Нечеткие оценки защищенности информационных систем

Fuzzy assessment of information system security

Ключевые слова: эффективность защиты – security efficiency, показатель защищенности – security indicator, угроза безопасности – security threat, уровень ущерба – damage level, мера опасности угрозы – threat level, коэффициент опасности – risk coefficient, дефазификация – dephasing.

В статье рассматривается оценка эффективности защиты информации в автоматизированной системе, основанная на сравнении показателей защищенности без применения технической защиты информации и ее применении в условиях нечеткого представления о степени опасности угроз.

The article covers the assessment of information security efficiency in an automated system, based on a comparison of security indicators with using the engineering information security and without it in fuzzy perceptions of threat level.

СУХАНОВ / SUKHANOV А.
Андрей Вячеславович
доктор технических наук, профессор,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербург

Во ряде научных работах [1] защищенность определяется исходя из ущерба информационной системе, связанного с реализацией угроз, носящих случайный характер, который оценивается через коэффициенты опасности угроз. Коэффициенты опасности представляются нечеткими величинами, а показатель защищенности информационной системы определяется посредством матрицы нечетких отношений между коэффициентом опасности множества угроз и степенью защищенности информационной системы.

Подход к оценке эффективности технической защиты информации в информационных системах основан на сравнении показателей защищенности без применения технической защиты информации и с применением технической защиты информации в условиях нечеткого представления о степени опасности комплекса антропогенных и техногенных угроз.

Под эффективностью понимают меру достижения цели технической защиты информации. Оценка эффективности технической защиты информации – процесс установления соответствия между результатом защиты и поставленной целью. С ростом сложности объектов анализа, состава и характеристик угроз (особенно угроз несанкционированного удаленного доступа) задача количественной оценки защищенности актуальна.

Оценка эффективности технической защиты информации возможна:

1) на основе сравнения значения показателя защищенности с нормативным (пороговым) значением;

2) на основе сравнения показателей защищенности информации без технической защиты информации и в условиях технической защиты информации. Оба подхода применяются на уровне частных моделей и методик.

Для комплексной оценки эффективности первый подход является мало приемлемым, так как сложно определить допустимые уровни снижения защищенности информации от комплекса угроз.

Второй подход применим при сравнительном анализе эффективности мер и средств защиты информации и не позволяет определить достаточность технической защиты информации.

Если защищенность информации оценивается показателем $\eta_0(t)$ без принятия мер защиты и $\eta_{\text{ТЗИ}}(t)$ в условиях технической защиты информации, то эффективность технической защиты информации может быть оценена относительным показателем [1]:

$$Э_{\text{отн}}(t) = \frac{\eta_{\text{ТЗИ}}(t) - \eta_0(t)}{\eta_0(t)}, \qquad \eta_0(t) > 0$$

Пусть известны возможные угрозы безопасности информации в информационной системе

и любая из этих угроз проявляется и реализуется за рассматриваемый период t с некоторой вероятностью $P_{\text{реал.u}}(t)$. Ущерб D_{u} от реализации u-й угрозы является величиной случайной, распределенной в интервале $[0, D_{\text{пр}}]$, где $D_{\text{пр}}$ – уровень ущерба, превышение которого неприемлемо. Если ущерб от реализации угрозы превышает $D_{\text{пр}}$, то он принимается равным $D_{\text{пр}}$. Отношение $D_{\text{u}}/D_{\text{пр}}$ будет характеризовать уровень опасности u-й угрозы и вероятность, что ущерб будет не более D_{u}. Вероятность, что уровень ущерба при реализации совокупности n из U возможных угроз не превысит величину $D_{\Sigma\text{n}}$:

$$\frac{D_{\Sigma n}}{D_{\text{пр}}} = -\frac{1}{n!}\frac{\partial^n}{\partial\lambda^n}\prod_{u=1}^{U}[(1 - P_{\text{реал.}u}(t)) + \lambda \cdot \frac{D_u}{D_{\text{пр}}}P_{\text{реал.}u}(t)]_{\lambda=0}$$

или

$$K_{\Sigma\, n} = -\frac{1}{n!}\frac{\partial^n}{\partial\lambda^n}\prod_{u=1}^{U}[1 - P_{\text{реал.}u}(t)) + \lambda \cdot K_u P_{\text{реал.}u}(t)]_{\lambda=0},$$

где λ – вспомогательный параметр, $K_{\Sigma\text{n}}$ и $K_{\text{и}}$ – отношения соответственно $D_{\Sigma\text{n}}$ и D_{u} к $D_{\text{пр}}$ назовем коэффициентами опасности угроз, так как они соответствуют уровню наносимого ущерба, вплоть до неприемлемого.

Если рассматривать все U угроз и учесть, что коэффициенты опасности являются функциями времени, то последняя формула преобразуется к виду:

$$K_{\Sigma}(t) = 1 - \prod\{1 - K_u(t) \cdot P_{\text{реал.}u}(t)\}, \qquad u = \overline{1, U}$$

Мера опасности угрозы – четко заданная величина либо нечеткая величина, характеризующая суждение эксперта об опасности угрозы. В первом случае защищенность информационной системы может быть оценена показателем – «степень защищенности»:

$$\eta(t) = \prod_{u}\{1 - K_u(t) \cdot P_{\text{реал.}u}(t)\}, \quad u = \overline{1, U}$$

Данный показатель позволяет оценить эффективность технической защиты информации как по всему множеству угроз, так и подмножеству угроз, составляющих определенную направленность: нарушение целостности, доступности или конфиденциальности информации. Достоинство показателя – полиморфизм, исключающий корректировку методов расчета в зависимости от состава угроз.

Определение коэффициентов опасности угроз в виде четких значений основано на аналитических соотношениях, связывающих эти коэффициенты с показателями ценности информации. Такие показатели в виде коэффициентов важности могут быть определены на основе эвристического анализа и категорирования информации в информационной системе по важности. Пусть информация на объекте информатизации представлена в виде файлов и для каждого файла пользователь устанавливает категорию важности информации. Например, может быть введены 4 категории важности информации:

– 1-я категория – особо важная;
– 2-я категория – очень важная;
– 3-я категория – важная;
– 4-я категория – маловажная.

При этом все угрозы разделяются на 3 группы:
– нарушение целостности;
– нарушение доступности;
– нарушение конфиденциальности информации.

Пользователем эвристически определяются коэффициенты важности f-го файла $Vz(t,f)<1$, относящегося к z-й категории.

Применительно к нарушению конфиденциальности информации соотношение для расчета коэффициентов опасности u-й угрозы имеет вид:

$$K_u(t) = 1 - \prod_{z=1}^{Z_u}\prod_{f=1}^{F_z}[1 - V_z(t,f)], \quad z = \overline{1, Z_u}$$

а для угроз, направленных на нарушение целостности и доступности информации, или для комплексных угроз коэффициент опасности:

$$K_u(t) = 1 - \prod_{z=1}^{Z_u}\prod_{f=1}^{F_z}\{1 - V_z(t,f) \cdot [1 - P_{\text{вост.}f}(t)]\}, \quad z = \overline{1, Z_u}$$

где Z_u – количество категорий важности информации, для которой u-я угроза представляет опасность; F_z – количество подлежащих защите файлов в системе, имеющих z-ю категорию важности; $P_{\text{вост.f}}(t)$ – вероятность восстановления за рассматриваемый период времени t целостности (доступности) информации, содержащейся в f-м файле (если файл не подвержен воздействию или коэффициент важности содержащейся в нем информации равен нулю, то эта вероятность тождественно равна 1).

При определении коэффициентов опасности угроз в виде нечетких величин необходимо проводить экспертный анализ опасности угроз. Такой подход может оказаться наиболее адекватным реальной опасности угроз, если анализ осуществляется высококвалифицированными специалистами. Как правило, различные эксперты по-разному

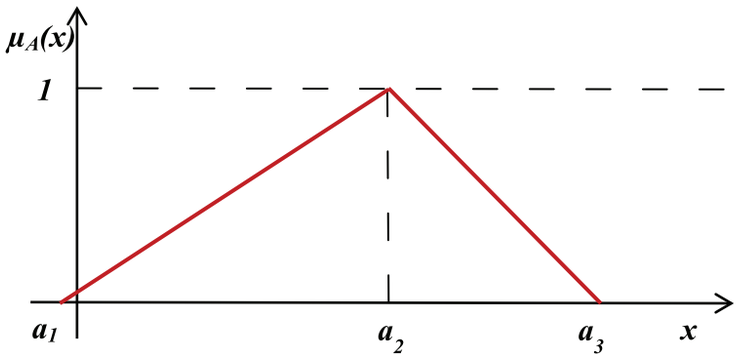

Рис. 1. Треугольное представление нечеткого числа

оценивают значение параметра и часто затрудняются задать конкретное число, поскольку существует много факторов, влияющих на оцениваемые величины и имеющих вероятностную природу. Для подобных ситуаций используется аппарат нечетких множеств, коэффициенты опасности задаются в виде нечетких чисел, способных принимать свои значения из определенного заданного интервала (множества) с различными значениями функций принадлежности [2].

Коэффициент опасности каждой угрозы описывается функцией принадлежности треугольной формы [3] (рис. 1).

То есть представляется тройкой чисел, определяющих левую и правую границу области определения, а также значение, соответствующее максимальной истинности коэффициента опасности угрозы. Значения функции принадлежности $\mu_A(x)$ для этих точек задаются так, что для средней точки это значение наибольшее, а остальные два являются нулевыми.

В соответствии с теорией нечетких множеств операции над значениями коэффициентов опасности K_u заменяются операциями над их функциями принадлежности $\mu_{Ku}(K_{ui})$. При обработке результатов опроса экспертов функция принадлежности может потерять треугольный вид.

Для случая задания коэффициентов опасности угроз нечеткими числами формула для показателя «степень защищенности» запишется в виде:

$$\eta(t) = \prod_{u=1}^{U}\left[1 - K_u(t) \circ P_{\text{реал.}u}(t)\right]$$

где операция $^\circ$ умножения нечетких чисел производится по следующему правилу:

$$\mu_D(x) = \sup_{a \cdot b = x} \min\ \mu_A(a)\mu_B(b)$$

Назовем нечеткое множество K_Σ, характеризующее опасности в информационной системе, пространством опасности (угроз) системы. Если между коэффициентом опасности множества угроз и показателем «степень защищенности» информационной системы имеется четкая зависимость, то она может быть представлена в простом виде:

$$\eta(t) = 1 - K_\Sigma(t)$$

Часто соотношение между коэффициентом опасности совокупности угроз и степенью защищенности ИС оказывается приблизительным. В этом случае необходимо определить причинные отношения между значениями этого коэффициента (предпосылками) и конечным результатом – степенью защищенности η (заключениями).

Для этих целей как ключевой момент методики экспертного оценивания эффективности средств технической защиты информации вводится матрица нечетких отношений R размерностью nxm. В матрица нечетких отношений заключены правила, определяющие причинные отношения между каждым членом предпосылок K_Σ и каждым членом заключений $\eta(t)$ [3]:

$$R = K_\Sigma \to \eta$$

Элементы матрицы $r_{ij} = \mu_R(K_\Sigma, \eta)$ должны отражать нечеткие отношения между K_Σ и η_i. Величину R можно рассматривать как нечеткое пространство на прямом произведении K_Σ x η полного пространства предпосылок K_Σ и полного пространства заключений η, а процесс получения нечеткого результата η с использованием данных K_Σ и знания $K_\Sigma^{\text{эт}} \to \eta^{\text{эт}}$ (эталонного преобразования) можно представить в виде:

$$\eta(t) = K_\Sigma(t) \cdot (K_\Sigma^{\text{эт}}(t) \to \eta^{\text{эт}}(t))$$

где знак • определяет операцию «max-min» композиции в качестве композиционного правила нечет-

кого вывода и операции взятия минимума в качестве нечеткой импликации:

$$\mu_\eta(\eta) = \max_{K_\Sigma}\{\min\ (\mu_{K_\Sigma}(K_\Sigma),\ \mu_R(K_\Sigma,\ \eta))\}.$$

Размерность матрицы нечетких отношений определяется количеством заданных числовых градаций коэффициента опасности и порогов функции принадлежности. Корректная формализация правил, с помощью которых формируется эта матрица, определит точность и достоверность конечного результата, являющегося выводом системы экспертного оценивания.

Возможны несколько вариантов построения правил вывода в зависимости от важности объекта информатизации и отношения к нему экспертов. Однако наиболее широко в экспертных оценках [3] используется набор правил, основанный на определении связи коэффициента K_Σ и показателя защищенности системы η в виде пропорциональной зависимости с равномерным уменьшением достоверности оценки. В простейшем случае значения элементов матрицы нечеткого вывода рассчитываются по формуле:

$$r_{ij} = \begin{cases} k_{\Sigma i} + \eta_j, \textit{ если эта сумма меньше } 1, \\ 0, \textit{ в противном случае.} \end{cases}$$

Оценить эффективность технической защиты информации можно, определяя степень защищенности $\eta(t)$ в условиях отсутствия и применения мер технической защиты информации. Для этого осуществляют дефаззификацию [4] одним из следующих способов;

1) задавшись требуемым уровнем функции принадлежности $\mu_\eta(\eta)$, проводят отсечение и выбирают первое приемлемое значение η:

$$\eta_\alpha = \{\eta_i \mid \mu_\eta(\eta_i) \geq \alpha\}$$

2) проводят отсечение по способу 1 и берут два крайних значения $\eta_н$ и $\eta_к$. Тогда значение коэффициента защиты будет определяться как:

$$\eta = \frac{\eta_H \mu_\eta + \eta_K \mu_\eta(\eta_K)}{\mu_\eta(\eta_H) + \mu_K(\eta_H)}$$

со степенью достоверности

$$\mu_\eta(\eta) = \mu_\eta(\eta_H) \cdot \mu_\eta(\eta_K)$$

Зная нечеткие значения и функции принадлежности коэффициентов опасности угроз, можно с учетом вероятностей реализации угроз по правилам теории нечетких множеств рассчитать нечеткие значения степени защищенности объекта информатизации от комплекса угроз.

Недостатками подобного оценивания являются статичность оценки защищенности и отсутствие взаимосвязи показателей защищенности с местоположением МЗ в структуре системы информационной безопасности.

Литература

1. *Жижелев А.В., Панфилов А.П., Язов Ю.К., Батищев Р.В.* К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств // Изв. вузов. Приборостроение. 2003. т. 46, № 7. С. 22 – 29;

2. *Кофман А.* Введение в теорию нечетких множеств. – М.: Радио и связь, 1982;

3. *Асаи К., Ватада Д., Иваи С.* и др. Прикладные нечеткие системы / Под ред. Т. Тэрано, К. Асаи, М. Сугэно. – М.: Мир, 1993;

4. *Круглов В.В., Борисов В.В.* Искусственные нейронные сети. Теория и практика.- 2-е изд., стереотип. – М.: Горячая линия - Телеком, 2002.