16. Powers, R. New criteria and a new algorithm for learning in multi-agent systems [Electronic resource] / R. Powers, Y. Shoham // In Advances in Neural Information Processing Systems. — MIT Press, 2005. — Available at: \www/URL: http://robotics.stanford.edu/~shoham/www%20papers/PowersShoham_Criteria_NIPS05.pdf
17. Myerson, R. B. Optimal coordination mechanisms in generalized principal-agent problems [Text] / R. B. Myerson // Journal of Mathematical Economics. — 1982. — Vol. 10, № 1. — P. 67–81. doi:10.1016/0304-4068(82)90006-4

РОЗРОБКА МОДЕЛІ КООРДИНАЦІЇ СИЛ ТА ЗАСОБІВ В ІЄРАРХІЧНІЙ СИСТЕМІ ЦИВІЛЬНОГО ЗАХИСТУ НАСЕЛЕННЯ

Запропоновано звести задачу координації в слабкоструктурованій ієрархічній системі цивільного захисту населення до задачі підтримки цілеспрямованого кооперативного прийняття рішень. Показано, що неявна координація може розглядатися як процес спільного пошуку рішень агентами в багатоагентній моделі з нормативним регулятором, а явна координація — як процес узгодження планів агентів.

Ключові слова: ієрархічна система, координація, багатоагентна модель, нормативний регулятор.

Ляшенко Елена Николаевна, *кандидат технических наук, доцент, кафедра информационных технологий, Херсонский национальный технический университет, Украина,* ***e-mail: lunaways@mail.ru****.*
Шерстюк Владимир Григорьевич, *доктор технических наук, профессор, кафедра информационных технологий, Херсонский национальный технический университет, Украина,*
e-mail: v_sherstyuk@bigmir.net*.*

Ляшенко Олена Миколаївна, *кандидат технічних наук, доцент, кафедра інформаційних технологій, Херсонський національний технічний університет, Україна.*
Шерстюк Володимир Григорович, *доктор технічних наук, професор, кафедра інформаційних технологій, Херсонський національний технічний університет, Україна.*

Liashenko Olena, *Kherson National Technical University, Ukraine,*
e-mail: lunaways@mail.ru*.*
Sherstyuk Vladimir, *Kherson National Technical University, Ukraine,*
e-mail: v_sherstyuk@bigmir.net

УДК 004.056
DOI: 10.15587/2312-8372.2015.47183

Шапорин В. О., Плачинда О. Е.

РАЗРАБОТКА МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОЦЕНКИ ВРЕДА АКТИВАМ

Предложены модели, описывающие поведение информационной системы при осуществлении сценариев угроз информационной безопасности. Для описания параметров значений использованы нечеткие лингвистические оценки. Для описания самих сценариев используется аппарат сетей Петри-Маркова. Для описания всего процесса оценки активов использована методология Coras. В совокупности получена модель, позволяющая описать влияние осуществления сценариев угроз на оценку активов системы.

Ключевые слова: *актив, угроза, методология Coras, нечеткие базы знаний, лингвистические переменные.*

1. Введение

Анализ рисков информационной безопасности является важной составляющей при проектировании систем безопасности информационных систем. Точность, объективность и компетентность действий команды проектировщиков, напрямую влияют на адекватность оценки того, какие активы организации необходимо защитить, какие риски угрожают им, и какие меры исправления и предотвращения необходимо применить [1].

На сегодняшний день процесс анализа рисков информационной безопасности сводится к действиям разработчиков, основанным на личном опыте. Существуют также и инструментальные средства анализа, которые основаны на построении оценок и выводов в терминах теории вероятностей [2]. Первый вариант требует высокой квалификации одного или нескольких архитекторов безопасности, достигнутых в результате длительного обучения, и не всегда позволяют дать объективную оценку в конкретной ситуации. Второй вариант предусматривает построение вероятностных зависимостей и функций распределения, что не всегда дает точный результат, а также не позволяет использовать накопленный опыт проектировщиков.

2. Анализ литературных данных и постановка проблемы

В области анализа рисков существует достаточное количество методологий и стандартов [2], однако наиболее удобной системой, с точки зрения поставленной задачи, является методология Coras [3]. Данная методология имеет достаточный набор элементов для построения анализа рисков, а также имеет возможность использовать значения данных элементов в терминах нечеткой логики [4].

Однако, теория нечетких множеств для построения оценок активов, взаимоотношений и описания других элементов, введенных с помощью методологии Coras практически не использовалась.

При описании нечетких параметров необходимо описать нечеткие значения, которые они принимают.

Чтобы избежать многозначности трактовки семантических значений одного и того же параметра в различных ситуациях, построим полные ортогональные семантические пространства, которые будут служить областями нечетких значений каждого из параметров вне зависимости от рассматриваемой системы.

Для построения полного ортогонального семантического пространства (ПОСП) некоторого нечеткого параметра $\tilde{p}_i$ определим множества нечетких значений $\tilde{D}_i = \{\tilde{p}_i^k\}_{k=1..K_i}$, где K_i — количество нечетких значений, принимаемых i-м параметром. Зададим эти нечеткие значения в виде нечетких чисел с треугольной функцией принадлежности μ_i^k, которая положительно определена на некотором интервале (p_{ib}^k, p_{ie}^k), где $p_{ib}^k, p_{ie}^k \in D_i$ — значения начала и конца интервала соответственно, а D_i — базовое множество нечетких значений параметра $\tilde{p}_i$. Для того чтобы построенные множества $\tilde{D}_i$ являлись ПОСП, необходимо, чтобы они удовлетворяли следующим аксиомам [4].

Пусть для параметра $\tilde{p}_i$ дан набор чисел $\left\{a_{ij}\right\}_{j=0}^{n}$, определяемый соотношениями:

$$a_{ij} = a_i + \frac{(b_i - a_i)}{n_i} j, \quad j = 0,...,n_i, \tag{1}$$

где $D_i = [a_i, b_i]$ — некоторый заданный сегмент на действительной оси, а n_i — некоторое целое число.

Используя данный набор чисел можно построить полное ортогональное семантическое пространство $\Xi_A(i)$, термы которого задаются формулой:

$$A_{ij} = \begin{cases} (a_i, a_i, a_{i1}), & j = 0, \\ (a_{ij-1}, a_{ij}, a_{ij+1}), & 1 \le i < n_i, \\ (a_{in_i-1}, a_{in_i}, a_{in_i}), & i = n_i, \end{cases} \tag{2}$$

где через $A = (a_{\min}, a, a_{\max})$ обозначается треугольное нечеткое число, функция принадлежности $\mu_A(x)$ которого определяется формулой:

$$\mu_A(x) = \begin{cases} 0, & x < a_{\min}, x > a_{\max}, \\ \dfrac{x - a_{\min}}{a - a_{\min}}, & a_{\min} \le x \le a, \\ 1, & x = a, \\ \dfrac{a_{\max} - x}{a_{\max} - a}, & a \le x \le a_{\max}. \end{cases} \tag{3}$$

В общем случае, нечеткое треугольное число $S_i = (s_{i\min}, s_i, s_{i\max})$, которое описывает значение параметра $\tilde{p}_i$, не будет совпадать ни с одним из нечетких значений из ПОСП Ξ_A. Для определения соответствия полученного значения какому-либо из нечетких значений ПОСП Ξ_A, можно использовать разные метрические отношения.

3. Объект, цель и задачи исследования

Объект исследования — поведение информационных систем при осуществлении сценариев угроз информационной безопасности.

Данная работа посвящена разработке систем, которые позволят формализовать и использовать опыт профессиональных проектировщиков и администраторов, и применять при оценивании активов и рисков системы качественные оценки, более близкие участникам системы и владельцам активов.

Для достижения поставленной цели были поставлены следующие задачи:

1. Выявление активов системы, а также выявление элементов, влияющих на данные активы, их оценивание и построение взаимоотношений между ними.
2. Построение моделей атак, задействованных в рассматриваемом случае.
3. Построение формализованной модели анализа рисков с помощью методологии Coras.

4. Модели поведения информационной системы при осуществлении сценариев угроз информационной безопасности

Зададим соответствующее метрическое отношение формулой:

$$S_i(\Xi) = \arg\min_j f_d(A_{ij}, S_i), \tag{4}$$

где

$$f_d(A_{ij}, S_i) = | s_i - a_{ij} |. \tag{5}$$

Тогда справедливо следующее утверждение.

Теорема 1. Пусть дано ПОСП $\Xi_A(i)$ определенное соотношениями (2). А соответствие нечеткого треугольного числа $S_i = (s_{i\min}, s_i, s_{i\max})$, нечеткому значению A_{ij} из ПОСП $\Xi_A(i)$, устанавливается с помощью соотношений (4), (5). Тогда нечеткое число $S_i(\Xi)$ определяется соотношением:

$$S_i(\Xi) = \begin{cases} A_{i,\left[\frac{s_i - a_i}{b_i - a_i} n_i\right]+1}, & \dfrac{s_i - a_i}{b_i - a_i} n_i - \left[\dfrac{s_i - a_i}{b_i - a_i} n_i\right] > 0{,}5, \\ A_{\left[\frac{s_i - a_i}{b_i - a_i} n_i\right]}, & \dfrac{s_i - a_i}{b_i - a_i} n_i - \left[\dfrac{s_i - a_i}{b_i - a_i} n_i\right] \le 0{,}5. \end{cases} \tag{6}$$

Применяя полученный результат можно описать несколько вспомогательных моделей.

Обозначим через $\tilde{x} = \{x_b, x, x_e\}$, $\tilde{y} = \{y_b, y, y_e\}$ и $\tilde{z} = \{z_b, z, z_e\}$ некоторые нечеткие числа с функциями принадлежности вида (3). Тогда согласно [5] можно написать:

$$\tilde{z} = \tilde{x} @ \tilde{y} = \bigcup_\alpha z_\alpha = \bigcup_\alpha x_\alpha @ y_\alpha. \tag{7}$$

где $x_\alpha, y_\alpha, z_\alpha$ — α-уровни нечетких значений $\tilde{x}, \tilde{y}, \tilde{z}$ соответственно; а символом @ обозначается один из символов $\{+, -, \cdot, /\}$. При этом справедливы следующие соотношения:

$$\begin{aligned} & x_\alpha + y_\alpha = \{x_{\alpha b} + y_{\alpha b}, x_{\alpha e} + y_{\alpha e}\}; \\ & x_\alpha - y_\alpha = \{x_{\alpha b} - y_{\alpha e}, x_{\alpha e} - y_{\alpha b}\}; \\ & x_\alpha \cdot y_\alpha = \{\min(x_{\alpha b} \cdot y_{\alpha b}, x_{\alpha b} \cdot y_{\alpha e}, x_{\alpha e} \cdot y_{\alpha b}, x_{\alpha e} \cdot y_{\alpha e}), \\ & \max(x_{\alpha b} \cdot y_{\alpha b}, x_{\alpha b} \cdot y_{\alpha e}, x_{\alpha e} \cdot y_{\alpha b}, x_{\alpha e} \cdot y_{\alpha e})\}; \\ & \frac{x_\alpha}{y_\alpha} = x_\alpha \cdot \frac{1}{y_\alpha} = \\ & = \left\{\min\left(\frac{x_{\alpha b}}{y_{\alpha b}}, \frac{x_{\alpha b}}{y_{\alpha e}}, \frac{x_{\alpha e}}{y_{\alpha b}}, \frac{x_{\alpha e}}{y_{\alpha e}}\right), \max\left(\frac{x_{\alpha b}}{y_{\alpha b}}, \frac{x_{\alpha b}}{y_{\alpha e}}, \frac{x_{\alpha e}}{y_{\alpha b}}, \frac{x_{\alpha e}}{y_{\alpha e}}\right)\right\}. \end{aligned} \tag{8}$$

Учитывая треугольность функций принадлежности, можно (7) с учетом (8) переписать в следующем виде:

$$\tilde{z}=\tilde{x}+\tilde{y}=\{x_b+y_b, x+y, x_e+y_e\},$$
$$\tilde{z}=\tilde{x}-\tilde{y}=\{x_b-y_e, x-y, x_e-y_b\},$$
$$\tilde{z}=\tilde{x}\cdot\tilde{y}=\{x_b\cdot y_b, x\cdot y, x_e\cdot y_e\},$$
$$\tilde{z}=\frac{\tilde{x}}{\tilde{y}}=\left\{\frac{x_b}{y_e},\frac{x}{y},\frac{x_e}{y_b}\right\}. \quad (9)$$

Модель 1. Пусть заданы множества входных параметров $\tilde{X}=\{\tilde{x}_i\}$, $\tilde{A}=\{\tilde{a}_i\}$, $\tilde{X}\cap\tilde{A}=\varnothing$ и выходной параметр $\tilde{y}$, причем, каждый параметр является нечетким и его значение определяется функцией принадлежности типа (3). Тогда каждый параметр будет определяться следующими значениями:

$$\tilde{x}_i=\{x_{ib}, x_i, x_{ie}\},$$
$$\tilde{a}_i=\{a_{ib}, a_i, a_{ie}\},$$
$$\tilde{y}=\{y_b, y, y_e\}.$$

Рассмотрим случай, когда отображение имеет следующий вид:

$$\tilde{y}=\sum_i \tilde{a}_i\tilde{x}_i. \quad (10)$$

Применяя для решения соотношения (10) формулы (4), (5) получим нечеткое значение параметра $\tilde{y}$, которое определяется следующим выражением:

$$\tilde{y}=\arg\min_{k=1..K_y} f_d(\tilde{y}^k, y').$$

Здесь y' нечеткое треугольное число определяемое соотношениями:

$$y'=\left(\sum_i a_{ib}x_{ib}, \sum_i a_i x_i, \sum_i a_{ie}x_{ie}\right). \quad (11)$$

Модель 2. Пусть заданы множества входных параметров $\tilde{X}=\{\tilde{x}_i\}$, $\tilde{A}=\{\tilde{a}_i\}$, $\tilde{X}\cap\tilde{A}=\varnothing$ и выходной параметр $\tilde{y}$, причем, каждый параметр является нечетким и его значение определяется функцией принадлежности типа (3). Тогда каждый параметр будет определяться следующими значениями:

$$\tilde{x}_i=\{x_{ib}, x_i, x_{ie}\},$$
$$\tilde{a}_i=\{a_{ib}, a_i, a_{ie}\},$$
$$\tilde{y}=\{y_b, y, y_e\}.$$

Рассмотрим случай, когда выходное отображение имеет следующий вид:

$$\tilde{y}=\frac{1}{\sum_i \tilde{a}_i}\sum_i \tilde{a}_i\tilde{x}_i. \quad (12)$$

Применяя для соотношения (12) формулы (4), (5) получим нечеткое значение параметра $\tilde{y}$, которое определяется следующим выражением:

$$\tilde{y}=\arg\min_{k=1..K_y} f_d(\tilde{y}_i^k, y_i').$$

Здесь y' нечеткое треугольное число определяемое соотношениями:

$$y'=(z_2, z_3, z_1), \quad (13)$$

где

$$z_1=\frac{1}{\sum_i a_{ib}}\sum_i a_{ie}x_{ie};\ z_2=\frac{1}{\sum_i a_{ie}}\sum_i a_{ib}x_{ib};$$
$$z_3=\frac{1}{\sum_i a_i}\sum_i a_i x_i.$$

Модель 3. Данная модель используется в некоторых задачах для определения функций принадлежности в случае, когда некоторые нечеткие переменные, применяемые в задачах, определяются с помощью функциональной зависимости вида:

$$\tilde{y}=g(\tilde{x})=1-e^{\tilde{x}},$$

где

$$\tilde{x}=\{x_b, x, x_e\}\in\tilde{P}_X,$$
$$\tilde{y}=\{y_b, y, y_e\}\in\tilde{P}_Y.$$

Проблема состоит в том, чтобы оценить функцию принадлежности, которая наилучшим образом определяет данное соотношение.

Функция $g(x)=1-e^x$ является функцией, определенной на всем множестве P_X, которая представляет собой отображение из множества P_X в множество P_Y. Это отображение индуцирует отображение $g(\tilde{x})$ из множества $\tilde{P}_X$ в множество $\tilde{P}_Y$: $\tilde{y}=g(\tilde{x})$. Такое преобразование можно определить следующим образом: $g(\tilde{x})$ есть нечеткое число, определенное на множестве P_Y с функцией принадлежности $\mu_y(y)$, где $\mu_y(y)=\mu_y(g(x))=\mu_x(g^{-1}(y))$. Отсюда видно, что:

$$\mu_y(y)=\begin{cases}1, & y=1-e^x,\\ 0, & y\le 1-e^{x_b}, y\ge 1-e^{x_e}.\end{cases} \quad (14)$$

Описывая функцию принадлежности параметра $\tilde{y}$ в виде (3), и принимая во внимание (14), можно записать:

$$y_b=1-e^{x_e}, y=1-e^x, y_e=1-e^{x_b}. \quad (15)$$

Так как $g^{-1}(y)=\ln(y)$ и учитывая соотношения (14), опишем функцию принадлежности $\mu_y(y)$:

$$\mu_y(t)=\mu_x(\ln(1-t))=\begin{cases}0, \quad t\le y_b, t\ge y_e,\\ \dfrac{\ln(1-t)-\ln(1-y_b)}{\ln(1-y)-\ln(1-y_b)}, y_b<t<y,\\ 1, \quad t=y,\\ \dfrac{\ln(1-t)-\ln(1-y_e)}{\ln(1-y)-\ln(1-y_e)}, y<t<y_e.\end{cases} \quad (16)$$

Полученная функция принадлежности $\mu_y(y)$ не является треугольной, так как на интервалах (y_b, y) и (y, y_e) имеет логарифмический вид. Можно определить трапецеидальную функцию, аппроксимирующую функцию вида (15) и сформулировать следующий результат, характеризующий степень приближения рассматриваемой функции.

Теорема 2. При малых значениях величин $|y_b - y|$ и $|y_e - y|$ функцию (16) можно аппроксимировать функцией вида (17):

$$\mu_y(t) = \begin{cases} 0, \quad t \le y_b, t \ge y_e; \\ \dfrac{t - y_b}{y - y_b}, y_b < t < y_{b_1}; \\ \quad 1, \quad t = y; \\ \dfrac{t - y_e}{y - y_e}, y < t < y_e. \end{cases} \qquad (17)$$

5. Процесс оценки активов с использованием методологии Coras

При построении диаграмм Coras [6, 7] следует определить центральный элемент диаграммы, вокруг которого будет строиться система вывода. Таким элементом может быть актив или несколько активов системы, или угрозы информационной безопасности системы. На рис. 1 представлена диаграмма, иллюстрирующая влияние некомпетентности легальных пользователей на активы, интересующие владельцев системы.

В диаграмме приняты следующие элементы:

— угроза. Пользователь, который своими действиями привел к инцидентам безопасности системы;

— сценарии угроз. Последовательность действий, которая реализует соответствующую атаку на систему;

— нежелательный инцидент. Ситуация к которой привела реализация сценария угрозы или другой инцидент;

— активы. Целевые элементы системы, оценку которых снижает реализация сценариев и инцидентов.

Данная диаграмма имеет единственный элемент «пользователь» из множества угроз $T = \{U\}$. Три сценария угроз — дискредитация логинов и паролей (DLP), некорректное использование почтовых (FMS) и поисковых (FSS) систем, составляют подмножество $T = \{DLP, FMS, FSS\}$.

Сценарии приводят к нежелательным инцидентам, множество которых составляет $U1 = \{HSP, HLE, VID, UGB, USB\}$, где HSP — инцидент перехвата идентификационных данных злоумышленником, HLE — вход злоумышленника в систему с правами пользователя, VID — инфицирование вирусом устройств пользователя, UGB — переход устройства пользователя под контроль вируса или злоумышленника, USB — блокировка работы системы пользователя.

Множество активов определено как $A = \{Dc, PDc, SYSi, PDa, DEVi\}$, где Dc — конфиденциальность корпоративных данных, PDc — конфиденциальность личных данных, $SYSi$ — целостность информационной системы, PDa — доступность личных данных, $DEVi$ — целостность устройств пользователя.

Все элементы диаграммы имеют свои лингвистические оценки, которые, как правило, характеризуют вероятность реализации процессов связанных с данным элементом. Наибольший интерес представляют такие элементы, как сценарии угроз, которые зависят от параметров системы и изменения которых влияют на конечный результат. Соответственно, необходимо иметь описания данных внутренних параметров для корректного представления процессов в системе.

Для построения модели конкретного сценария угрозы следует иметь аппарат, который позволяет описать характеристики производимых атак. Такими параметрами выступают состояния системы во время атаки, временные характеристики атаки и конечная вероятность проведения атаки. Наиболее удобным инструментом для построения моделей является аппарат сетей Петри-Маркова [8–10].

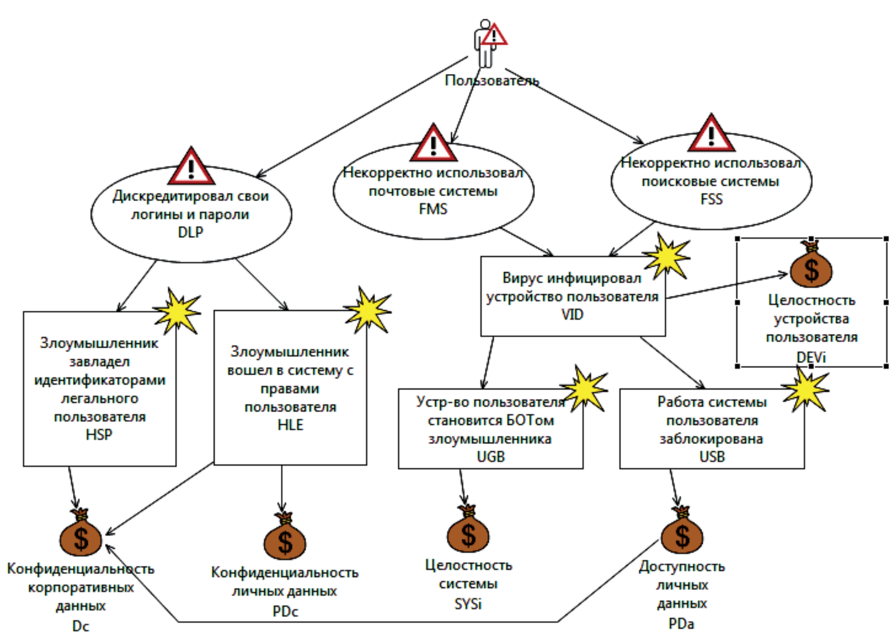

Рис. 1. Диаграмма угроз Coras. Влияние пользователя

В рассматриваемой системе представлены три сценария угроз, каждый из которых ведет к одному или более нежелательному инциденту. Модели данных сценариев в терминах аппарата сетей Петри-Маркова представлены на рис. 2.

Данные модели в упрощенном виде иллюстрируют этапы проведения атак на рассматриваемую систему и имеют следующие описания:

Сценарий FMS: $S1$ — пользователь готов к работе; $S2$ — поисковая система запущена; $S3$ — запрос обработан, ответ сформирован; $S4$ — вирус проникает на устройство; $t1$ — пользователь запускает поисковую систему; $t2$ — пользователь формирует запрос; $t3$ — пользователь активирует опасную ссылку.

Сценарий FSS: $S1$ — пользователь готов к работе; $S2$ — поль-

ISSN 2226-3780

зователь получил письмо; $S3$ — письмо со скрытым вирусом открыто; $t1$ — пользователь вошел в почтовую систему; $t2$ — пользователь открыл письмо.

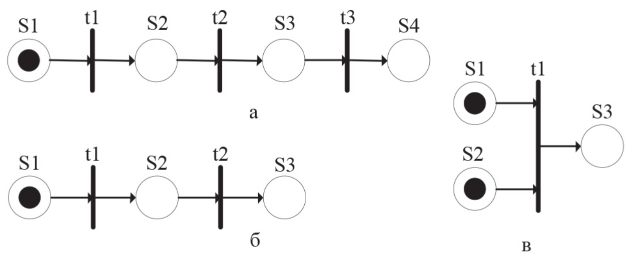

Рис. 2. Модели сценариев угроз: *а* — FMS, *б* — FSS, *в* — DLP

Сценарий DLP: $S1$ — пользователь готов к идентификации; $S2$ — злоумышленник или программа-шпион готовы к прослушиванию; $S3$ — данные переданы в открытом виде, или в непроверенную систему; $t1$ — пользователь проводит идентификацию и аутентификацию.

Далее необходимо построить математическую модель, которая позволяет оценивать вероятность осуществления сценария угрозы учитывая указанные параметры сценария. Для сценария FMS данная модель выглядит так:

$$P(t)=1-e^{-\frac{t}{\tau}}, \quad \tau_{FMS}=\tau_{11}+\tau_{22}+\tau_{33}, \tag{18}$$

где τ_{11} — среднее время подготовки к запуску поисковой системы, τ_{22} — среднее время формулирования запроса, τ_{33} — среднее время обработки запроса поисковой системы.

Для сценария FSS модель выглядит следующим образом:

$$P(t)=1-e^{-\frac{t}{\tau}}, \quad \tau_{FSS}=\tau_{11}+\tau_{22}, \tag{19}$$

где τ_{11} — среднее время подготовки к запуску почтовой системы, τ_{22} — среднее время просмотра и открытия письма.

Для сценария DLP модель выглядит следующим образом:

$$P(t)=1-e^{-\frac{t}{\tau}}, \quad \tau_{DLP}=\frac{\tau_{11}+\tau_{11}\tau_{21}+\tau_{21}}{\tau_{11}+\tau_{21}}, \tag{20}$$

где τ_{11} — среднее время процесса аутентификации, τ_{21} — среднее время перехвата и анализа данных.

Таким образом, введя для моделей (18)–(20) ПОСП для каждого входного параметра τ_{11}, τ_{22}, τ_{33} модели 1, τ_{11}, τ_{22} модели 2 и τ_{11}, τ_{21} модели 3, можно сопоставить конкретные лингвистические термы для оценки данных параметров. Используя данные оценки и описанные в соотношениях (11), (13), (15) моделей можно определять лингвистические термы, описывающие вероятности возникновения сценариев угроз.

6. Выводы

Используя разработанные модели, становится возможным применять естественную оценку рисков и угроз, которые способны снизить ценность активов информационной системы. Основой данного подхода является использование нечетких лингвистических термов в качестве параметров, описывающих особенности функционирования системы.

При разработке данного подхода использовалось двухэтапное проектирование, которое заключалось в следующем:

— проектирование полного семантического ортогонального пространства, соответствующего поставленной задаче. Данное ПОСП должно отображать все возможные термы для описания процессов в системе, избегая при этом избыточности оценок;

— разработка моделей атак, которые представляют собой множество сценариев угроз для информационной системы, используя при этом для описания параметров модели термы из разработанного ранее ПОСП.

Литература

1. Петренко, С. Методика построения корпоративной системы защиты информации [Электронный ресурс] / Сергей Петренко // CIT forum. — 2003. — Режим доступу: \www/URL: http://citforum.ru/security/articles/metodika_zashity/
2. Пастоев, А. Методологии управления IT-рисками [Электронный ресурс] / Алексей Пастоев // Открытые системы. — 2006. — № 8. — Режим доступа: \www/URL:http://www.osp.ru/os/2006/08/3584582/
3. Lund, S. Model-Driven Risk Analysis [Text] / Soldal Lund, Bjornar Solhaug, Ketil Stolen. — Berlin: Springer-Verlag, 2011. — 476 p. doi:10.1007/978-3-642-12323-8
4. Рыжов, А. П. Элементы теории нечетких множеств и ее приложений [Текст] / А. П. Рыжов. — М., 2003. — 81 с.
5. Тишин, П. М. Нечеткая многокритериальная оценка проектных решений в многоуровневых иерархических системах [Текст] / П. М. Тишин, Г. С. Гайворонская, К. В. Ботнарь // Вісник СНУ ім. В. Даля. — 2008. — № 8. — С. 210–214.
6. Шапорин, В. О. Оценка вероятности проведения атаки на сетевые ресурсы с использованием аппарата нечеткой логики [Текст] / В. О. Шапорин, П. М. Тишин, Н. Б. Копытчук, Р. О. Шапорин // Электротехнические и компьютерные системы. — 2013. — № 12(88). — С. 95–101.
7. Шапорин, В. О. Лингвистическая оценка активов сложной компьютерной системы для анализа рисков информационной безопасности [Текст] / В. О. Шапорин, П. М. Тишин, Р. О. Шапорин // Электротехнические и компьютерные системы. — 2015. — № 18(94). — С. 28–32.
8. Ларкин, Е. В. Форматы данных для структурно-параметрического описания сетей Петри-Маркова [Текст] / Е. В. Ларкин, В. А. Соколов, В. В. Котов, Н. А. Котова // Успехи современного естествознания. — 2008. — № 1. — С. 43–47.
9. Никитина, Г. Н. Анализ сетей Петри Маркова в концепции работы информационной системы [Текст] / Г. Н. Никитина // Известия Тульского государственного университета. — 2011. — № 5–3. — С. 29–34.
10. Радько, Н. М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа [Текст] / Н. М. Радько, И. О. Скобелев. — Москва: РадиоСофт, 2010. — 232 с.

РОЗРОБКА МОДЕЛЕЙ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЛЯ ОЦІНКИ ШКОДИ АКТИВАМ

Запропоновано моделі, які описують поведінку інформаційної системи при здійсненні сценаріїв загроз інформаційній безпеці. Для опису параметрів значень використані нечіткі лінгвістичні оцінки. Для опису самих сценаріїв використовується апарат мереж Петрі-Маркова. Для опису всього процесу оцінки активів використана методологія Coras. Загалом отримана модель, що дозволяє описати вплив здійснення сценаріїв загроз на оцінку активів системи.

Ключові слова: актив, загроза, методологія Coras, нечіткі бази знань, лінгвістичні змінні.

Шапорин Владимир Олегович, *старший преподаватель, кафедра компьютерных интеллектуальных систем и сетей, Одесский национальный политехнический университет, Украина,*
e-mail: shaporin_v@ukr.net.
Плачинда Ольга Евгеньевна, *кандидат технических наук, доцент, кафедра нефтегазового и химического машиностроения, Одесский национальный политехнический университет, Украина,*
e-mail: olga_plach2007@mail.ru.

Шапорін Володимир Олегович, *старший викладач, кафедра комп'ютерних інтелектуальних систем та мереж, Одеський національний політехнічний університет, Україна.*
Плачінда Ольга Євгеніївна, *кандидат технічних наук, доцент, кафедра нафтогазового та хімічного машинобудування, Одеський національний політехнічний університет, Україна.*

Shaporin Vladimir, *Odessa National Polytechnic University, Ukraine,*
e-mail: shaporin_v@ukr.net.
Plachinda Olga, *Odessa National Polytechnic University, Ukraine,*
e-mail: olga_plach2007@mail.ru

УДК 004.4'242
DOI: 10.15587/2312-8372.2015.47904

Бузовский О. В.,
Алещенко А. В.

РАЗРАБОТКА СИСТЕМЫ ГЕНЕРАЦИИ КОДОВ ПО ГРАФИЧЕСКИМ СХЕМАМ АЛГОРИТМА С ПРОМЕЖУТОЧНЫМ ЯЗЫКОМ ТРАНСЛЯЦИИ

Проанализированы способы представления графических схем алгоритма (ГСА) и обосновано использование нотации UML и блок-схем с дополнительной таблицей типов переменных для задания исходных данных при генерации исполняемых кодов. Выделены ошибки структуры ГСА и семантические ошибки для верификации, а также описаны способы трансляции ГСА в исполняемый код. Разработана система генерации исполняемых программных кодов по ГСА.

Ключевые слова: *UML, ГСА, трансляция, генерация программных кодов, проектирование, программная инженерия, Java.*

1. Введение

В настоящее время широко распространены CASE-системы (Computer-Aided System/Software Engineering), которые позволяют автоматизировать процесс разработки программных продуктов. Однако такая автоматизация, как правило, не является полной, так как внутренние коды методов классов предлагается вписывать вручную.

Следовательно, актуальной является задача полной автоматизации процесса создания программных продуктов, в рамках которой реализовывается собственная система автоматической генерации программных кодов по графическим схемам алгоритма (ГСА).

2. Анализ литературных данных и постановка проблемы

На данный момент существует множество способов графического изображения алгоритма. Среди наиболее известных способов можно назвать следующие: блок-схема, UML-диаграммы (деятельности, состояния, последовательности), дракон-схема и диаграмма Насси-Шнейдермана.

Анализ существующих графических нотаций бизнес-процессов показывает, что наиболее эффективными с точки зрения отражения концептуальных и реализационных особенностей является модельный аппарат UML. Данный факт в сумме с простотой изучения делает UML наиболее популярным графическим языком описания проектных решений [1].

Особенностью UML-диаграмм есть то, что они поддерживают объектно-ориентированную парадигму. Среди статических моделей объектно-ориентированных программ основной является диаграмма классов. Генерация объектно-ориентированного программного кода по UML-диаграмме классов дает на выходе так называемый «скелет» программного продукта, так как она определяет реализацию конкретных методов, но не позволяет получить полный исполняемый код [2].

По этой причине CASE-системы, которые используют UML, не позволяют полностью автоматизировать процесс создания программного продукта. Вместе с тем следует отметить, что большой процент затрат в рамках проекта связан именно с кодированием тел методов.

В работе [3] представлена система, которая генерирует исходных код для класса, который не содержит методов, что значительно сужает область использования такой системы. В работе [4] приведено описание системы с широким кругом функциональных возможностей, но являющейся узкоспециализированной — итоговая сгенерированная программа предназначена для работы только с графическими изображениями или потоковым видео.

Система, представленная в работе [5], поддерживает только структурную модель программирования, обходя вниманием объектно-ориентированную, что также сужает круг решаемых ею задач.

Алгоритм трансляции неструктурированной модели процесса в структурную форму приведен в работе [6]. Описанная в этой статье система, использующая