Дровникова Ирина Григорьевна,
доктор технических наук, доцент;
Арутюнова Валентина Игоревна,
кандидат технических наук;
Алфёров Владимир Павлович

АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ ПРИ РЕАЛИЗАЦИИ СЛАБО УЯЗВИМОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИОННОМУ РЕСУРСУ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

AN ANALYTICAL MODEL EVALUATING THE PERFORMANCE OF THE SUBSYSTEM OF PROTECTION OF CONFIDENTIAL INFORMATION WHEN IMPLEMENTED POORLY AFFECTED ACCESS TO INFORMATION RESOURCES ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

В статье предложена аналитическая модель комплексной оценки эффективности функционирования подсистемы защиты конфиденциальных сведений, являющейся объектом управления слабо уязвимым разграничением доступа штатных пользователей к информационному ресурсу систем электронного документооборота. Для комплексной оценки используется полумарковская модель, разработанная на основе графовой формализации динамики функционирования подсистемы защиты конфиденциальных сведений.

In the article the analytical model of complex estimation of efficiency of functioning of the subsystem of protection of confidential information which is the object of weakly vulnerable access control of regular users to an information resource of systems of electronic document flow is offered. The semi-Markov model developed on the basis of graph formalization of dynamics of functioning of a subsystem of protection of confidential data is used for a complex assessment.

Для решения задач комплексной оценки эффективности мероприятий по управлению слабо уязвимым разграничением доступа (РД) к информационному ресурсу (ИР) системы электронного документооборота (СЭД) в [1] разработана система показателей эффективности функционирования подсистемы защиты конфиденциальных сведений (ПЗКС). Математическое обеспечение оценки данных показателей заключается в разработке аналитической модели комплексной оценки эффективности функционирования ПЗКС, осуществляемой путём использования комплексного показателя. Оценка комплексного показателя производится через элементарные показатели, подразделяемые на качественные (показатель функциональности ПЗКС $E_{ф}$, показатель эксплуатируемости ПЗКС $E_{э}$) и количественный (показатель своевременности реализации защиты ИР (ЗИР) $E_{с}$).

Характеризующие эффективность параметры $E_{ф}$, $E_{э}$ оцениваются с помощью проведения анализа имеющейся технической документации на программный продукт ПЗКС на основе использования качественной шкалы, позволяющей производить символьную лингвистическую оценку и, соответственно, вводить булеву независимую переменную.

Методика расчёта параметра $E_{с}$ базируется на моделировании функционирования ПЗКС в реальном времени, которую можно представить, как систему массового обслуживания [2]. Функционирование ПЗКС в режиме реального времени математически описывается на основе аппарата сетей Петри [3]. Поскольку время реализации ПЗКС защитных функций лежит в основе своевременности реализации функций ЗИР в СЭД, то в соответствии с [1] показатель $E_с$ предлагается определять по формуле:

$$E_c = P\left(\tau_c \le \tau_{\max c}\right), \tag{1}$$

где: $\tau_с$ — время реализации защитных функций ПЗКС; $\tau_{\max с}$ — максимально допустимое значение указанного времени (представляет собой случайно распределённую величину, аппроксимируемую экспоненциальным законом распределения со средним значением τ_m).

Параметр $E_с$ удобно вычислять с использованием количественной шкалы для осуществления оценки с помощью действительных чисел 0 или 1.

Для того, чтобы оценить параметр $E_с$ применимо выражение (1) с использованием графовой формализации процесса функционирования ПЗКС и разработанной на её основе полумарковской модели [4]. Используемая модель может быть описана с помощью конечного полумарковского процесса (КПМП) [5], вход в исходное и конечное состояния которого ассоциируются с обращением к ПЗКС и завершением решения подсистемой функциональных задач по конкретному обращению соответственно. Вычисление интервально-переходных вероятностей КПМП следует рассматривать в качестве основной задачи его анализа [6].

Характеризующий процесс функционирования ПЗКС КПМП можно описать с помощью полумарковской матрицы для проведения оценки параметра $E_с$:

$$H_c(\tau) = \left\| H_{c\,ij}(\tau) \right\|,\ i = \overline{1,n},\ j = \overline{1,n} \tag{2}$$

где $H_{c\,ij}(\tau)$ — случайный элемент матрицы, описывающий вероятность перехода КПМП из состояния *i* в состояние *j* за промежуток времени, меньший *τ*.

Вычисление $H_{c\,ij}(\tau)$ осуществляется по формуле:

$$H_{c\,ij}(\tau) = p_{c\,ij}\, G_{c\,i}(\tau),\ i = \overline{1,n}, \tag{3}$$

где: $p_{c\,ij}$ — вероятности перехода КПМП из состоянии *i* в состояние *j*; $G_{c\,i}(\tau)$ — функции распределения времени нахождения КПМП в состоянии *i*.

Для определения вероятностей $p_{c\,ij}$ и $G_{c\,i}(\tau)$ при $i = \overline{1,n}$, $j = \overline{1,n}$ целесообразно применение разрешающих процедур и процедур временной задержки переходов сети Петри, формально описывающей процесс функционирования ПЗКС в его динамике. При осуществлении комплексной оценки эффективности функционирования ПЗКС используются, как правило, стандартные законы распределения функций $G_{c\,i}(\tau)$, однако изначально отсутствует информация о точных значениях вероятностей $p_{c\,ij}$, поэтому заранее известными следует считать лишь их предварительные значения. Результаты, полученные путём статистической обработки данных о параметрах реализации ПЗКС защитных функций в процессе решения сервисных задач в СЭД, позволяют осуществить коррекцию значений данных вероятностей.

Параметр $E_с$, позволяющий описать вероятностно-временные характеристики (ВВХ) процесса функционирования ПЗКС в его динамике, может рассматриваться как вероятность КПМП вовремя достичь конечного состояния. Поэтому в качестве основы исследования ВВХ динамики функционирования ПЗКС следует использовать систему уравнений полных вероятностей перехода КПМП из произвольных состояний в конечное состояние в течение временного интервала, меньшего τ [6]:

$$Q_{c\,i}(\tau) = p_{c\,in} \cdot G_{c\,i}(\tau) + \sum_{j=1}^{n-1} p_{c\,ij} \cdot G_{c\,i}(\tau) * Q_{c\,j}(\tau), \quad i = \overline{1, n-1}, \tag{4}$$

где $Q_{ci}(\tau)$ — имеющий вероятностный характер параметр, характеризующий возможность КПМП перейти из состояния i в конечное состояние n за промежуток времени, меньший τ.

Построенная система интегральных уравнений (4) является результатом анализа системы уравнений интервально-переходных вероятностей КПМП, формализовано описывающего процесс функционирования ПЗКС в его динамике, и раскрывает взаимосвязь ВВХ отдельных состояний КПМП с ВВХ всего процесса в целом.

Использование преобразований Лапласа [7] позволяет упростить систему уравнений (4) для производящих функций путём преобразования её из интегральной в алгебраическую [6]:

$$q_{ci}(\nu) = p_{c\,in} \cdot g_{c\,i}(\nu) + \sum_{j=1}^{n-1} p_{c\,ij} \cdot g_{c\,i}(\nu) * Q_{c\,j}(\nu), \quad i = \overline{1, n-1}, \tag{5}$$

где: $q_{ci}(\nu)$, $g_{ci}(\nu)$ — преобразования Лапласа для производящих функций $Q_i(\tau)$ и $G_i(\tau)$ соответственно.

Применительно к полумарковской матрице $H_{cij}(\tau)$ используется следующее выражение для расчёта преобразования Лапласа её элементов:

$$h_{c\,ij}(\nu) = p_{c\,ij} \cdot g_{c\,i}(\nu). \tag{6}$$

Рассмотрим алгоритм расчёта величины $g_{ci}(\nu)$ для типовых распределений времени нахождения ПЗКС в состоянии i [7].

Если время пребывания ПЗКС в состоянии i случайным образом распределено в пределах интервала $[a_i; b_i]$ равномерно, то имеем:

$$g_{c\,i}(\nu) = \frac{\exp(-a_i\nu)\left[1 - \exp(-b_i\nu)\right]}{b_i\nu}. \tag{7}$$

При использовании экспоненциального закона распределения для описании времени пребывания ПЗКС в состоянии i со средним значением b_i величина $g_{ci}(\nu)$ может рассчитываться по формуле:

$$g_{c\,i}(\nu) = \frac{1}{1 + b_i\nu}. \tag{8}$$

В случае использования нормально распределённой случайной величины со средним значением μ_i и малой дисперсией σ_i^2 для описания времени нахождения ПЗКС в состоянии i значение $g_{ci}(\nu)$ может быть рассчитано по формуле:

$$g_{c\,i}(\nu) = \exp(-\mu_i\nu + \frac{1}{2}\sigma_i^2\nu^2) \tag{9}$$

Приняв $h_{ij} = h_{cij}(\nu)$, $q_i = q_{ci}(\nu)$ и с учётом (6) преобразуем систему уравнений (5) к следующему виду:

$$\begin{cases} (1-h_{1,1})q_1 - h_{1,2}q_2 - h_{1,3}q_3 - \ldots - h_{1,n-1}q_{n-1} = h_{1,n}; \\ -h_{2,1}q_1 + (1-h_{2,2})q_2 - h_{2,3}q_3 - \ldots - h_{2,n-1}q_{n-1} = h_{2,n}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -h_{n-1,1}q_1 - h_{n-1,2}q_2 - h_{n-1,3}q_3 - \ldots + (1-h_{n-1,n-1})q_{n-1} = h_{n-1,n}. \end{cases} \tag{10}$$

Для решения системы уравнений (10) целесообразным является использование метода исключения Гаусса в том случае, если «ведущие» коэффициенты уравнений не принимают нулевых значений [6]. Такое ограничение выполняется для представленной системы уравнений, поскольку при $i = \overline{1, n-1}$ $h_{ii} < 1$, а следовательно, коэффициенты

$(1-h_{ii})$ входящих в систему уравнений положительны.

Осуществив деление каждого члена 1-го уравнения на коэффициент $(1-h_{11})$, получим приведённое уравнение:

$$q_1 - h_{1,2}^{(1)} q_2 - h_{1,3}^{(1)} q_3 - \ldots - h_{1,n-1}^{(1)} q_{n-1} = h_{1,n}^{(1)}, \tag{11}$$

где: $h_{1,j}^{(1)} = \dfrac{h_{1,j}}{1-h_{1,1}}$, $j = \overline{2,n}$.

Исключение неизвестного q_1 из оставшихся уравнений системы (10) можно произвести путём умножения уравнения (11) на коэффициент $(-h_{i,1})$ при q_1 в каждом из уравнений при $i = \overline{2, n-1}$ и вычета результирующего уравнения из i-го уравнения.

В результате получаем следующую систему уравнений:

$$\begin{cases} q_1 - h_{1,2}^{(1)} q_2 - h_{1,3}^{(1)} q_3 - \ldots - h_{1,n-1}^{(1)} q_{n-1} = h_{1,n}^{(1)}; \\ (1-h_{2,2}^{(1)}) q_2 - h_{2,3}^{(1)} q_3 - \ldots - h_{2,n-1}^{(1)} q_{n-1} = h_{2,n}^{(1)}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -h_{n-1,2}^{(1)} q_2 - h_{n-1,3}^{(1)} q_3 - \ldots + (1-h_{n-1,n-1}^{(1)}) q_{n-1} = h_{n-1,n}^{(1)}. \end{cases}, \tag{12}$$

где: $h_{i,j}^{(1)} = h_{i,j} + h_{i,1} h_{1,j}^{(1)}$, $i = \overline{2, n-1}$, $j = \overline{2, n}$. (13)

Аналогичным образом, путём использования прямого хода метода Гаусса, исключим неизвестное q_2 из системы уравнений (12). В итоге получим коэффициенты, рассчитываемые по формулам (13).

В результате многократного проведения описанных преобразований получим следующую систему приведённых уравнений:

$$\begin{cases} q_1 - h_{1,2}^{(1)} q_2 - h_{1,3}^{(1)} q_3 - \ldots - h_{1,n-1}^{(1)} q_{n-1} = h_{1,n}^{(1)}; \\ \qquad q_2 - h_{2,3}^{(2)} q_3 - \ldots - h_{2,n-1}^{(2)} q_{n-1} = h_{2,n}^{(2)}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad\qquad q_{n-1} = h_{n-1,n}^{(n-1)}. \end{cases}, \tag{14}$$

где: $h_{k,j}^{(k)} = \dfrac{h_{k,j}^{(k-1)}}{1-h_{k,k}^{(k-1)}}$, $h_{i,j}^{(k)} = h_{i,j}^{(k-1)} + h_{i,k}^{(k-1)} h_{k,j}^{(k)}$, $h_{ij}^{(0)} = h_{ij}$, $k = \overline{1, n-1}$, $i = \overline{k+1, n-1}$, $j = \overline{k+1, n}$. (15)

На основе применения обратного хода метода Гаусса далее можно последовательно найти неизвестные системы уравнений:

$$\begin{cases} q_{n-1} = h_{n-1,n}^{(n-1)}; \\ q_{n-2} = h_{n-2,n}^{(n-2)} + h_{n-2,n-1}^{(n-2)} q_{n-1}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ q_1 = h_{1,n}^{(1)} + h_{1,n-1}^{(1)} q_{n-1} + h_{1,n-2}^{(1)} q_{n-2} + \ldots + h_{1,2}^{(1)} q_2. \end{cases} \tag{16}$$

Характеризующий ВВХ динамики функционирования ПЗКС показатель своевременности реализации ЗИР E_c, вычисленный по формуле (1), можно выразить через ВВХ выполнения функций по ЗИР ПЗКС, используя выражение:

$$E_c = q_{c1}(\nu_m), \tag{17}$$

где: $\nu_m = \dfrac{1}{\tau_m}$ — параметр показательного закона распределения случайной величины (максимальное значение) $\tau_{\max c}$; τ_m — математическое ожидание $\tau_{\max c}$.

Учитывая, что при расчёте параметра E_c в роли аргумента ν может быть использована характеристика v_m, будем придерживаться следующей методики определения указанного параметра: на первом этапе осуществляется процедура вычисления $g_i(v_m)$ по формулам (7) — (9), на втором этапе — величины $h_{ij}(v_m)$ согласно выражению (6), на третьем — коэффициентов системы уравнений (14) с использованием формулы (15). Окончательный расчёт параметра $E_с$, определённого (17), вычисляется на основе (16), учитывая, что $v = v_m$.

Максимальную величину любого из рассчитанных параметров можно воспринимать как оптимальное значение качества функционирования ПЗКС по данному вычисляемому параметру.

При проведении процедуры комплексной оценки эффективности эксплуатации ПЗКС в качестве управляемого объекта слабо уязвимым РД необходимо использовать комплексный параметр $E_к$, интегрирующий частные параметры эффективности.

Для определения интегрального $E_к$ необходимо проанализировать частные параметры эффективности функционирования ПЗКС. Поскольку качественные показатели $E_ф$ и $E_э$ являются булево значимыми переменными их не рекомендуется использовать как интегральный параметр, учитывая их ограничения:

$$E_ф = 1;\ E_э = 1, \tag{18}$$

которые представляют собой единое ограничение:

$$E_ф \wedge E_э = 1. \tag{19}$$

Методика расчёта параметра $E_с$ приведена ниже. Общие требования, предъявляемые к оперативности СЭД, имеют ограничение на эксплуатацию ПЗКС, которое можно распространить и на $E_с$:

$$E_c \geq E_{\min c}, \tag{20}$$

где $E_{\min с}$ — наименьшее значение $E_с$, определённое требованиями к ПЗКС от несанкционированного доступа в технической документации на эксплуатацию СЭД.

Таким образом, окончательное выражение для вычисления интегрального параметра эффективности функционирования ПЗКС может быть представлено в виде:

$$E_к = \begin{cases} E_c, & если \quad \left(E_c \geq E_{\min c}\right) \wedge E_ф \wedge E_э = 1, \\ 0, & иначе. \end{cases} \tag{21}$$

Выше изложенное позволяет сделать вывод о том, что разработана математическая модель для оценки показателей эффективности эксплуатации ПЗКС как объекта управления процессом слабо уязвимого РД штатных пользователей к ИР в СЭД. Комплексная оценка эффективности эксплуатации ПЗКС адекватна оценке показателя своевременности реализации ЗИР при допущении, что значение показателя $E_с$ не будет меньшим фиксированного значения $E_{\min с}$, а оставшиеся имеющиеся частные элементарные параметры являются допустимыми. При оценке параметра $E_с$ использована полумарковская модель, созданная на базе формальной модели динамики эксплуатации ПЗКС в СЭД в режиме реального времени.

ЛИТЕРАТУРА

1. Дровникова И.Г. Моделирование оценки эффективности функционирования подсистемы защиты конфиденциальных сведений систем автоматизированного документооборота / И.Г. Дровникова, В.П. Алфёров // Общественная безопасность, законность и правопорядок в III тысячелетии: сб. ст. Междунар. науч.-практич. конф. (Воронеж, 27 июня 2018 г.). — В. 4. — Ч. 2.– 2018. — С. 32-35.

2. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного до-

кументооборота: монография / И.И. Застрожнов [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2015. — 106 с.

3. Мараховский В.Б. Моделирование параллельных процессов. Сети Петри / В.Б. Мараховский, Л.Я. Розенблюм, А.В. Яковлев. — СПб.: Профессиональная литература, 2014. — 400 с.

4. Рогозин Е.А. Разработка модели функционирования типовой системы защиты информации от несанкционированного доступа на основе теории графов с конечным числом состояний / Е.А. Рогозин, А.Д. Попов, В.В. Конобеевских // Проблемы обеспечения надёжности и качества приборов, устройств и систем: межвуз. сб. науч. тр. — Воронеж: ВГТУ, 2017. — С. 34-40.

5. Королюк В.С. Полумарковские процессы и их приложения / В.С. Королюк, А.Ф. Турбин. — Киев: Наукова думка, 1976. — 184 с.

6. Авсентьев О.С. Методика управления защитой информационного ресурса системы электронного документооборота / О.С. Авсентьев, И.Г. Дровникова, И.И. Застрожнов, А.Д. Попов, Е.А. Рогозин // Труды СПИИРАН. № 2 (57) (2018). — С.-Пб.: СПИИРАН, 2018. — 2018. — № 2(57). — С. 188-210. — DOI 10.15622/sp.57.8.

7. Глушко А.В. Преобразование Лапласа. Свойства и применения: пособие по спецкурсу / А.В. Глушко, В.П. Глушко. — Воронеж: ВГУ, 2004. — 59 с.