитывать, что осуществление этапов анализа связано со многими нерешенными проблемами, например при определении системы оцениваемых показателей и коэффициентов их сравнительной значимости, а также с затруднениями при разработке вычислительного алгоритма.

Литература

1. Конев А.А. Подход к описанию структуры системы защиты информации /А.А. Конев, Е.М. Давыдова // Доклады ТУСУРа. – 2013. – № 2 (28). – С.107–111.
2. Шеремет А.Д. Комплексный анализ хозяйственной деятельности. – М.: Инфра-М, 2006. – 415 с.
3. Евсютин О.О. Использование клеточных автоматов для решения задач преобразования информации / О.О. Евсютин, С.К. Росошек // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 173–174.
4. Мещеряков Р.В. Модель обработки информации в различных шкалах // Современные информационные технологии. – 2008. – № 8. – С. 101–103.
5. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

Данилова Ольга Тимофеевна
Канд. физ.-мат. наук, доцент каф. комплексной защиты информации
Омского государственного технического университета (ОмГТУ)
Тел.: 8 (381-2) 62-87-07
Эл. почта: olga.danlot@yandex.ru

Широков Егор Владимирович
Ст. преподаватель каф. комплексной защиты информации ОмГТУ
Эл. почта: 9785870@gmail.com

Danilova O.T., Shirokov E.V.

Analysis of results of audit of system of information security with application of a complex comparative assessment

In this article we propose a method based on a set of comparative evaluations, to analyze the data security system. The advantages of this method are as follows: firstly, It is based on an interdisciplinary approach to the assessment of such complex phenomena as the struct the system of protection, and secondly, the logic of this technique allows to overcome the shortcomings of methods for assessing structural changes and thus avoid the subjectivity of the individual indicators, and thirdly, the methods are simple and flexible.

Keywords: information security, complex assessment, methodology of evaluation.