ТЕОРЕТИКО-СЕМАНТИЧЕСКИЕ АСПЕКТЫ ОРГАНИЗАЦИИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Бутусов И.В.[1], Нащекин П.А.[2], Романов А.А.[3]

Рассматриваются теоретико–семантических аспекты организации комплексной системы защиты информационной системы на базе бизнес–процессной модели с конкретными компонентами защиты. Системный взгляд на организацию комплексной защиты информационных систем в настоящее время связан с бизнес–процессным подходом, позволяющим встроить вопросы защиты ИС в современную методологию управления ИТ–средой в интересах предприятия. Целевым защищаемым ресурсом являются бизнес–процессы ИС и их непрерывное функционирование с точки зрения угроз информационной безопасности.

Показано, что основные трудности реализации бизнес–процессного подхода связаны с отсутствием формализмов, описывающих такие слабо формализуемые понятия процесса проектирования комплексной системы защиты, как качество информационной безопасности, угроза, возможности злоумышленника, механизмы и объект защиты, с необходимостью формирования областей предпочтений с учетом субъективных оценок лиц, принимающих решения. Целевая функция системы защиты представляется, как правило, в виде основных свойств безопасности (конфиденциальности, целостности, доступности и т.п.), которые измеряются в лингвистических шкалах и как следствие являются носителями определенной семантики. Семантика целевой функции порождает нечеткость при формировании областей предпочтений механизмов и объектов защиты. Основные свойства безопасности, представленные в лингвистический шкалах привносят элементы нечеткости в бизнес–процессную модель и в формирование областей предпочтений механизмов и объектов защиты. Показано, что семантика свойственна всем механизмам и объектам защиты в модели бизнес–процессного подхода к организации комплексной защиты и что теоретический аспект связан с естественным представлением нечетких множеств, представляющих семантику значений лингвистических переменных, в терминах математической информатики. Анализ теоретико–семантических аспектов бизнес–процессного подхода к организации защиты ИС позволяет обосновать необходимость совмещения жизненных циклов информационной системы и ее комплексной системы защиты.

***Ключевые слова**: бизнес–процессы информационной системы, организация комплексной системы защиты, целевой защищаемый ресурс, семантика целевой функции лингвистические переменные, предпочтения, пороги разделения*

Системный взгляд на организацию комплексной защиты информационных систем (ИС) в настоящее время связан с бизнес-процессным подходом, позволяющим встроить вопросы защиты ИС в современную методологию управления ИТ-средой в интересах предприятия [1,2]. Целевым защищаемым ресурсом являются бизнес-процессы ИС и их непрерывное функционирование с точки зрения угроз информационной безопасности. Это дает возможность рассматривать организацию безопасности ИС комплексно с учетом ее архитектурно-функциональных особенностей, оценить достаточность планируемых к использованию механизмов и средств защиты, определить метрики и целевой уровень безопасности для защищаемого ресурса [3,4,5].

Основные трудности реализации бизнес-процессного подхода связаны с отсутствием формализмов, описывающих такие слабо формализуемые понятия процесса проектирования комплексной системы защиты, как качество информационной безопасности, угроза, возможности злоумышленника, механизмы и объект защиты, с необходимостью формирования областей предпочтений с учетом субъективных оценок лиц, принимающих решения. Целевая функция системы защиты представляется, как правило, в виде основных свойств безопасности (конфиденциальности, целостности, доступности и т.п.), которые *измеряются в лингвистических шкалах* и как следствие являются носителями определенной семантики. Семантика целевой функции порождает нечет-

1 Бутусов Игорь Викторович, ОАО «Концерн «Системпром», Москва, butusigor@yandex.ru
2 Нащекин Павел Александрович, ОАО «Концерн «Системпром», Москва, npa@systemprom.ru
3 Романов Александр Анатольевич, доктор технических наук, ОАО «Концерн «Системпром», Москва, ralexhome@yandex.ru

кость при формировании областей предпочтений механизмов и объектов защиты [6,7,8].

Прежде всего, при рассмотрении теоретико-семантических аспектов бизнес-процессного подхода к организации комплексной защиты ИС отметим, что понятие *информационная система* в информатике тесно связано с понятием *отображение* в математике. Действительно, пусть (A,R,I) – ИС. В информатике обычно рассматривается описание множества R представлений с интерпретацией I в множестве A элементов (информаций). Интерпретация I данному представлению r ставит в соответствие некоторое абстрактное информационное содержание I[r]. Таким образом, интерпретации соответствует отображение $I: R \rightarrow A$. R называют также системой представления, а A – семантической моделью [8].

В целях исследования теоретико-семантических аспектов бизнес-процессного подхода к организации комплексной защиты ИС представим защищенную систему кортежем $S =< \{ИС\}, KS^{цель}, \{y\}, \{MZ\} >$[1]. Здесь $\{MZ\}$ – комплекс механизмов защиты от внешних воздействий $\{y\}$, обеспечивающий целевую функцию $KS^{цель} = (C, D, K, ...)$ для компонент защиты ИС. ИС реализует совокупность бизнес-процессов $bp^s = (f_1^s, ..., f_{m_s}^s)$, где $f_{m_s}^s$ – функции, образующие бизнес-процесс $bp^s \in BP$. Каждая функция представляет собой последовательность операций $f_{m_s}^s = \{IO_{m_s k}\}$ (k – номер операции, m – номер бизнес-процесса s). Операции $\{IO_{m_s k}\}$ реализуют обращения прикладного уровня через управляющие механизмы к системно-технической платформе: API-интерфейсы, продукты уровня MW (процессы системно-прикладного слоя; высокоуровневая организация данных – БД, БЗ, хранилища, форматы); клиенты прикладных протоколов – прикладной, презентационный, сессионный), OW – системная среда (оконный программный интерфейс; ядро ОС; низкоуровневая организация – файловая система, форматы; клиенты прикладных протоколов – транспортный, сетевой) [1,2].

Механизмы средств защиты $MZ =< MZ^{API}, MZ^{MW}, MZ^{OW} >$ обеспечивают защиту объектов API, MW, OW:

$MZ^{API} = \{MZ_f^{API}, MZ_{bp}^{API}, MZ_q^{API}, MZ_{pr}^{API}\}$, здесь

MZ_f^{API} - защита обращения к экранным формам API, MZ_{bp}^{API} - защита обращений к бизнес-логике, MZ_q^{API} - защита обращений к запросам, MZ_{pr}^{API} - защита обращений к клиентам прикладных протоколов;

$MZ^{MW} = \{MZ_{pw}^{MW}, MZ_{hd}^{MW}, MZ_{pp}^{MW}\}$, здесь

MZ_{pw}^{MW} - защита обращений к процессам MW, MZ_{hd}^{MW} – защита обращений к высокоуровневым данным, MZ_{hd}^{MW} - защита обращений к прикладным протоколам;

$MZ^{OW} = \{MZ_f^{OW}, MZ_y^{OW}, MZ_{nd}^{OW}, MZ_{ps}^{OW}\}$, здесь

MZ_f^{OW} - защита обращений к экранным формам ОС, MZ_y^{OW} - защита обращений к ядру ОС, MZ_{nd}^{OW} - защита обращений к низкоуровневым данным, MZ_{ps}^{OW} - защита обращений к системным протоколам.

Целевая функция для средств защиты $\overline{KS^{цель}}$ задает требования безопасности конкретных ИС в части целостности (C), доступности (D), конфиденциальности (K) и др. с использованием лингвистических переменных. Другими словами, $\overline{KS^{цель}}$ формирует требования к средствам защиты уровней API (MZ^{API}), MW (MZ^{MW}), OW (MZ^{OW}).

Лингвистические переменные обладают высокой выразительной способностью для человека, но привносят элементы нечеткости в бизнес-процессную модель организации комплексной защиты ИС, так как содержат семантические правила, задающие функции принадлежности нечетких множеств (семантику значений лингвистических переменных) [8,9].

Напомним, что лингвистической называется переменная, принимающая значения из множества слов или словосочетаний некоторого естественного или искусственного языка. Множество допустимых значений лингвистической переменной называется терм-множеством. Формально лингвистическая переменная задается пятеркой $< \hat{X}, T, U, G, M >$[6], где $\hat{X}$ – имя переменной; T – терм-множество, каждый элемент которого (терм) представляется как нечеткое множество на универсальном множестве U; G – синтаксические правила, часто в виде грамматики, порождающие названия термов; M – семантические правила, задающие функции принадлежности нечетких термов, порожденных синтаксическими G.

Например, для лингвистической переменной $\hat{X}$ = «конфиденциальность» оставшуюся четверку можно определить следующим образом: универсальное множество U =[0,20]; терм-множество T = {«высокая», «средняя», «низкая»} с функциями принадлежности

$$\mu_{низкая} = \frac{1}{1 + \left(\frac{u-10}{7}\right)^{12}}, \quad \mu_{средняя} = \frac{1}{1 + \left(\frac{u-20}{3}\right)^{6}},$$

$$\mu_{высокая} = \frac{1}{1+\left(\frac{u-30}{6}\right)^{10}};$$

синтаксические правила G, порождающие новые термы с использованием квантификаторов «не», «очень» и «более-менее»; семантические правила M, определяющие правила расчета функций принадлежности: «не t» = $(1-\mu_t(u)$, «очень t» = $(\mu_t(u))^2$ и «более-менее t» = $\sqrt{\mu_t(u)}$. (Рис. 1.)

Вернемся к рассмотрению бизнес-процессной модели организации комплексной защиты ИС.

Ранее отмечалось, что математически понятие ИС аналогично понятию отображение. Следовательно, с использованием введенных обозначений логично определить несколько групп отношений.

Первая группа отношений связывает множества всех операций $IO = \{io_1,...,io_k\}$, всех функций $F = \{f_1,...,f_m\}$ и всех бизнес-процессов $BP = \{bp_1,...,bp_n\}$:

отношение OF определено на множествах IO и F и, в общем случае, $\chi_{OF}(io_i, f_j) = \mu_{\widetilde{OF}}(io_i, f_j) = 1$, если операция io_i требуется для исполнения функции f_j, $i = \overline{1,k}$, $j = \overline{1,n}$. Здесь χ - характеристическая функция классического множества, μ - функция принадлежности нечеткого множества для случая субъективных оценок применения операция io_i в функции f_j (над обозначением нечеткого множества в отличие от обычного присутствует волнистая линия);

отношение FB определено на множествах F и BP; в общем случае $\chi_{FB}(f_i, bp_j) = \mu_{\widetilde{FB}}(f_i, bp_j) = 1$, если функция f_i задействована в бизнес-процессе bp_j, $i = \overline{1,n}$, $j = \overline{1,m}$.

Вторая группа отношений определена на множествах всех операций $IO = \{io_1,...,io_k\}$, всех защищаемых ресурсов ИС $ZR = \{zr^{api}, zr^{mw}, zr^{ow}\} = \{zr_1^{api},...,zr_{p1}^{api}, zr_1^{mw},...,zr_{p2}^{mw}, zr_1^{ow},...,zr_{p3}^{ow}\}$ и всех механизмов защиты $MZ = \{mz^{api}, mr^{mw}, mr^{ow}\} = \{mr_1^{api},...,mr_{q1}^{api}, mr_1^{mw},...,mr_{q2}^{mw}, mr_1^{ow},...,mr_{q3}^{ow}\}$:

отношение OS связывает множества всех операций IO и защищаемых ресурсов ZR; для простоты изложения запишем $\chi_{OS}(io_i, zr_j) = \mu_{\widetilde{OS}}(io_i, zr_j) = 1$, если для выполнения операции io_i требуется ресурс zr_j, $i = \overline{1,k}$, $j = \overline{1,p}$;

отношение SZ связывает множества всех защищаемых ресурсов ZR и всех механизмов защиты MZ; в общем случае $\chi_{SZ}(zr_i, mz_j) = \mu_{\widetilde{SZ}}(zr_i, mz_j) = 1$, если для защиты ресурса zr_i требуется механизм защиты mz_j, $i = \overline{1,p}$, $j = \overline{1,q}$.

Третья, и последняя группа отношений связывает множества всех требований безопасности $\overline{KS^{цель}} = \{C, D, K,...\} = \{kr_1,...,kr_d\}$, всех защищаемых ресурсов ИС $ZR = \{zr^{api}, zr^{mw}, zr^{ow}\} = \{zr_1^{api},...,zr_{p1}^{api}, zr_1^{mw},...,zr_{p2}^{mw}, zr_1^{ow},...,zr_{p3}^{ow}\}$ и всех механизмов защиты $MZ = \{mz^{api}, mr^{mw}, mr^{ow}\} = \{mr_1^{api},...,mr_{q1}^{api}, mr_1^{mw},...,mr_{q2}^{mw}, mr_1^{ow},...,mr_{q3}^{ow}\}$:

нечеткое отношение $\widetilde{TS}$ определяется значениями функций принадлежности $\mu_{\widetilde{TS}}(kr_i, zr_j)$, которая определяет kr_i требования по защите ресурса zr_j, формализованные соответствующим значением лингвистической переменной, $i = \overline{1,d}$, $j = \overline{1,p}$;

другое отношение, определяемое и используемое в этой группе – это отношение SZ.

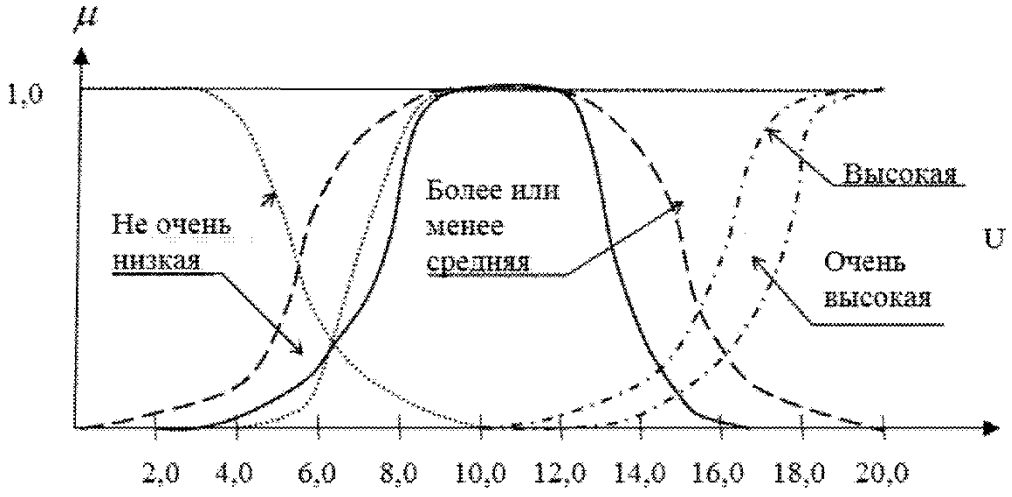

Рис. 1. *Лингвистическая переменная «конфиденциальность»*

Для анализа отношений в каждой группе применима типовая методика, целью которой является формирование областей предпочтения с учетом определенных (семантических) порогов разделения (степеней различения нечетких множеств) [6]. В основу методики положен подход, предложенный в работе [9], который строится, как нам кажется, на парадигме, что объект Z должен иметь характерные свойства (признаки) Y, которые позволяют ему исполнять некоторый функционал X (набор функций) и которые появились в силу необходимости обеспечения исполнения этого функционала.

Пусть $X = \{x_1, x_2, ..., x_n\}$ – требуемое к исполнению множество функций (требуемый к исполнению функционал); $Y = \{y_1, y_2, ..., y_p\}$ – множество свойств, характерных для объектов $Z = \{z_1, z_2, ..., z_m\}$.

Определена $\mu_{\tilde{R}} : X \times Y \to [0,1]$ функция принадлежности нечеткого бинарного отношения $\tilde{R}$. Для всех $x \in X$ и всех $y \in Y$ $\mu_{\tilde{R}}(x, y)$ – степень важности для требуемой к исполнению функции x свойства $y \in Y$ (потребность в наличии свойства y). Далее, пусть $\mu_{\tilde{S}} : Y \times Z \to [0,1]$ есть функция принадлежности нечеткого бинарного отношения $\tilde{S}$. Для всех $x \in X$ и всех $z \in Z$ $\mu_{\tilde{S}}(y, z)$ – степень принадлежности или совместимости объекта z со свойством y (оценка наличия свойств y объекта z). На базе отношений $\tilde{R}$ и $\tilde{S}$ можно сформировать отношение $R\tilde{T}$, элементы которого определяются функцией принадлежности

$$\mu_{\tilde{A}_i}(x, z_i) = \frac{\sum_y \mu_{\tilde{R}}(x, y) \bullet \mu_{\tilde{S}}(y, z_i)}{\sum_y \mu_{\tilde{R}}(x, y)},$$

для всех $x \in X$, $y \in Y$, $z \in Z$.

Сумма $\sum_y \mu_{\tilde{R}}(x, y)$ интерпретируется как средневзвешенное число существенных свойств y, которые необходимы для исполнения функции x, а $\mu_{\tilde{A}_i}(x, z_i)$ представляет собой *взвешенную степень предпочтения* объекта z_i для исполнения требуемой функции x.

Функция предпочтения должна удовлетворять определению выпуклого нечеткого подмножества:

$$\mu_{\tilde{A}_i}[\lambda(x_1, z_i) + (1-\lambda)(x_2, z_i)] \geq \min[\mu_{\tilde{A}_i}(x_1, z_i), \mu_{\tilde{A}_i}[\lambda(x_2, z_i)]$$

для всех x_1 и x_2, всех $z_i \in Z$ и всех $\lambda \in [0,1]$.

Поскольку все $\mu_{\tilde{A}_i}(x, z_i)$ выпуклые, их пересечения также выпуклые функции. Таким образом, формируется матрица W:

$$\tilde{W} = \begin{bmatrix} \mu_{\tilde{A}_1}(x_1, z_1) \cap \mu_{\tilde{A}_2}(x_1, z_2), ..., \mu_{\tilde{A}_{m-1}}(x_1, z_{m-1}) \cap \mu_{\tilde{A}_m}(x_1, z_m) \\ \mu_{\tilde{A}_1}(x_2, z_1) \cap \mu_{\tilde{A}_2}(x_2, z_2), ..., \mu_{\tilde{A}_{m-1}}(x_2, z_{m-1}) \cap \mu_{\tilde{A}_m}(x_2, z_m) \\ ..... \\ \mu_{\tilde{A}_1}(x_n, z_1) \cap \mu_{\tilde{A}_2}(x_n, z_2), ..., \mu_{\tilde{A}_{m-1}}(x_n, z_{m-1}) \cap \mu_{\tilde{A}_m}(x_n, z_m) \end{bmatrix}$$

В рассматриваемой модели порог разделения функционала ограничивается условием $l < \min_{ij} \max_x \min[\mu_{\tilde{A}_i}(x, z_i), \mu_{\tilde{A}_j}(x, z_j)]$ [8,9].

Если порог l выбран, то области предпочтений M_i, $i = \overline{1,m}$ требуемых к исполнению функций x_j между объектами z_i описываются уровневыми множествами

$$M_i = \{x \mid \mu_{\tilde{A}_i}(x) \geq \min_{ij} \max_x \min[\mu_{\tilde{A}_i}(x, z_i), \mu_{\tilde{A}_i}(x, z_j)]$$

для всех $x \in M_i$.

Нечеткое множество предпочтений с учетом вычисленного порога определяется в виде нормализованных нечетких множеств: $\tilde{M}_i = \{\mu_{\tilde{z}_i}(x_1), ... \mu_{\tilde{z}_i}(x_n)\}$, здесь

$$\mu_{\tilde{z}_i}(x_j) = \begin{cases} \mu_{\tilde{A}_i}(x_j, z_i), \_ если \_ \mu_{\tilde{A}_i}(x_j, z_i) > l \\ 0, \_ если \_ (\mu_{\tilde{A}_i}(x_j, z_i) \leq l \end{cases}$$

Результаты применения рассмотренной методики к приеденным выше группам отношений заключаются в следующем.

Третья группа отношений:

1) сформированы области нечетких предпочтений $\tilde{M}_i^{mz} = \{\mu_{m\tilde{z}_i}(kr_1), ..., \mu_{m\tilde{z}_i}(kr_d)\}$, где $\mu_{m\tilde{z}_i}(kr_j)$ - степень обеспечения выполнения требования по безопасности kr_j механизмом защиты mz_i.

2) $Z\tilde{R}_i^{TS} = \tilde{M}_i^{mz} \circ T\tilde{S}$, $Z\tilde{R}_i^{TS} = \{\mu_{Z\tilde{R}_j^{TS}}(zr_1), ..., \mu_{Z\tilde{R}_i^{TS}}(zr_p)\}$, где $\mu_{Z\tilde{R}_i^{TS}}(zr_j)$ – степень обеспечения защиты ресурса zr_j при использовании механизма защиты mz_i, $\circ$ – min-max-композиция.

3) $Z\tilde{R}^{TS} = \cup_i Z\tilde{R}_i^{TS}$, $Z\tilde{R}^{TS} = \{\mu_{Z\tilde{R}}(zr_1), ..., \mu_{Z\tilde{R}}(zr_p)\}$, где $\mu_{Z\tilde{R}}(zr_j)$ – степень обеспечения защиты ресурса zr_j при использовании всех допустимых для него механизмов защиты mz.

Вторая группа отношений:

1) сформированы области нечетких предпочтений $\tilde{M}_i^{mz} = \{\mu_{m\tilde{z}_i}(io_1), ..., \mu_{m\tilde{z}_i}(io_k)\}$, где $\mu_{m\tilde{z}_i}(io_j)$ – степень обеспечения защиты операции oi_j механизмом защиты mz_i;

2) $Z\tilde{R}_i^{OS} = \tilde{M}_i^{mz} \circ O\tilde{S}$, $Z\tilde{R}_i^{OS} = \{\mu_{Z\tilde{R}_i^{OS}}(zr_1), ..., \mu_{Z\tilde{R}_i^{OS}}(zr_p)\}$, где $\mu_{Z\tilde{R}_i^{OS}}(zr_j)$ – степень обеспечения защиты ресурса zr_j при использовании механизма защиты mz_i, $\circ$ – min-max-композиция;

3) $\widetilde{ZR}^{OS} = \bigcup_i \widetilde{ZR}_i^{OS}$, $\widetilde{ZR}^{OS} = \{\mu_{\widetilde{ZR}^{OS}}(zr_1),...,\mu_{\widetilde{ZR}^{OS}}(zr_p)\}$, где $\mu_{\widetilde{ZR}}(zr_j)$ – степень обеспечения защиты ресурса zr_j при использовании всех допустимых для него механизмов защиты mz ;

4) $\widetilde{ZR} = \widetilde{ZR}^{TS} \cup \widetilde{ZR}^{OS}$, $\mu_{\widetilde{ZR}}(zr_i) = \min\{\mu_{\widetilde{ZR}^{OS}}(zr_i), \mu_{\widetilde{ZR}^{TS}}(zr_i)\}$ – степень обеспечения защиты ресурса zr_i при использовании всех допустимых для него механизмов защиты mz с учетом обеспечения требований по безопасности kr ;

5) $\widetilde{IO}^{OS} = \widetilde{ZR} \circ \widetilde{OS} = \{\mu_{\widetilde{IO}^{OS}}(io_1),...,\mu_{\widetilde{IO}^{OS}}(io_k)\}$, где $\mu_{\widetilde{IO}^{OS}}(io_j)$ – степень защиты операции io_j выбранными механизмами защиты mz с учетом требований по безопасности kr , защищаемых ресурсов zr и степени использования ресурсов при выполнении этой операции.

Первая группа отношений:

1) сформированы области нечетких предпочтений $\widetilde{M}_i^{bp} = \{\mu_{b\widetilde{p}_i}(io_1),...,\mu_{bp_i}(io_k)\}$, где $\mu_{bp_i}(io_j)$ – степень задействования операции oi_j в бизнес-процессе bp_i ;

2) $\widetilde{IO}_i^{OF} = \widetilde{IO}^{OS} \cap \widetilde{M}_i^{bp}$, $\mu_{IO_i^{OF}}(io_j) = \min\{\mu_{\widetilde{IO}_i^{OS}}(io_j), \mu_{\widetilde{M}_i^{bp}}(io_j)\}$, $i = \overline{1,k}; j = \overline{1,q}$; где $\mu_{IO_i^{OF}}(io_j)$ - степень защищенности операции io_j с учетом ее занятости в бизнес-процессе bp_i ;

3) $\widetilde{F}_i = \widetilde{IO}^{OF} \circ \widetilde{OF} = \{\mu_{\widetilde{F}_i}(f_1),...,\mu_{\widetilde{F}_i}(f_m)\}$, где $\mu_{\widetilde{F}_i}(f_j)$ - степень защищенности функции f_j с учетом ее операций, занятых в бизнес-процессе bp_i;

4) $\widetilde{F} = \bigcup_i \widetilde{F}_i$, $\mu_{\widetilde{F}}(f_j) = \max_i\{\mu_{\widetilde{F}_i}(f_j)\}$, где $\mu_{\widetilde{F}}(f_j)$ - степень защищенности функции f_j с учетом всех задействованных в ее выполнении операций.

5) $\widetilde{BP} = \widetilde{F} \circ \widetilde{FB} = \{\mu_{\widetilde{BF}}(bp_1),...,\mu_{\widetilde{BF}}(bp_n)\}$, где $\mu_{\widetilde{BF}}(bp_j)$ - степень защищенности бизнес-операции bp_i с учетом с учетом задействованных в ее реализации функции f .

Анализ результатов применения методики формирование областей предпочтения с учетом определенных (семантических) порогов разделения к выделенным группам отношений бизнес-процессного подхода к организации комплексной защиты ИС показывает, что семантика основных свойств безопасности (конфиденциальности, целостности, доступности, …), содержащаяся в значениях этих свойств распространяется, начиная с третьей группы отношений, на вторую и первую группы. Таким образом, семантика свойственна всем механизмам и объектам защиты в модели бизнес-процессного подхода к организации комплексной защиты ИС и определяет нечеткость при формировании соответствующих областей предпочтений с использованием вычисляемых семантических порогов разделения (степеней различения нечетких множеств). Это семантический аспект.

Теоретический аспект связан с естественным представлением нечетких множеств, представляющих семантику значений лингвистических переменных, в терминах математической информатики.

Согласно [7] семантика всякого сведения об объекте предполагает наличие следующих четырех величин: опорного множества X объектов, семантического указателя x одного из объектов X , т.е. $x \in X$, подмножества δ объектов из X , т.е. $\delta \subset X$ и семантической достоверности p , которая характеризует достоверность (определенность) выполнения главного условия $x \in \delta$.

Если x_0 – точка X и δ – некоторое непустое подмножество X, которое определяется свойством δ , то факт принадлежности $x_0 \in \delta$ или истинное высказывание «точка x_0 из X обладает свойством δ » записывается в виде в виде одноместного предиката $\delta(x_0), x_0 \in X$.

Если P – решетка достоверностей, X – опорное множество, $x_0 \in X$ и $\delta \subset X$, и если про точку x_0 известно с семантической достоверностью $p \in P$, что $x_0 \in \delta$, то имеется сведение о точке $x_0 \in X$, которое записывается в форме триады $(p)\delta(x_0)$, которая интерпретируется как принадлежность $x_0 \in \delta$ с достоверностью p или высказывание «точка x_0 из X обладает свойством δ с семантической достоверностью p».

Если более точно, то согласно основным положениям математической информатики [7] под информационным описанием $\Delta(x)$ произвольного объекта x понимается структурированная совокупность сведений вида $(p)\delta(x)$:

$$\Delta(x) = \{(p_i)\delta_i\}(x), i = \overline{1, N_\delta} .$$

Сведения $\{(p_i)\delta_i\}(x)$ интерпретируются как «объект x из X характеризуется свойством δ_i с семантической достоверностью p_i », δ_i – подмножество объектов из X , характеризующихся одноименным свойством $\delta_i \subset X$, а p_i – семантическая достоверность того, что $x \in \delta_i$.

Рассмотрим информационное описание $\Delta(x_i) = \{(p)\delta_p; 0 < p \le 1\}(x_i)$, где δ_p – семейство подмножеств таких, что $x_i \in \delta_p, 0 < p \le 1$, с семантической достоверностью p . Для δ_p можно подобрать информационные описания $\Delta(x_j) = \{(p')\delta_{p'}; 0 < p' \le 1\}(x_j)$, $i \ne j$, такие, что $\delta_p = \{x_j \mid x_j \in \delta_{p'}, p' \ge p\}$. Следовательно, δ_p и $\delta_{p'}$ – множества уровней p и p' нечеткого свойства (множества) $\widetilde{\delta} : \widetilde{\delta} = \{x, p_{\widetilde{\delta}}(x)\}$,

$p_{\tilde{\delta}}(x) = \mu_{\tilde{\delta}}(\delta) : X \to [0,1]$ – функция принадлежности по Л. Заде. Следовательно, семантика информационного описания $\Delta(x_i)$ и $\Delta(x_j)$ в соответствии с математической информатикой формально представлена нечетким свойством $\tilde{\delta}$.

Следует отметить научную и практическую актуальность исследования теоретико-семантических аспектов организации комплексной системы защиты ИС. По сути эти исследования позволяют обосновать методическую и технологическую необходимость выделения в жизненном цикле ИС самостоятельного этапа «Перенос ИС» в новую операционную среду, в рамках которого осуществляется модернизация и развитие бизнес-процессов крупных ИС, работающих непрерывно в реальном масштабе времени.

Решение этой проблемы при проектировании и создании отечественных программно-аппаратные средств, операционных сред и на их основе ИС связано с обеспечением требований переносимости ПО и интероперабельности путем последовательного применения принципов открытых систем и методологии функциональной стандартизации [10].

Как следует из анализа теоретико-семантических аспектов бизнес-процессного подхода к организации защиты ИС на этапе ее переноса одновременно реализуется комплексная система защиты информации с учетом архитектурно-функциональных особенностей, оценки достаточности планируемых к использованию механизмов и средств защиты, определения метрики и целевого уровня безопасности для защищаемого ресурса. Такой подход позволяет совместить в рамках этапа «Перенос ИС» жизненные циклы ИС и ее системы комплексной защиты. Принципиальные особенности такого совмещения заключаются, на наш взгляд, в следующем: 1) формирование требований и для ИС, и для комплексной системы защиты информации (КСЗИ) основывается на бизнес-модели проектируемого процесса; 2) ИС должна вводиться в эксплуатацию одновременно с КСЗИ; 3) эксплуатация характеризуется выявлением ситуаций, требующих перехода к этапу переноса/модернизации как ИС, так КСЗИ; 4) в переходный период импортозамещения в сфере информационно-коммуникационных технологий работоспособность функциональных частей ИС в существующих отечественных операционных средах можно обеспечить только с использованием импортных технологических средств по уровням интероперабельности с последующим их замещением отечественными, что позволяет увеличивать уровень доверенности аппаратно-программных сред [11,12,13,14].

Заключение

Семантика свойственна всем механизмам и объектам защиты в модели бизнес-процессного подхода к организации комплексной защиты ИС и определяет нечеткость при формировании соответствующих областей предпочтений с использованием вычисляемых семантических порогов разделения (степеней различения нечетких множеств). Это семантический аспект.

Теоретический аспект связан с естественным представлением нечетких множеств, представляющих семантику значений лингвистических переменных, в терминах математической информатики.

Анализ теоретико-семантических аспектов бизнес-процессного подхода к организации защиты ИС позволяет обосновать необходимость совмещения жизненных циклов информационной системы и ее комплексной системы защиты.

В начальный период импортозамещения в сфере информационно-коммуникационных технологий работоспособность функциональных частей ИС в существующих отечественных операционных средах можно обеспечить только с использованием импортных технологических средств по уровням интероперабельности с последующим их замещением отечественными, что позволяет увеличивать уровень доверенности аппаратно-программных сред.

Литература:

1. Лукинова О.В. Метод конструирования бизнес-процессов, обеспечивающих безопасность информационной системы, на основе межкатегорийного представления плоскости защиты модели OSE/RM // Надежность. 2013. №4. С. 118-127.
2. Лукинова О.В. Семантическое описание факторов безопасности информационных систем при проектировании систем защиты // Системы высокой доступности. 2013. Т. 9. № 3. С. 149-156.
3. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1 (2), 2014. С. 40-48.
4. Зотова А.В., Петренко С.А., Здирук К.Б., Сычев Л.П. Доверенная среда облачных вычислений // Защита информации, INSIDE № 1, 2013. – С. 28-33.
5. Здирук К. Б., Астрахов А. В., Лонский А. В. Модель защиты информации в гетерогенных вычислительных сетях на базе архитектуры встроенных «защищенных контуров». Труды X Российской научно-технической конференции «Новые информационные технологии в системах связи и управления» (1–2 июня 2011 г., Калуга), 2011. С. 543–545.

6. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: Мир, 1976. 165 с.
7. Чечкин А.В. Математическая информатика. М.: Наука, 1991. 416 с.
8. Кузьмин А.С., Романов А.А. Логико-семантические представления вербальных описаний в информатике. М.: Медиа Группа «Авангард, 2014. 208 с.
9. Кузьмин А.С., Романов А.А. О правилах, исключениях из правил и особенностях представления семантики в слабоструктурированных системах // Приборы и системы. Управление, контроль, диагностика. 2014. № 10. С. 29-36.
10. Бойченко А., Корнеев Д.Г., Лукинова О.В. Интероперабельность информационных систем на основе стека EIF и модели OSE/RM. В сборнике: Теория активных систем Материалы международной научно-практической конференции. под общей редакцией В.Н. Буркова. Москва, 2014. С. 230-233.
11. Бородакий Ю.В., Добродеев А.Ю., Бутусов И. В. Доверенная среда - основа гарантированной безопасности! // «Information Security / Информационная безопасность», № 2, 2013. - С. 36-37.
12. Хабибуллин И.В. Основные проблемные вопросы создания доверенной программно-аппаратной среды для асу органов военного и государственного управления // Вопросы кибербезопасности. 2014. № 3 (4). С. 14-19.
13. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.
14. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С. 10-16.

Рецензент: Горелкин Георгий Александрович, кандидат технических наук, начальник управления планирования, координации и сопровождения научных исследований, ученый секретарь диссертационного совета ОАО «Концерн «Системпром», г. Москва, *e-mail: gorelking@yandex.ru.*

THEORETICAL-SEMANTIC ASPECTS OF INTEGRATED INFORMATION SYSTEMS SECURITY POLICY

Butusov I.V. [4]***, Nashchekin P.A.*** [5]***, Romanov A.A.*** [6]

Examines theoretical and semantic aspects of the integrated system for the protection of information systems based on business process models with specific components of protection. A systematic view on the Organization of the comprehensive protection of information systems currently associated with a business continuous approach that allows you to embed IP protection issues in the modern IT environment management methodology for enterprise. Trust protected resource are IP business processes and their continuous operation from the point of view of information security threats.

It has been shown that the main difficulties implementing business process approach linked to the lack of formalisms that describe such weakly formalizuemye concept design process integrated system protection, as the quality of information security, threat, attacker, mechanisms and the object of protection, with the need to develop areas of preference, taking into account the subjective assessments of decision-makers. The objective function of the protection system appears, usually in the form of basic properties of security (confidentiality, integrity, availability, etc.), which are measured in linguistic scales and as a consequence are the bearers of a particular semantics. The semantics of the target function gives rise to uncertainty in the formation of areas of preference mechanisms and objects of protection. Basic security properties presented in linguistic fuzziness elements bring scales in the business process model and the formation of areas of preference mechanisms and objects of protection.

It is shown that the semantics is characteristic of all mechanisms and objects of protection in the model business process approach to comprehensive protection and that the theoretical aspect involves the natural representation of fuzzy sets, representing the semantics of values of linguistic variables in terms of mathematical informatics. Analysis of theoretical-semantic aspects of a business process approach to IP protection allows you to justify the necessity of combining life cycles of information system and its complex system of protection.

Keywords*: business processes, information systems, organization of complex system of protection, trust the protected resource, the semantics of the target function linguistic variables, preferences, separation Rapids*

4 Igor Butusov, OJSC «Concern «Systemprom», Moscow, butusigor@yandex.ru
5 Pavel Nashchekin, OJSC «Concern «Systemprom», Moscow, npa@systemprom.ru
6 Aleksandr Romanov, Doctor of Technical science, OJSC «Concern «Systemprom», Moscow, ralexhome@yandex.ru

References:

1. Lukinova O.V. Metod konstruirovaniya biznes-protsessov, obespechivayushchikh bezopasnost' informatsionnoy sistemy, na osnove mezhkategoriynogo predstavleniya ploskosti zashchity modeli OSE/RM, Nadezhnost'. – 2013, – pp. 118-127
2. Lukinova O.V. Semanticheskoe opisanie faktorov bezopasnosti informatsionnykh sistem pri proektirovanii sistem zashchity, Sistemy vysokoy dostupnosti. 2013. T. 9. No 3, pp. 149-156.
3. Zhidkov I.V., Kadushkin I.V. O priznakakh potentsial'no opasnykh sobytiy v informatsionnykh sistemakh, Voprosy kiberbezopasnosti, No 1 (2), 2014, - pp. 40-48.
4. Zotova A.V., Petrenko S.A., Zdiruk K.B., Sychev L.P. Doverennaya sreda oblachnykh vychisleniy, Zashchita informatsii. INSIDE № 1, 2013, pp. 28-33.
5. Zdiruk K. B., Astrakhov A. V., Lonskiy A. V. Model' zashchity informatsii v geterogennykh vychislitel'nykh setyakh na baze arkhitektury vstroennykh «zashchishchennykh konturov», Trudy Kh Rossiyskoy nauchno-tekhnicheskoy konferentsii «Novye informatsionnye tekhnologii v sistemakh svyazi i upravleniya», 1–2 iyunya 2011 g. – Kaluga, 2011, pp. 543–545.
6. Zade L.A. Ponyatie lingvisticheskoy peremennoy i ego primenenie k prinyatiyu priblizhennykh resheniy. - M.: Mir, 1976. - 165 P.
7. Chechkin A.V. Matematicheskaya informatika. - M.: Nauka, 1991. - 416P.
8. Kuz'min A.S., Romanov A.A. Logiko-semanticheskie predstavleniya verbal'nykh opisaniy v informatike. – M.: Media Gruppa «Avangard, 2014. - 208 P.
9. Kuz'min A.S., Romanov A.A. O pravilakh, isklyucheniyakh iz pravil i osobennostyakh predstavleniya semantiki v slabostrukturirovannykh sistemakh, Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2014. No 10, pp. 29-36.
10. Boychenko A., Korneev D.G., Lukinova O.V. Interoperabel'nost' informatsionnykh sistem na osnove steka EIF i modeli OSE/RM, V sbornike: Teoriya aktivnykh sistem Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. pod obshchey redaktsiey V.N. Burkova. Moskva, 2014, pp. 230-233.
11. Borodakiy Yu.V., Dobrodeev A.Yu., Butusov I. V. Doverennaya sreda - osnova garantirovannoy bezopasnosti! «Information Security / Informatsionnaya bezopasnost'», No 2, 2013, - pp. 36-37.
12. Khabibullin I. V. Osnovnye problemnye voprosy sozdaniya doverennoy programmno-apparatno sredy dlya ASU organov voennogo i gosudarstvennogo upravleniya, Voprosy kiberbezopasnosti. 2014. No 3 (4). pp. 14-19.
13. Markov A.S., Tsirlov V.L. Opyt vyyavleniya uyazvimostey v zarubezhnykh programmnykh produktakh, Voprosy kiberbezopasnosti. 2013. No 1 (1), pp. 42-48.
14. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost' avtomatizirovannykh sistem upravleniya voennogo naznacheniya, Voprosy kiberbezopasnosti. 2013. No 1 (1), pp. 10-16.