УДК 004.056

О.Т. Данилова, Е.Н. Толстых

Анализ системы защиты информации с применением инструментов качества и метода динамического программирования

Рассматривается практическое применение некоторых инструментов качества для анализа состояния комплексной системы защиты информации организации с целью выявления причинно-следственных связей, получения качественных и количественных характеристик уровней защищенности для принятия решений по их эффективной модернизации.

Ключевые слова: информационная безопасность, диаграмма Парето, корректирующие мероприятия.

Для анализа сложного многоаспектного процесса защиты информации требуются достоверные и комплексные оценки его качества и эффективности, позволяющие не только отражать общие результаты состояния процесса, но и выбирать и применять механизмы по его управлению. Очевидно, что по результатам анализа должны проводиться корректирующие мероприятия, имеющие своей целью повышение эффективности и надежности работы рассматриваемого процесса. В связи с этим возникают две проблемы: с одной стороны, желательно, чтобы корректирующие мероприятия были экономически оправданными, а с другой стороны, улучшение характеристик надежности одних составляющих процесса может негативно сказываться на работе других, и это надо учитывать как на этапе анализа, так и в динамике развития всей комплексной системы защиты информации.

Оценка показателей защиты информации с применением диаграммы Парето

Оценка показателей защиты информации может быть сформирована на основании выявленной аудиторской группой степени выполнения требований посредством экспертного оценивания. Положим, что в результате опроса имеется: $M=\{M_1,M_2,...,M_i,...,M_I\}$ – множество классов и семейств функциональных показателей качества процесса защиты информации; $m=\{m_1,m_2,...m_j,...,m_J\}$ – множество функциональных требований обеспечения уровня защиты в классе M_i; $R=\{R_1,R_2,...R_k,...,R_K\}$ – множество причин, из-за которых не выполняются те или иные требования информационной безопасности. По полученным данным можно построить причинно-следственную диаграмму Исикавы для выявления и ранжирования (распределения по степени важности) имеющихся причинно-следственных связей (рис. 1).

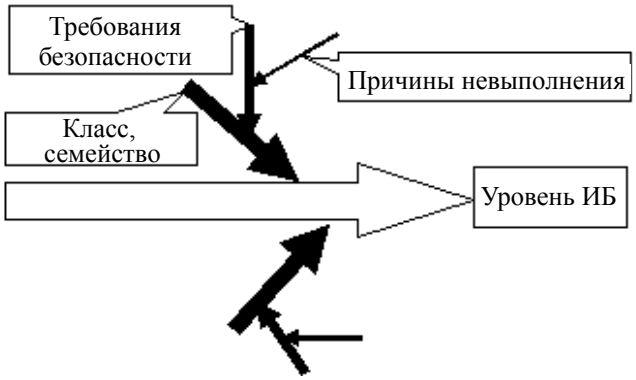

Рис. 1. Схема построения диаграммы Исикавы

Результаты причинно-следственных связей используются для построения кумулятивной кривой диаграммы Парето, позволяющей дать ответ на вопрос: «Какие причины необходимо устранить для достижения некоторой доли желаемого результата?» [1].

Фактически кумулятивная линия диаграммы Парето (рис. 2) указывает эмпирическую функцию распределения, а ступенчатая функция определяет эмпирическую плотность вероятности. Следует обратить внимание, что эмпирическая плотность вероятности по способу построения всегда будет похожей на плотности стандартных законов распределения: нормального и экспоненциального.

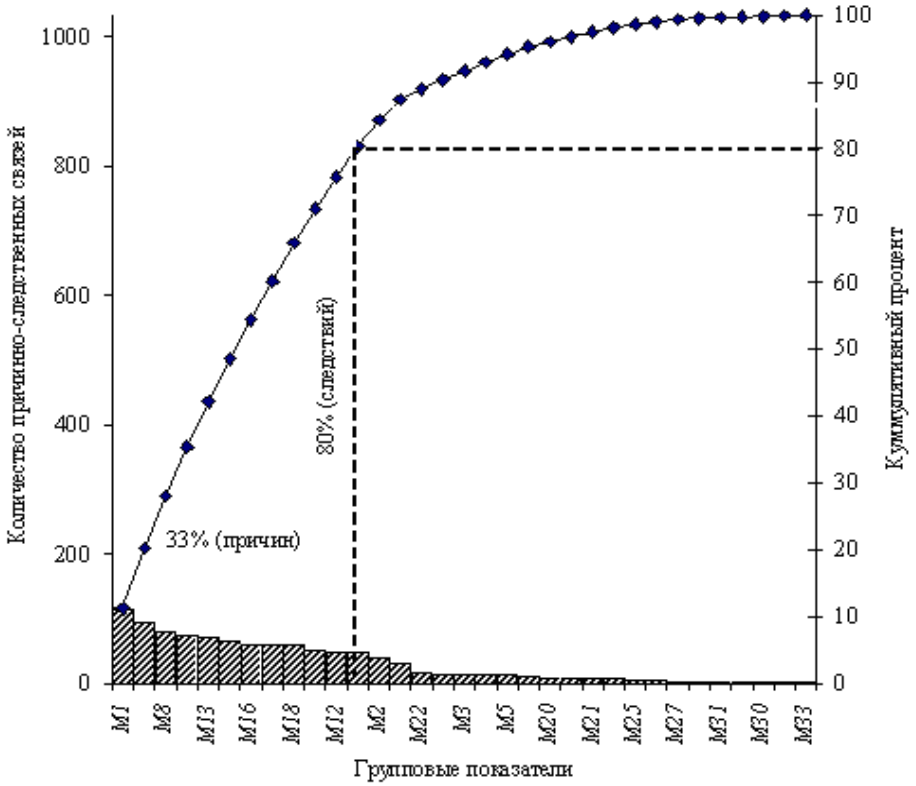

Рис. 2. Диаграмма Парето

То есть гистограмма с определенной точностью аппроксимируется или половиной гауссианы $\frac{1}{\sigma\sqrt{2\pi}}e^{-x^2/2\sigma^2}$, или экспонентой $\lambda e^{-\lambda}$ [2]. Для проведения сравнительного анализа необходимо, чтобы эмпирические данные были одной размерности со значениями функции нормального распределения. В соответствии с целями сравнения интересующей частью будет являться вторая половина нормального распределения, и поэтому следует рассматривать интеграл $\int_0^x \frac{1}{\sigma\sqrt{2\pi}}e^{-x^2/2\sigma^2}dx = 1$, тогда плотность вероятности нормального распределения равна $\frac{2}{\sigma\sqrt{2\pi}}e^{-x^2/2\sigma^2}$. С помощью метода наименьших квадратов и критерия χ^2 можно с гарантированной точностью выбрать тот закон, который наиболее точно аппроксимирует полученную гистограмму. В этом случае представляется возможным оценивать вероятность сбоя системы с требуемой точностью для большого количества показателей K. Причем чем больше будет K, тем более обоснованной будет оценка.

Рассмотрим значения ступенчатой функции $x_1,...x_K$ и определим наилучшее значения σ и λ, исходя из условий минимума функционалов:

$$J(\sigma) = \sum_{i=1}^{K}(x_i - \frac{2}{\sigma\sqrt{2\pi}}e^{-\frac{x_i^2}{2\sigma^2}})^2, \quad I(\lambda) = \sum_{i=1}^{K}(x_i - \lambda e^{-\lambda x_i})^2 .$$

Отметим, что искомые значения удобнее находить с помощью метода дихотомии, применяемого непосредственно к функционалам, а не с помощью метода Ньютона, т.к. решение нелинейных уравнений

$$\frac{\partial J}{\partial \sigma}=0, \quad \frac{\partial I}{\partial \lambda}=0$$

сопряжено с ненужными трудностями: неединственностью решения и выбором начального приближения.

Выбирая малый шаг по параметру, увеличиваем σ или λ до тех пор, пока монотонное убывание значений функционалов не сменится на монотонное возрастание. Далее, разбивая отрезок, содержащий корень, добиваемся требуемой точности и, проведя сравнение результатов, уточняем закон, которому подчиняется рассматриваемая диаграмма. Для этого необходимо подсчитать значение

$$\chi^2=\sum\frac{(\text{Э}-\text{Т})^2}{\text{Т}},$$

где Э – полученное эмпирическое значение; Т – теоретическое значение (нормальное или экспоненциальное).

Для проверки гипотезы о том, что эмпирическая функция является нормальной функцией, необходимо вычислить χ^2 при $\text{Т}=\frac{2}{\sigma\sqrt{2\pi}}e^{-x^2/2\sigma^2}$ и экспоненциальной при $\text{Т}=\lambda e^{-\lambda x}$.

Если приведенную диаграмму Парето по полученным данным наиболее точно аппроксимирует нормальный закон распределения, то это означает, что на рассматриваемые классы M адаптивно влияет множество различных факторов, причем влияние каждого из них вносит малый вклад в отклонение от нормального распределения, а их воздействия почти независимы. При полученном распределении следование принципу Парето или «Правилу 20/80», при котором 20% причин порождает 80% последствий (в нашем случае анализ показал наличие 33% влияющих причин), неприемлемо ввиду независимости этих причин, и, следовательно, для повышения уровня показателей защищенности необходимо проводить корректирующие мероприятия по всем классам и семействам функциональных показателей качества процесса защиты информации. Если же результаты подчиняются экспоненциальному закону распределения, то согласно принципу Парето для повышения уровня защищенности на 80% достаточно уделить основное внимание первым 20% показателей.

Решение задачи планирования корректирующих мероприятий

Одной из актуальных задач управления информационной безопасностью является задача эффективного планирования по проведению корректирующих мероприятий при заданном ограничении на общее время выполнения.

Данную задачу целесообразно решать методом динамического программирования, в основе которого лежит сведение задачи оптимизации к задаче определения экстремальной траектории (минимальной или максимальной длины) в некотором специальным образом построенном семействе возможных траекторий. Для решения дискретных задач метод динамического программирования сводится к определению пути максимальной или минимальной длины в специальным образом построенной сети [3].

Пусть требуется выполнить некоторый комплекс корректирующих мероприятий по повышению уровня информационной безопасности с заданным временем выполнения каждой работы t_i и некоторым эффектом u_i, под которым будем понимать определенное количество причин, которые негативно влияют (или могут повлиять) на выполнение тех или иных требований. Устранение таких причин приводит к выполнению требований к соответствующему классу M_i, а значит, и отражает повышение общего уровня информационной безопасности в целом.

Нужно выбрать подмножество корректирующих мероприятий W так, чтобы их суммарный эффект

$$U(W)=\sum_i u_i$$

был максимальным при ограничении на общее время выполнения работ $\sum_i t_i \le \text{Т}_{\text{р.д.}}$

Пусть для выполнения набора работ W_k по проведению корректирующих мероприятий для повышения уровней защищенности выделенных классов и семейств функциональных показателей качества процесса защиты M_1, M_2, M_3, M_4, M_5 отведено $\text{Т}_{\text{р.д}}$ = 100 рабочих дней. Строим на

плоскости систему координат, проводя из начала координат две дуги: одну – горизонтальную в точку (W_1, 0), а другую – наклонную в точку (W_1, 100), где 100 – время выполнения первой работы. Первая дуга соответствует случаю, когда первое мероприятие не выполняется, а вторая – когда выполняется. Из каждой полученной точки (W_1, 0) и (W_1, 100) проводим также по две дуги для второго мероприятия. Получаем четыре точки (W_2, 0), (W_2, 40), (W_2, 30) и (W_2, 70), соответствующие четырем возможным вариантам для двух работ, и т.д. В результате получаем сеть, приведенную на рис. 3.

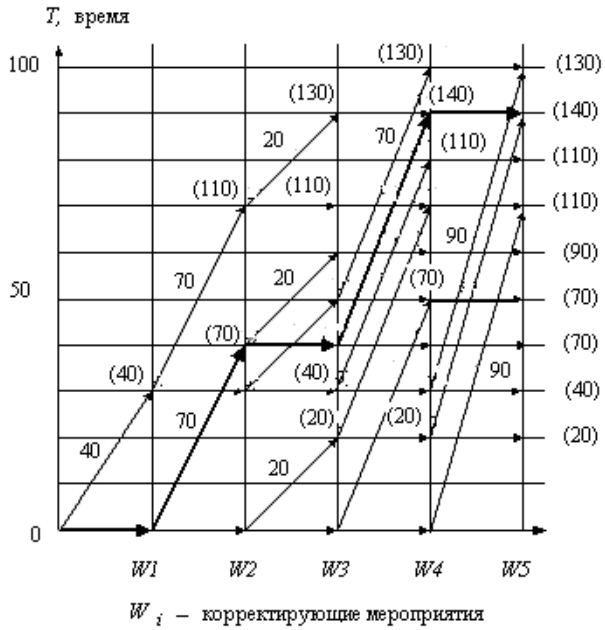

Рис. 3. Сеть для выбора выполнения работ по проведению корректирующих мероприятий

Очевидно, что любой путь в сети из начальной вершины 0 в одну из конечных вершин соответствует некоторому набору работ. И наоборот, любому набору работ с общим временем выполнения не более 100 рабочих дней однозначно соответствует путь в сети, соединяющей начальную вершину с одной из конечных. Значение координаты по второй оси равно суммарному времени выполнения корректирующих мероприятий. Если принять длины горизонтальных дуг равными, а длины наклонных равными эффекту u_i для соответствующей работы, то длина пути, соединяющего начальную вершину с одной из конечных, будет равна суммарному эффекту соответствующего набора корректирующих мероприятий. Таким образом, задача сводится к определению пути, имеющему максимальную длину. Для нашего случая путь максимальной длины выделен на рисунке жирными дугами, а суммарный эффект U равен 140.

Заключение

На основе проведенных исследований можно сделать следующие выводы:

1. Практическое применение диаграмм Исикавы и Парето для проведения анализа состояния информационной безопасности организации позволяет выявлять причинно-следственные связи между показателями уровней защищенности информации, получать их качественные и количественные характеристики.

2. На основании результатов сравнения ступенчатой функции диаграммы Парето, определяющей эмпирическую плотность вероятности, с законами распределения можно определить основные экономически выгодные решения для повышения качества информационной безопасности в целом.

3. Применение метода динамического программирования позволяет задать приоритеты выполнения корректирующих мероприятий по повышению уровня защиты информации в заданный промежуток времени, что приводит, например, к эффективному планированию деятельности сотрудника службы информационной безопасности.

Литература

1. Исикава К. Японские методы управления качеством. – М.: Экономика, 1988. – 216 с.

2. Кнут Д.Э. Искусство программирования: в 3 т.: пер. с англ. – М.: Вильямс, 2007. – Т. 2: Получисленные методы. – 768 с.

3. Беллман Р. Динамическое программирование и современная теория управления / Р. Беллман, Р. Калаба. – М.: Наука, 1969. – 118 с.

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

Толстых Егор Николаевич
Магистрант каф. комплексной защиты информации ОмГТУ
Эл. почта: t.egor@list.ru

Danilova O.T., Tolstykh Y.N.
Analysis of information security systems with the use of quality tools, and dynamic programming method

This article examines the practical application of some quality tools to analyze complex information security system (KSSI) organization in order to identify causal relationships, obtaining qualitative and quantitative level KSSI for making decisions on their effective modernization.
Keywords: information security, Pareto chart, corrective actions.