С. С. Велигодский
Сбербанк РФ,
Н. Г. Милославская
Московский инженерно-физический институт (государственный университет)

ПОКАЗАТЕЛИ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ УЯЗВИМОСТИ КОРПОРАТИВНОГО ПОРТАЛА

Количественным выражением того, что в результате недостаточного обеспечения информационной безопасности (ИБ) корпоративного портала (КП) будет полностью или частично нарушена конфиденциальность, целостность или доступность информационных ресурсов (ИР), является показатель количественной оценки параметров уязвимости.

Под уязвимостью КП понимается свойство, обусловливающее возможность реализации угроз безопасности обрабатываемой и хранимой в нем информации [1].

Если рассматривать КП как некий объект или информационную систему, о свойствах которой ничего определенного сказать нельзя (функционирование КП и системы обеспечения ИБ КП происходит в условиях неопределенности), то можно утверждать, что у данного объекта или системы с некоторой вероятностью может быть уязвимость. Тем самым уязвимость можно рассматривать как вероятностную категорию, мерой которой может быть вероятность, характеризующая ее уровень, а также возможные потери в случае ее использования. Величина этой вероятности определяется действием как внешних, так и внутренних факторов [2].

Точную оценку уязвимости портала получить невозможно, но можно выявить наиболее уязвимые места и участки и сделать прогноз об использующих их возможных угрозах ИБ для КП, т. е. оценить уровень уязвимости (УУ).

Поскольку уязвимость с рассматриваемой точки зрения носит вероятностный характер, для оценки УУ возможно применение классических принципов статистической вероятности с использованием стохастических моделей. Формой выражения являются точечные и интервальные оценки последствий полного или частичного использования уязвимости, а следовательно, и потери.

Если исходить из того, что на практике уязвимость возникает тогда, когда система обеспечения информационной безопасности (СОИБ) не способна предотвратить обнаружение или использование уязвимости злоумышленником, можно определить показатель (критерий) оценки УУ как вероятность получения фактического значения результата деятельности СОИБ (например, механизм противодействия атакам не смог ее предотвратить) КП меньше требуемого (намеченного, планируемого, прогнозируемого) значения.

$$R = \rho(X < Д_{тр}), \quad (1)$$

где R — показатель (функция распределения) оценки степени обеспечения УУ;

ρ — вероятность;

X — текущее значение результата деятельности СОИБ;

$Д_{тр}$ — требуемое (планируемое) значение результата деятельности СОИБ.

Использовать показатель R можно только после установления типа и параметров закона распределения значений результатов деятельности СОИБ КП.

Наиболее полное представление о степени обеспечения УУ (1) дает закон распределения (функция распределения или функция плотности распределения) возможных значений результатов деятельности СОИБ КП. В условиях ограниченного статистического материала обычно сложно подобрать подходящую функцию распределения.

Вместе с тем известно, что на работоспособность и безопасность КП влияет большое количество внешних и внутренних факторов, поэтому применима гипотеза, в соответствии с которой показатель УУ как случайная величина подчинен нормальному или близкому к нормальному закону распределения.

Кривая функции плотности нормального распределения представляет собой графическое изображение зависимости плотности распределения вероятностей возможных значений показателя работоспособности/безопасности (Рис. 1), где X — это случайная величина — текущее (случайное, так как условия неопределенности) значение параметра, f(x) — функция плотности распределения вероятности принимаемых случайной величиной значений.

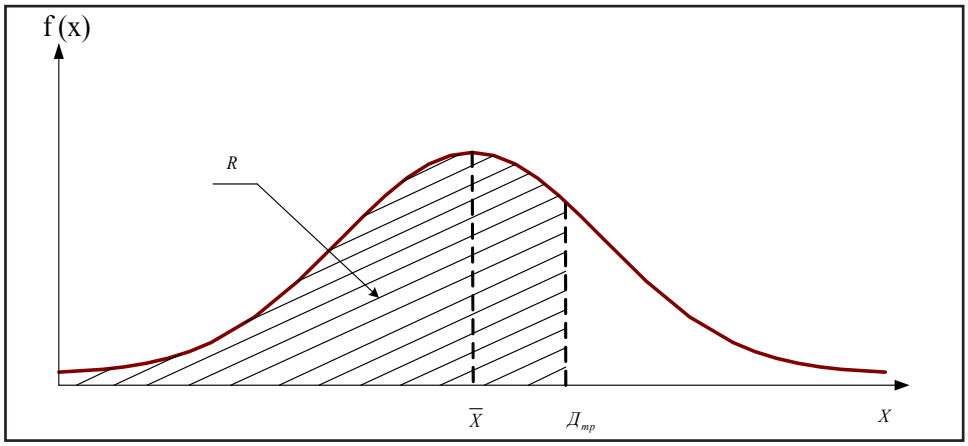

Рис. 1. Кривая плотности нормального распределения

Из кривой плотности можно увидеть, что значения результата наиболее тесно группируются вокруг величины $\overline{X}$ (кривая плотности в этой точке максимальна), а по мере убывания влево и вправо значений результатов их плотность падает.

В частности, вероятность получения показателя не ниже требуемого определяется площадью под кривой, которая для нормального закона распределения равна

$$R = \frac{1}{\sigma_x \sqrt{2\pi}} \int_{-\infty}^{Д_{тр}} e^{\frac{(x-\bar{x})^2}{2\sigma_x^2}} dx \quad , \qquad (2)$$

где $\bar{x}$, σ_x — числовые характеристики распределения: математическое ожидание и дисперсия соответственно.

Исходя из кривой плотности распределения возможных значений показателя УУ, можно построить (обычно в другой системе координат) кривую распределения вероятности уязвимости (Рис. 2) [2].

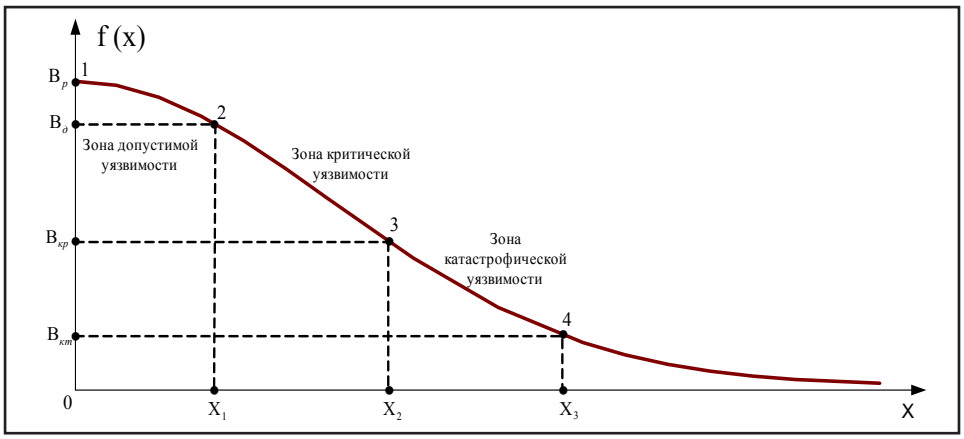

Рис. 2. Кривая уязвимости

Эта кривая имеет четыре характерные точки, каждой из которых соответствует определенное значение вероятности проявления уязвимости (рис. 2):

- точка 1 определяет вероятность B_{ρ} нулевой уязвимости — отсутствие отклонения полученных значений показателя от расчетного;
- точка 2 характеризует ожидаемую (расчетную) уязвимость, т. е. уязвимость, вероятность которой равна $B_{д}$ (допустимая уязвимость);
- точка 3 соответствует критической уязвимости, вероятность которой равна $B_{кр}$ (критическая уязвимость связана с расчетным уровнем защищенности КП);
- точка 4 характеризует катастрофическую уязвимость с вероятностью $B_{кт}$, вызывающую катастрофические для состояния КП потери.

Точка 2 определяет границу зоны допустимой уязвимости, точка 3 — границу зоны критической уязвимости, точка 4 — границу зоны катастрофической уязвимости.

Знание величин вероятностей B_{ρ}, $B_{д}$, $B_{кр}$, $B_{кт}$ достаточно для того, чтобы в подавляющем большинстве случаев правильно управлять рисками ИБ и создавать комплекс средств СОИБ КП. Но необходимо дополнительно установить предельные значения этих показателей, выше которых они не должны подниматься. Предельные значения вероятностей возникновения допустимой, критической и катастрофической уязвимостей соответственно обозначаются $К_{д}$, $К_{кр}$, $К_{кт}$. Величины этих показателей должна устанавливать и рекомендовать применяемая СОИБ КП (включая политики ИБ организации).

Можно сформулировать следующие условия допустимых масштабов потерь для КП:

- показатель допустимой уязвимости не должен превышать предельного значения ($B_{\rho} < К_{д}$);
- показатель критической уязвимости должен быть меньше предельной величины ($B_{кр} < К_{кр}$);
- показатель катастрофической уязвимости не должен быть выше предельного уровня ($B_{кт} < К_{кт}$).

При этом основная задача максимально точно определить зону допустимой уязвимости для организации эффективной работы комплекса.

Точечная оценка уязвимости КП не несет информации о ее достоверности. Поэтому необходим подход, заключающийся в определении вероятности получения результата в заданных пределах.

В частности, вероятность того, что результат примет значения, принадлежащие интервалу $[x_1, x_2]$, равна

$$R = \rho(x_1 \le x \le x_2) = F(x_2) - F(x_1). \qquad (3)$$

Для вычисления вероятности (3) осуществляют смещение и сжатие исходного нормального распределения к стандартному нормальному распределению за счет введения центрированных и нормированных случайных величин:

$$t_1 = \frac{x_1 - \bar{x}}{\sigma_x}; t_2 = \frac{x_2 - \bar{x}}{\sigma_x} .$$

Тогда вероятность получения результата в заданных пределах выражается через нормированную функцию Лапласа (интеграл вероятностей):

$$R(t) = \Phi(t_2) - \Phi(t_1) = \frac{1}{\sqrt{2\pi}} \int_{t_1}^{t_2} e^{-\frac{u^2}{2}}\, du, \qquad (4)$$

вычисляемую одним из приближенных способов [3].

Графическая интерпретация выражения (3) — вероятность того, что результат будет находиться в заданных пределах, — представлена на рис. 3. В частности, если отклонение от среднего значения ожидаемого результата — среднее квадратическое отклонение ($\bar{x} \pm \sigma$), то показатель оценки УУ равен R_1, при отклонениях ($\bar{x} \pm 2\sigma$) - R_2, а при отклонениях ($\bar{x} \pm 3\sigma$) - R_3.

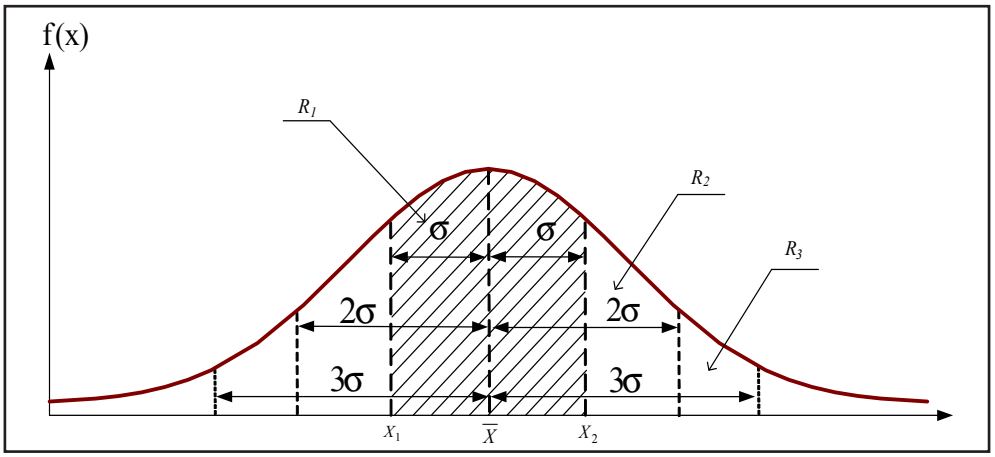

Рис. 3. Соотношение площади под кривой нормального распределения в зависимости от расстояния до $\bar{x}$

В приведенных оценках коэффициенты $U_\gamma = \{1,2,3...\}$ при среднеквадратических отклонениях являются квантилями распределения случайной величины **X** (результата операции) и определяются на основе решения уравнения:

$R(x < U_\gamma) = \gamma$,

где величина γ задана $(0 < \gamma < 1)$, а U_γ неизвестно.

Квантиль U_γ есть точка на числовой прямой, которая делит полную вероятность в отношении γ: (1– γ). Величина γ характеризует достоверность оценки УУ и в теории вероятностей называется доверительной вероятностью, или коэффициентом доверия.

Квантиль U_γ при заданном значении γ дает возможность установить границы доверительного интервала $\{x_1, x_2\}$, от которых зависит точность оценки УУ. Получить высокую точность с высоким уровнем доверительной вероятности невозможно. С увеличением достоверности оценки расширяется интервал $\{x_1, x_2\}$ так, что с высокой вероятностью можно гарантировать относительно низкую точность.

Статистические показатели по своей информативности несколько уступают вероятностным, так как в основе своей являются параметрами соответствующих законов распределения, но при этом требуют меньшего объема исходной информации для оценивания УУ.

По своему предназначению данная группа оценивает [4]:

- среднее ожидаемое значение результата действий по снижению УУ;
- разброс (изменчивость) возможного результата действий по снижению УУ относительно среднего ожидаемого значения.

Для дискретных случайных величин среднее ожидаемое значение является средневзвешенным из всех возможных значений результата $\mathbf{x_i}$ и вероятностей $\boldsymbol{\rho_i}$ его появления:

$$\bar{x} = \sum_{i=1}^{n} x_i p_i \ . \qquad (5)$$

В действительности, приходится иметь дело со статистическими аналогами приведенных ранее характеристик случайных величин, которые определяются выборочным путем. В этом случае говорят о выборочной средней:

$$\tilde{x} = \frac{\sum_{i=1}^{n} x_i}{n} \ , \qquad (6)$$

где n — число наблюдений.

Выборочные характеристики случайных величин являются оценками соответствующих вероятностных характеристик. При увеличении числа наблюдений статистические характеристики сходятся по вероятности к соответствующим математическим характеристикам и при достаточном **n** могут быть приняты приближенно равными им ($\tilde{x} \approx \bar{x}$).

Наиболее простой формой статистического показателя, характеризующего уровень уязвимости, является показатель размаха вариации ожидаемого результата

$$R = x_{max} - x_{min}, \quad (7)$$

где x_{max}, x_{min} — соответственно наибольшее и наименьшее значения результата в выборочном наблюдении.

Достоинством статистического показателя R является простота расчета. Однако размах вариации в этом случае учитывает только крайние значения результата, поэтому область его применения ограничена достаточно однородными совокупностями.

Точнее вариацию результата характеризуют статистические показатели УУ, учитывающие значимость разброса всех возможных значений результата действий на снижение УУ КП. Поскольку среднее ожидаемое значение является обобщающей характеристикой свойств рассматриваемой совокупности возможных значений результатов действий по снижению УУ, то в настоящее время наиболее распространена точка зрения, согласно которой мерой уязвимости КП следует считать дисперсию, среднее квадратическое отклонение (стандартное отклонение), коэффициент вариации.

Дисперсия как показатель УУ для дискретных случайных величин представляет собой средневзвешенную величину из квадратов отклонений действительных результатов от средних ожидаемых:

$$\sigma^2_R = \sum_{i=1}^{n} (x_i - \bar{x})^2 p_i, \quad (8)$$

где x_i — i-е значение случайной величины;

ρ_i — вероятность того, что i-я случайная величина примет значение x_i.

Для непрерывных случайных величин:

$$\sigma^2_R = \int_{-\infty}^{\infty} (x - \bar{x})^2 f(x) dx, \quad (9)$$

где $\bar{x} = \int_{-\infty}^{\infty} x f(x) dx$;

f(x) — плотность распределения случайной величины.

$$\sigma_R = \sqrt{\sigma^2_R} \quad (10)$$

является именованной величиной и указывается в тех же единицах, в каких измеряется варьирующий признак.

Статистическими аналогами приведенных характеристик, определяемых выборочным путем, являются выборочная дисперсия, выборочное, среднее квадратическое отклонение (стандартное отклонение). Выборочные характеристики случайных величин являются оценками соответствующих вероятностных характеристик.

Для выборочной дисперсии (оценка дисперсии) формула будет иметь вид:

$$\sigma^{-2}_R = \frac{\sum_{i=1}^{n} (x_i - \tilde{x})^2}{n} \text{ или } = \frac{\sum_{i=1}^{n} (x_i - \tilde{x})^2}{n-1}, \quad (11)$$

где $\tilde{x}$ — оценка средней арифметической, определяемая по формуле

$$\tilde{x} = \frac{\sum_{i=1}^{n} x_i}{n}. \quad (12)$$

Для выборочного среднего квадратического отклонения (оценка среднего квадратического отклонения) формула будет иметь вид:

$$\tilde{\sigma}_R = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \tilde{x})^2}{n}} \text{ или } = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \tilde{x})^2}{n-1}} \quad . \tag{13}$$

При увеличении числа наблюдений, очевидно, все статистические характеристики будут сходиться по вероятности к соответствующим математическим характеристикам и при достаточном **n** могут быть приняты приближенно равными им.

Поскольку уязвимость рассматривается как свойство, мерой проявления которого может быть вероятность, характеризующая УУ, вероятностные показатели оценки УУ рассчитываются на основе классических принципов статистической вероятности. При решении практических задач наиболее эффективными являются точечные и интервальные оценки УУ. Статистические показатели по своей информативности несколько уступают вероятностным, так как в основе своей являются параметрами соответствующих законов распределения, но при этом требуют меньшего объема исходной информации для оценивания УУ.

Таким образом, для снижения УУ КП до уровня допустимой уязвимости для конкретной среды функционирования КП необходимо определить базовые обязательные элементы СОИБ – политики ИБ и соответствующую нормативную базу, обеспечивающую выполнение политик; в СОИБ КП задействовать штатные средства ИБ – подсистемы идентификации и аутентификации, контроля доступа и аудита (при их наличии). Кроме того, использовать средства, предназначенные для противодействия максимальному вектору возможных атак – системы обнаружения и предотвращения вторжений с возможностью выявления аномалий как на уровне среды передачи данных, так и на прикладном уровне, что при конфликтном взаимодействии в условиях неопределенности позволит значительно снизить УУ и повысить защищенность КП.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р 50922-2006 Защита информации. Термины и определения.
2. *Пярин В. А., Кузьмин А. С., Смирнов С. Н.* Безопасность электронного бизнеса / Под ред. действительного члена РАЕН, д. т. н., проф. В. А. Минаева. М.: Гелиос АРВ, 2002.
3. *Михалевич В. С., Волкович В. Л.* Вычислительные методы исследования и проектирования сложных систем. М.: Наука, 1982.
4. *Бешелев С. Д., Гурвич Ф. Г.* Математико-статистические методы экспертных оценок. М.: Статистика, 1980.