УДК 519.72

ВЕРОЯТНОСТНАЯ МОДЕЛЬ АЛГОРИТМА РАСЧЕТА ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.К. Джоган, В.Н. Думачев, В.В. Здольник

Воронежский институт Министерства внутренних дел Российской Федерации

Представлена членом редколлегии профессором В.И. Коноваловым

Ключевые слова и фразы: вероятностный показатель эффективности; защита информации; оценка эффективности; показатель эффективности.

Аннотации: Рассмотрены критические характеристики, используемые при конструировании систем информационной безопасности. Приведен алгоритм расчета показателя эффективности таких систем, в основу которого положены вероятностные модели распределения защитных функций.

С точки зрения применения средств обеспечения информационной безопасности наибольший интерес представляют соотношения их временных характеристик и временных характеристик процесса вскрытия защитных механизмов. При разработке систем информационной безопасности (**СИБ**), определяющим показателем эффективности является время обеспечения защитных функций [1].

Определение 1. Временем обеспечения защитных функций $\tau_{(di)}$ называется время с момента обращения к СИБ до окончания реализации ею своих функций по данному обращению.

Утверждение 1. Защитные функции СИБ считаются реализованными своевременно, если время $\tau_{(di)}$ не превышает некоторой максимально допустимой величины $\tau_{(m)}$, обусловленной стратегией вскрытия злоумышленником защитных механизмов СИБ, то есть при выполнении неравенства

$$\tau_{(di)} \le \tau_{(m)}. \qquad (1)$$

Утверждение 2. Максимальное время $\tau_{(m)}$ имеет для каждой конкретной ситуации свое конкретное значение, обусловленное активным периодом воздействия на защитный механизм, в соответствии с конкретной ситуацией и применением определенной стратегии. При этом, в общем случае, можно говорить о:

1) максимальном времени $\tau_{(m1)}$ при реализации этапа исследования механизмов идентификации и аутентификации СИБ;

2) максимальном времени $\tau_{(m2)}$ при реализации этапа контроля работы основных механизмов СИБ;

3) максимальном времени $\tau_{(m3)}$ при реализации третьего этапа несанкционированного копирования, модификации или удаления информации в информационной системе.

В общем случае обе входящие в неравенство (1) величины являются случайными, поэтому его выполнение является случайным событием. Вероятность этого события $P(\tau_{(di)} \le \tau_{(m)})$ представляет собой среднее количество ситуаций, когда СИБ своевременно реализует свои функции в течение интервала ΔT времени относительно общего числа таких ситуаций, то есть имеет место соотношение

$$P(\tau_{(di)} \le \tau_{(m)}) = \frac{1}{K}\sum_{k=1}^{K}\theta\left(\tau_{(m)}^{k} - \tau_{(di)}^{k}\right), \qquad (2)$$

где $\tau_{(di)}^{k}$ – время реализации СИБ при k-й попытке ее вскрытия; $\tau_{(m)}^{k}$ – максимально допустимое время реализации соответствующих шагов стратегии вскрытия защитных механизмов при k-й попытке; K – общее число попыток вскрытия защитных механизмов на временном интервале ΔT;

$$\theta(t) = \begin{cases} 1, & \text{при } t \ge 0, \\ 0, & \text{при } t < 0 \end{cases}$$

– единичная ступенька Хэвисайда.

С учетом изложенного можно сделать вывод о том, что вероятность $P(\tau_{(di)} \le \tau_{(m)})$ достаточно полно характеризует защищенность от вскрытия защитных механизмов. Поэтому ее целесообразно использовать в качестве показателя E эффективности СИБ, то есть

$$E = P(\tau_{(di)} \le \tau_{(m)}).$$

При этом следует говорить о защищенности механизмов доступа от исследования подсистемы доступа ее СИБ:

$$E = P(\tau_{(di)} \le \tau_{(m1)}),$$

защищенности от исследования основных механизмов СИБ:

$$E = P(\tau_{(di)} \le \tau_{(m2)}),$$

и защищенности от несанкционированного копирования, модификации или удаления информации:

$$E = P(\tau_{(di)} \le \tau_{(m3)}).$$

С целью получения выражения для $P(\tau_{(di)} \le \tau_{(m)})$ воспользуемся тем обстоятельством, что время $\tau_{(di)}$ можно представить в виде комбинации следующих времен:

– τ_{I}, затрачиваемого на реализацию первого уровня защиты информации в СИБ – идентификации и аутентификации;

– τ_{II}, затрачиваемого на реализацию второго уровня защиты информации в СИБ – обеспечения правил разграничения доступа;

– τ_{III}, затрачиваемого на реализацию третьего уровня защиты информации в СИБ – контроля целостности информации;

– τ_{IV}, затрачиваемого на реализацию четвертого уровня защиты информации в СИБ – специальных преобразований информации;

$$\tau_{(di)} = \tau_{I} + \tau_{II} + \tau_{III} + \tau_{IV}.$$

Случайный характер времени $\tau_{(di)}$ определяется тем, что его составляющие времена τ_{I}, τ_{II}, τ_{III} являются случайными, тогда как время τ_{IV} представляет собой практически детерминированную величину.

Далее, по аналогии с [2], при произвольных плотностях распределений случайных величин τ_{I}, τ_{II}, τ_{III}, $\tau_{(m)}$, соответственно, используя операции свертки, определения математического ожидания, а также сходства $P(\tau_{(di)} \le \tau_{(m)})$ с классической функцией распределения вероятностей, выражение для защищенности от вскрытия защитных механизмов можно представить в виде

$$E = P(\tau_{(di)} \le \tau_{(m2)}) = 1 - P(\tau_{(m2)} < \tau_{(di)}) = 1 - \int_{0}^{\tau_{(di)}} f_{(m)}(x)dx, \qquad (3)$$

где

$$\tau_{(di)} = \tau_{IV} + \int_{0}^{\infty} y f_{I}(y_{I})\, f_{II}(y_{II} - y_{I})\, f_{III}(x - y_{II}) dy_{I} dy_{II} dy.$$

Из общей интегральной формулы (3), задавая конкретные законы случайных величин τ_{I}, τ_{II}, τ_{III}, $\tau_{(m)}$, можно получить конкретные аналитические зависимости $P(\tau_{(di)} \le \tau_{(m)})$ защищенности от вскрытия защитных механизмов.

Анализ стратегий несанкционированного доступа к защищаемой информации [3] показывает, что случайную величину максимального времени $\tau_{(m)}$, обусловленную стратегией вскрытия злоумышленником защитных механизмов СИБ, с достаточной степенью достоверности можно аппроксимировать экспоненциальным законом распределения.

В этом случае имеет место выражение

$$f_{(m)}(\tau) = \frac{\theta(\tau - \tau_{(m)}^{\min})}{\bar{\tau}_{(m)}} e^{-\frac{\tau - \tau_{(m)}^{\min}}{\bar{\tau}_{(m)}}},$$

где $\bar{\tau}_{(m)}$ – среднее значение случайной величины $\tau_{(m)}$; $\tau_{(m)}^{\min}$ – минимальное значение $\tau_{(m)}$.

Что касается случайных величин времен τ_{I}, τ_{II}, τ_{III}, то типовыми аппроксимациями являются представления их равномерно, экспоненциально или нормально распределенными.

В этом случае имеют место следующие выражения:

$$f(\tau) = \frac{\theta(\tau - \tau^{\max}) - \theta(\tau - \tau^{\min})}{\tau^{\max} - \tau^{\min}};$$

$$f(\tau) = \frac{\theta(\tau - \tau^{\min})}{\bar{\tau}} e^{-\frac{\tau - \tau^{\min}}{\bar{\tau}}};$$

$$f(\tau)=\frac{\theta(\tau-\tau^{\min})}{\sigma\sqrt{2\pi}}\mathrm{e}^{-\frac{(\tau-\bar{\tau})^2}{2\sigma^2}},$$

где $\tau^{\max}$, $\tau^{\min}$ – максимальное и минимальное значения времени τ соответственно; $\bar{\tau}$ – среднее значение случайной величины τ; σ – среднеквадратичное отклонение τ.

С учетом изложенного выше, выражение (3) можно записать в виде

$$E=1-\frac{1}{\bar{\tau}_{(m)}}\int_{\tau_{(m)}^{\min}}^{\tau_{(di)}}\exp\left(-\frac{x-\tau_{(m)}^{\min}}{\bar{\tau}_{(m)}}\right)dx,$$

где

$$\tau_{(di)}=\int_0^{\infty}xf_{\mathrm{I}}(y_{\mathrm{I}})\,f_{\mathrm{II}}(y_{\mathrm{II}}-y_{\mathrm{I}})\,f_{\mathrm{III}}(x-y_{\mathrm{II}})dy_{\mathrm{I}}dy_{\mathrm{II}}dx.$$

Перепишем последнее выражение в виде

$$\tau_{(di)}=\int_0^{\infty}xI(x)dx.$$

В этом выражении запишем свертку $I(x)$ в пространстве Фурье

$$I(\omega)=f_{\mathrm{I}}(\omega)f_{\mathrm{II}}(\omega)f_{\mathrm{III}}(\omega).$$

Фурье-образы равномерного (р), экспоненциального (э) и нормального (н) законов распределения имеют вид

$$f(\omega)=\frac{\mathrm{e}^{-i\omega\tau^{\min}}-\mathrm{e}^{-i\omega\tau^{\max}}}{i\omega(\tau^{\max}-\tau^{\min})};\qquad(\text{р})$$

$$f(\omega)=\frac{\mathrm{e}^{-i\omega\tau^{\min}}}{\frac{1}{\bar{\tau}}+i\omega};\qquad(\text{э})$$

$$f(\omega)=\mathrm{e}^{-i\omega\bar{\tau}-\frac{\omega^2\sigma^2}{2}}.\qquad(\text{н})$$

Рассмотрим частный случай аналитического выражения для показателя эффективности защищенности от несанкционированного доступа при конкретной комбинации закона распределения случайных величин времен τ_{I}, τ_{II}, τ_{III}.

$$I(\tau)=\frac{\bar{\tau}_{\mathrm{II}}}{2(\tau_{\mathrm{I}}^{\max}-\tau_{\mathrm{I}}^{\min})}\left(\mathrm{erf}\left(-\frac{\tau-z_1}{\sqrt{2}\sigma_{\mathrm{III}}}\right)-\mathrm{erf}\left(-\frac{\tau-z_2}{\sqrt{2}\sigma_{\mathrm{III}}}\right)\right)+\frac{\bar{\tau}_{\mathrm{II}}}{2(\bar{\tau}_{\mathrm{I}}-\bar{\tau}_{\mathrm{II}})}\mathrm{e}^{-\frac{\tau-z_2}{\bar{\tau}_{\mathrm{II}}}+\frac{\sigma_{\mathrm{II}}^2}{\bar{\tau}_{\mathrm{II}}^2}}\times$$

$$\times\left(1+\mathrm{erf}\left(\frac{\tau-z_2}{\sqrt{2}\sigma_{\mathrm{III}}}-\frac{\sigma_{\mathrm{III}}}{\sqrt{2}\bar{\tau}_{II}}\right)\right)-\frac{\bar{\tau}_{\mathrm{II}}}{2(\bar{\tau}_{\mathrm{I}}-\bar{\tau}_{\mathrm{II}})}\mathrm{e}^{-\frac{\tau-z_1}{\bar{\tau}_{\mathrm{II}}}+\frac{\sigma_{\mathrm{II}}^2}{\bar{\tau}_{\mathrm{II}}^2}}\left(1+\mathrm{erf}\left(\frac{\tau-z_1}{\sqrt{2}\sigma_{\mathrm{III}}}-\frac{\sigma_{\mathrm{III}}}{\sqrt{2}\bar{\tau}_{\mathrm{II}}}\right)\right),\qquad(\text{рэн})$$

где $z_1=\tau_{\mathrm{I}}^{\max}+\tau_{\mathrm{II}}^{\min}+\bar{\tau}_{\mathrm{III}}$, $z_2=\tau_{\mathrm{I}}^{\min}+\tau_{\mathrm{II}}^{\min}+\bar{\tau}_{\mathrm{III}}$.

После соответствующих преобразований получим аналитическое выражение для $\tau_{(di)}$:

$$\tau_{(di)} = \frac{1}{\tau_{\mathrm{I}}^{\min} - \tau_{\mathrm{I}}^{\max}} \left(- \frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)^2}{2} + \frac{\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)^2}{2} \right.$$

$$- \frac{1}{2\bar{\tau}_{\mathrm{II}}^2} \mathrm{e}^{\left(\frac{1}{2}\sigma^2\bar{\tau}_{\mathrm{II}}^2 + \bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)\right)} - \frac{1}{2\bar{\tau}} \mathrm{e}^{\left(\frac{1}{2}\sigma^2\bar{\tau}_{\mathrm{II}}^2 + \bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)\right)} \times$$

$$\times \left(\frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)\left(1 + \mathrm{erf}\left(\frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}{\sigma\sqrt{2}}\right)\right)}{\bar{\tau}_{\mathrm{II}}\sqrt{\mathrm{e}^{\sigma^2\bar{\tau}_{\mathrm{II}}^2}}\,\mathrm{e}^{\bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}} + \right.$$

$$+ \frac{\sigma\sqrt{2}}{\bar{\tau}_{\mathrm{II}}\sqrt{\pi}\sqrt{\mathrm{e}^{\sigma^2\bar{\tau}_{\mathrm{II}}^2}}\,\mathrm{e}^{\bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}\sqrt{\mathrm{e}^{\frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)^2}{\sigma^2}}}} -$$

$$\left. \left. - \frac{1}{\bar{\tau}_{\mathrm{II}}^2}\mathrm{erf}\left(\frac{1}{\sqrt{2}}\sigma\bar{\tau}_{\mathrm{II}} + \frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}{\sigma\sqrt{2}}\right) + \frac{1 + \mathrm{erf}\left(\frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}{\sigma\sqrt{2}}\right)}{\bar{\tau}_{\mathrm{II}}\sqrt{\mathrm{e}^{\sigma^2\bar{\tau}_{\mathrm{II}}^2}}\,\mathrm{e}^{\bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}} \right) \right) +$$

$$+ \frac{1}{2\bar{\tau}_{\mathrm{II}}^2} \mathrm{e}^{\left(\frac{1}{2}\sigma^2\bar{\tau}_2^2 + \bar{\tau}_2\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)\right)} + \frac{1}{2} \mathrm{e}^{\left(\frac{1}{2}\sigma^2\bar{\tau}_2^2 + \bar{\tau}_2\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)\right)} \times$$

$$\times \left(\frac{\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)\left(1 + \mathrm{erf}\left(\frac{\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}{\sigma\sqrt{2}}\right)\right)}{\bar{\tau}_{\mathrm{II}}\sqrt{\mathrm{e}^{\sigma^2\bar{\tau}_{\mathrm{II}}^2}}\,\mathrm{e}^{\bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}} + \right.$$

$$+ \frac{\sigma\sqrt{2}}{\bar{\tau}_{\mathrm{II}}\sqrt{\pi}\sqrt{\mathrm{e}^{\sigma^2\bar{\tau}_{\mathrm{II}}^2}}\,\mathrm{e}^{\bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}\sqrt{\mathrm{e}^{\frac{\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)^2}{\sigma^2}}}} -$$

$$\left. \left. - \frac{1}{\bar{\tau}_{\mathrm{II}}^2}\mathrm{erf}\left(\frac{1}{\sqrt{2}}\sigma\bar{\tau}_{\mathrm{II}} + \frac{\left(\tau_{\mathrm{I}}^{\min} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}{\sigma\sqrt{2}}\right) + \frac{1 + \mathrm{erf}\left(\frac{\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}{\sigma\sqrt{2}}\right)}{\bar{\tau}_{\mathrm{II}}\sqrt{\mathrm{e}^{\sigma^2\bar{\tau}_{\mathrm{II}}^2}}\,\mathrm{e}^{\bar{\tau}_{\mathrm{II}}\left(\tau_{\mathrm{I}}^{\max} + \tau_{\mathrm{II}}^{\min} + \bar{\tau}_{\mathrm{III}}\right)}} \right) \right).$$

Подставляя это значение в выражение (3), можно рассчитать показатель эффективности E. Приведенный алгоритм может быть использован в решении широкого круга задач, связанных с оценкой эффективности мер и средств защиты информации.

Список литературы

1. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел / А.А. Чекалин [и др.]. – М. : Горячая линия – Телеком, 2006. – 313 с.

2. Джоган, В.К. Задача моделирования информационных процессов в компьютерных системах подразделений службы судебных приставов в интересах оценки уровня их защищенности / В.К. Джоган // Охрана, безопасность, связь – 2007 : материалы Всерос. науч.-практ. конф. / Воронеж. ин-т МВД России. – Воронеж, 2008. – С. 68–70.

3. Остапенко, А.Г. О возможности применения вероятностных показателей в приложениях теории информационной безопасности / А.Г. Остапенко, С.В. Скрыль // Радиотехника. – 2002. – № 11. – С. 97–100.

Stochastic Model of Calculation of Efficiency Index for Data Security Systems

V.K. Dzhogan, V.N. Dumachev, V.V. Zdolnik

Voronezh Institute of Ministry of Internal Affairs, Voronezh

Key words and phrases: data security; efficiency evaluation; efficiency index; stochastic efficiency index.

Abstract: The paper studies critical characteristics used in designing of data security systems. The algorithm of calculation of the basic index of efficiency of data security systems is propose on the basis of stochastic models of security functions distribution.

Stochastikes Modell des Algorytmes der Berechnung des Zeichnes der Effektivität der Systeme der Informationssicherheit

Zusammenfassung: Es sind die kritischen Charakteristiken, die bei dem Konstruieren der Systeme der informativen Sicherheit verwendet sind, untersucht. Aufgrund der wahrscheinlichen Modelle der Verteilung der Schutzfunktionen ist der Algorithmus der Berechnung der Hauptkennziffer der Effektivität der Systeme des technischen Schutzes der Information angeboten.

Modèle probable de l'algorithme du calcul de l'indice de l'efficacité des systèmes de la sécurité informatique

Résumé: Sont examinées les cacactéristiques critiques utilisées lors de la construction des systèmes de la garde de la sécurité informatique. A la base des modèles probables de la répartition des fonctions de garde est proposé un algorithme du calcul de l'indice essentiel de l'efficacité des systèmes de la garde technique de l'information.