4.Розробка діаграми IDEF3 для опису діяльності на кадрі. Головною організаційною одиницею нотації IDEF3 є діаграма (робота), що відображає дію на кадрі. Ім'я цієї роботи «Очікування дії на кадрі ...». Робота «Очікування дії на кадрі ...» представляє всі можливі дії користувача.

Дії на кадрі - це події, які можна розбити на дві групи - натискання на кнопки, що призводять до зміни кадру, і дії, які видозмінюють деякі поля кадру (наприклад, введення) і не призводять до його зміни .

Для відображення логіки взаємодії стрілок при злитті і розгалуженні існують перехрестя для злиття і перехрестя для розгалуження. До перехресть відносяться: синхронні та асинхронні «і», «або», «виключне «або».

В процесі роботи в середовищі BPwin були підтверджені основні переваги IDEF-технології і виявлені деякі недоліки редактора.

Недоліки редактора BPwin: відсутність режима Undo, руйнування конфігурації моделі при редагуванні розмірів окремих її елементів, складність переміщення діаграм по дереву моделі.

1. *Маклаков С.В.* Создание информационных систем с AllFusion Modeling Suite-М.:ДИАЛОГ-МИФИ, 2003-432 с.
2. *Черемных С.В., Семенов И.О., Ручкин В.С.* Структурный анализ систем:IDEF – технологий – М.: Финансы и статистика, 2003 – 208 с: ил. – (Прикладные информационные технологии).
3. *Самойлов В.Д.* Модельное конструирование компьютерных приложений – Киев:Наукова думка, 2007 – 198 с.

Поступила 17.01.2011р.

УДК 681.3

А.Н. Давиденко, к.т.н., ИПМЕ им. Г.Е. Пухова НАНУ, Киев

АНАЛИЗ ОСНОВНЫХ ИНФОРМАЦИОННЫХ КОМПОНЕНТ СИСТЕМ ДОСТУПА

In the article questions are considered forming and existence of dictionaries, containing description of base elements of subject domains entering in the complement of the system of access of the informative system. Terms are offered and formalizated eliminating possibilities origins of contradiction in instance where two different subject domains, that use different base elements on attitude toward each other, possess the maximal levels of abstraction.

В статье рассмотрены вопросы формирования и существования словарей, содержащих описание базовых элементов предметных областей,

входящих в состав системы доступа информационной системы. Предложены и формализованы условия исключающие возможности возникновения противоречивости в ситуации, когда две различные предметные области, которые используют различные базовые элементы по отношению друг к другу, обладают максимальными уровнями абстракции.

Системы доступа [1-5] реализуют взаимосвязь между объектом доступа и пользователем средств, которые представляет объект пользователю. В этом случае, такая взаимосвязь реализуется в виде интерфейса между пользователем и объектом доступа. В большинстве случаев, данные, которыми оперирует объект, не имеют формы отображения, которая совпадала бы с данными, которыми оперирует пользователь, особенно если таким пользователем является не процесс, а человек, решающий свою прикладную задачу. Поэтому, система доступа, которая ограничивается только функциями интерфейса, должна обладать достаточно развитой информационной структурой. Такая информационная структура необходима для решения задач преобразования области интерпретации данных пользователя, которые представлены в соответствующей форме, в форму, которая приемлема для объекта доступа. Соответствующая система доступа должна осуществлять и обратные преобразования форм представления данных. Очевидно, что соответствующие преобразования форм представления данных тесно связаны с описаниями предметных областей интерпретации, которыми пользуется пользователь и областей, интерпретации, которые допустимы в объекте доступа. Если принять во внимание, что таких пользователей с различными областями интерпретации их прикладных задач у одного объекта доступа может быть много, то становится очевидной достаточно большая сложность решения задачи преобразований одних форм представления данных в другую и наоборот. В современных системах доступа задача преобразования входных данных в необходимую для объекта форму распределена по всем составляющим, которые используют систему доступа. Таким образом, для системы доступа выделена лишь часть функциональных преобразований, которые решают задачу согласования данных, исходящих от пользователя к объекту доступа и наоборот. К таким задачам, которые определены для системы доступа, можно отнести следующие:

- задачи предоставления пользователю преемственного интерфейса;
- исходное преобразование данных пользователя в форму представления приемлемую для объекта;
- преобразование данных, поступающих от объекта доступа к пользователю, в форму приемлемую для отдельного пользователя;
- формирование дополнительных комментариев к данным, предназначенным отдельному пользователю, если пользователем является человек и последний сформировал запрос о таких комментариях;

– задача идентификации пользователя, целью решения которой является определение отдельного пользователя, если таких пользователей может быть больше одного.

Приведенные выше задачи представляют собой классический набор функций системы доступа, для случая, когда не рассматриваются задачи безопасности системы доступа, объекта доступа и обеспечения безопасности пользователей, которые используют соответствующую систему доступа (SD).

Для решения задач безопасности SD, для удобства, будем говорить о безопасности SD подразумевая безопасности всех перечисленных составляющих, необходима достаточно развитая система информационного обеспечения тех подсистем, которые непосредственно ориентированы на решение задач защиты всех компонент SD. При корректном проектировании SD, причинами изменения уровня безопасности могут быть, в первую очередь, внешние факторы, которые могут воздействовать на работу SD. Внутренние факторы, которые тоже могут негативно влиять на работу SD рассматривать не будем, так как к ним будем относить такие факторы как возникновение неисправности или возникновение дефектов, влияющих на штатные режимы работы SD. Поскольку внешние факторы воздействующие негативно на SD инициируют соответствующие воздействия недетерминировано, то характерным для решения задач защиты SD являются следующие методы:

– методы прогнозирования возникновения атак на SD со стороны внешних опасностей;
– методы адаптации SD к изменяющимся внешним условиям, в которых функционирует SD;
– методы распознавания негативных внешних воздействий на SD или распознавание атак;
– методы определения текущего уровня безопасности отдельных компонент и системы SD в целом;
– методы противодействия атакам, которые были выявлены на различных этапах их реализации, включая конечный этап реализации атаки, если последняя является успешной.

Из приведенных базовых методов решения задач обеспечения безопасности видно, что для их реализации и инициации не существует или достаточно сложно определить детерминированный набор входных данных, которые обеспечивали бы возможность однозначно определить алгоритм реализации соответствующих методов решения задач, которые в совокупности решали бы задачу обеспечения безопасного функционирования системы SD. В связи с этим, целесообразно для решения приведенных задач использовать средства, которые в максимально возможной мере были бы пригодны для реализации приведенных выше методов решения отдельных

составляющих задачи обеспечения безопасности функционирования системы SD. Исходя из ранее проведенного анализа возможностей нейронных сетей, как средств решения задач распознавания, адаптации к изменяющимся внешним воздействиям, которые могут быть основой для решения задач прогнозирования изменений во внешних воздействиях, а также ряда других задач, включая задачи определения уровня безопасности и задачи инициации средств противодействия атакам, в настоящей работе в качестве универсальных средств решения задачи безопасности SD в целом, выбраны средства, которые реализуются на основе использования нейронных сетей.

Одной из важных особенностей использования системы различных типов нейронных сетей является необходимость в использовании достаточно развитой информационной системы, которая отображала бы все необходимые для функционирования нейронных систем данные. Кроме того, в рамках соответствующей информационной системы должны существовать средства, которые обеспечивали бы предварительную обработку соответствующих данных, прежде чем последние можно было бы подавать в функциональные блоки, которые реализованы на основе использования нейронных сетей. Совершенно очевидно, что информационная система (IS) должна основываться на описаниях предметных областей, которые описывают интерпретацию данных, которые используются во всех фрагментах SD. Поэтому рассмотрим основные компоненты IS, которые необходимы для решения задач информационного обеспечения системы безопасности SD, которую сокращенно будем обозначать символами BSD. К таким компонентам отнесем следующие:

- словари, содержащие описание базовых элементов предметных областей (S_C);
- система синтаксических правил формирования описаний интерпретации базовых элементов (Ω);
- система семантических параметров, которые характеризуют особенности интерпретации базовых элементов и других компонент BSD (Λ);
- система семантических правил, которые регламентируют способы построения описания интерпретации элементов, которые используются при функционировании системы BSD;
- система правил преобразования описаний компонент системы BSD (Σ).

Словари представляют собой описания идентификаторов и других компонент, которые используются в SD. Поскольку предметные области со стороны пользователей или внешние предметные области могут иметь различный уровень абстракции, то нет смысла привязываться к одному из возможных языков, которым могла бы описываться отдельная предметная

область. В данном случае изменение уровня абстракции языка определяется количеством новых базовых идентификаторов, которые вводятся в качестве обозначения реальных объектов или факторов, которые имеют своё самостоятельное значение в некоторой предметной области интерпретации. Примером такого типа изменения уровня абстракции в описании предметной области может служить использование профессиональной терминологии. При этом, такая терминология может быть еще и не общепринятой. В этом случае, соответствующую терминологию называют жаргоном. Следовательно, наиболее низким уровнем абстракции будет обладать язык, который строится на основе базовых компонент, описывающих наиболее широко распространенную предметную область. При использовании такого способа определения изменения уровня абстракции языка, может иметь место ситуация, когда две различные предметные области, которые используют различные базовые элементы по отношению друг к другу, обладают максимальными уровнями абстракции. Для исключения возможности возникновения такой противоречивости, примем следующие условия.

Условие 1. Измерение изменения уровня абстракции возможно только между двумя описаниями предметных областей, которые имеют не меньше половины общих базовых элементов.

Условие 2. Измерение величины изменения уровня абстракции возможно только между двумя последовательно модифицируемыми описаниями предметных областей.

Условие 3. Изменение величины уровня абстракции между двумя последовательно рассматриваемыми описаниями предметной области не может превышать 10% от общего количества базовых элементов модифицируемого описания предметной области.

Принимая во внимание, что описание предметной области представляет собой словарь S_C, то приведенные выше условия можно описать формально. Для этого примем, что последовательное преобразование S_C, которое приводит к изменению уровня абстракции определенного описания предметной области, в общем виде запишется следующим соотношением:

$$A(S_C) = \{S_{C1} \rightarrow [F_{A1}(S_{C1}) = S_{C2}] \rightarrow ... \rightarrow [F_{A(n-1)}(S_{C(n-1)})] \rightarrow S_{Cn} \quad (1)$$

где F_{Ai} - преобразование S_{Ci}, которое приводит к увеличению уровня абстракции описания предметной области S_{Ci}. В этом случае условие 1 запишется в виде следующего соотношения:

$$[S_{Ci} \cap S_{C,(i+1)} = 1/2(S_{Ci} \,\&\, S_{C,(i+1)})] \rightarrow U_{Ai}[F_{Ai}(S_{Ci})] \quad (2)$$

где U_{Ai} - функция определяющая величину изменения уровня абстракции в $S_{C(i+1)}$, который реализуется соотношением $F_{Ai}(S_{Ci}) \rightarrow S_{C,(i+1)}$.

Условие 2 формально описывается следующим соотношением:

$\Delta Q_i = Q_{Ai}[S_{Ci}, F(S_{Ci})]$, где ΔQ_i - величина изменения уровня

абстракции в $S_{C,(i+1)}$ по отношению к S_{Ci}.

Условие 3 формально записывается в виде следующего соотношения:

$$Q_{Ai}(S_{C,(i+1)}) \le 0{,}1 \mid S_{Ci} \mid ,$$

где $\mid S_{Ci} \mid$ - параметр, характеризующий S_{Ci} и используемый для вычисления $Q_{Ai}(S_{Ci})$. В простейшем случае, этот параметр представляет собой мощность множества S_{Ci}.

Условия 1 и 2 предполагают использование одной и той же предметной области, которая допускает на отдельном этапе модификации своё развитие. Если эти условия не выполняются, то соответствующие S_{Ci} и S_{Cj} являются различными. В рамках принятого подхода к оценке уровня абстракции описания S_{Ci} отсутствует возможность сравнивать по параметру уровня абстракции S_{Ci} с S_{Ci+j}, если $j \ge 2$. Таким образом, соотношение (1) описывает некоторую эволюцию развития S_{Ci}, которая происходит на протяжении изменений S_C от S_{C1} до S_{Cn}. Поскольку описание предметной области S_C является базовым, для работы системы BSD, то необходимо более полно рассмотреть S_C, все процессы, которые могут происходить в рамках S_C и процессы, которые связаны с преобразованиями самих словарей S_C. Очевидно, что соответствующие процессы должны описываться параметрами, которые их характеризуют. К таким процессам отнесем следующие изменения и модификации, которые могут происходить в S_C:

- процессы изменения уровня абстракции в описании предметной области, $A(S_C)$;
- процессы эволюционного развития S_C, $(E(S_C))$;
- процессы локальных модификаций S_C, $(M(S_C))$;
- процессы вырождения S_C, $(V(S_C))$;
- процессы деградации S_C, $(D(S_C))$;
- стабилизирующие процессы в S_C, $(C(S_C))$;
- катастрофические процессы в S_C, $(K(S_C))$.

Процессы изменения уровня абстракции описываются в общем случае соотношением (1) и формальными представлениями условий 1-3. Такой параметр, как уровень абстракции S_C, который будем обозначать символом μ, представляет собой характеристику однократного преобразования $S_{Ci} \to S_{C(i+1)}$.

Процессы эволюционного развития S_C охватывают целый ряд преобразований семантического словаря S_C и, в общем случае, могут быть

представлены в виде следующего соотношения:

$$E(S_C) = \{f_1[S_{C1}, d_1(t)] \to f_2[S_{C2}, d_2(t)] \to ... \to f_n[S_{Cn}, d_n(t)]\},$$

где f_i - функция, которая описывает преобразование в словаре S_C с учетом интерактивного взаимодействия с системой доступа, которая расширена подсистемой безопасности доступа, $d_i(t)$ - интерактивное взаимодействие пользователя, который использует описание предметной области S_{Ci}, t - время реализации соответствующего взаимодействия. Очевидно, что этот процесс $E(S_C)$ должен оцениваться критериями, которые определяют его, как эволюционный процесс. Все процессы, которые могут происходить в S_C, инициируются пользователем, при этом, пользователь может быть санкционированным и несанкционированным. Естественно предположить, что все процессы, которые происходят в S_C, описываются параметрами, значения которых отличаются между собой в случае их инициализации санкционированными пользователями и несанкционированными пользователями. Более того, процессы, инициированные несанкционированным пользователем, могут приводить к ситуациям, которые являются недопустимыми, что определяется следующими факторами, возникающими в S_C:

- противоречивостью, возникающей в S_C и проявляющейся в различных формах (μ_e);
- конфликтами между компонентами S_C, возникающие в результате несанкционированной инициации процессов в S_C, (η_e);
- нарушения процесса функциональных преобразований, которые регламентированы выше приведенными типами процессов и могут состоять в циклических модификациях S_C, в дублировании элементов S_C и других проявлениях соответствующих нарушений (χ_e).

Эволюционность процессов в произвольных объектах определяется по отношению к окружающей среде, в которой соответствующий объект функционирует. В настоящем случае, окружающая среда для S_C сводится к системе доступа, с которой взаимодействует S_C посредством инициации пользователем взаимодействия с системой доступа. Поэтому критерии эволюционности процессов должны характеризовать увеличение уровня безопасности. В общем случае, уровень безопасности доступа характеризуется некоторым центральным параметром системы доступа, который учитывает все факторы, влияющие на уровень безопасности. В данном случае, рассмотрим этот параметр только в части, которая учитывает факторы, связанные с S_C. Факторы, которые отражают изменение уровня безопасности приведены выше. Эти факторы обладают следующей особенностью. Поскольку их появление обуславливается действиями

несанкционированного пользователя, то последний не инициирует непосредственных изменений в S_C, а осуществляя несанкционированный доступ к объекту, и в случае его выявления, дает основание внешним по отношению к S_C компонентам, интерпретировать данные, которые он использовал, как таковые, которые принадлежат S_C. Таким образом, можно принять, что эволюционный процесс в S_C имеет место, если $[\gamma = \mu_e + \eta_e + \chi_e] \to \min(\gamma)$. Для упрощения рассмотрения, примем, что все μ_e, η_e и χ_e являются равноценными с точки зрения их влияния на уровень безопасности и будем их обозначать одним символом ξ_i.

Процессы локальных модификаций S_C или $M(S_C)$ чаще всего связаны с необходимостью со стороны легального пользователя, расширить возможности в получении ресурсов из объекта доступа. Несмотря на то, что такая модификация проводится легальным пользователем, она может привести к возникновению факторов типа ξ_i, особенно, если S_C уже расширялась на предыдущих этапах функционирования системы: $P \leftrightarrow SD \leftrightarrow OD$, где P - пользователь, OD - объект доступа.

Процессы вырождения $V(S_C)$ представляют собой такие преобразования в S_C, которые приводят к уменьшению возможного разнообразия при формировании запросов на обслуживание. Определение величины параметра, который характеризует процесс деградации, достаточно сложно, поскольку простое уменьшение компонент в S_C не приводит к уменьшению возможных запросов к системе SD. Запросы, которые могут формироваться на основе данных из S_C, будем обозначать z_i. Для формирования запросов z_i кроме данных из S_C, используются системы вывода новых формул запроса, которая включает в себя систему правил формирования семантических правильных формул Ω и систему семантических правил $P\Lambda$, что формально можно записать следующим образом:

$$[S_C, \Omega(S_C), P\Lambda(S_C), \Lambda] \to z_i . \qquad (3)$$

Прежде чем в конструктивном виде представлять соотношение (3), рассмотрим на качественном уровне остальные процессы.

Процессы деградации $D(S_C)$ отличаются от процессов $V(S_C)$ тем, что $D(S_C)$ не приводят к уменьшению количества элементов в S_C, а лишь приводят к уменьшению количества запросов, которые могут быть выведены на основе использования S_C. Поскольку z_i в соответствии с (2) зависит не только от S_C, то рассмотрим, какие преобразования в S_C могут повлиять на возможность вывода z_i из Σ, где $\Sigma = \{S_C, \Omega(S_C), P\Lambda(S_C), \Lambda\}$. Поскольку

количество элементов в S_C в результате $D(S_C)$ не изменяется, то $D(S_C)$ должно влиять на $\Omega(S_C)$ и $P\Lambda(S_C)$, или хотя бы на одну из этих компонент. Поскольку $P\Lambda$ и Ω представляют собой системы правил, то процессы $D(S_C)$ осуществляют такое преобразование $(\Omega \& P\Lambda) \vee \Omega \vee P\Lambda$, которое делает невозможным их использование при выводе z_i. Этот фактор проявляется в том случае, если соответствующие x_i из S_C изменяют свои интерпретационные описания $T(x_i)$ таким образом, что $\Omega(S_C)$, или $P\Lambda(S_C)$ или $(\Omega(S_C) \& P\Lambda(S_C))$ становятся противоречивыми, при реализации соотношения (2) или процедура z_i приводит к конфликтной ситуации в процессе $L_i(S_C, \Omega(S_C), P\Lambda(S_C), \Lambda) \to z_i$, где L_i - функция логического вывода z_i.

Стабилизирующие процессы $C(S_C)$ представляют альтернативу для процессов дестабилизирующих, к которым можно отнести процессы $V(S_C)$ и $D(S_C)$. Дело в том, что $V(S_C)$ и $D(S_C)$ могут инициироваться внешними, по отношению к SD факторами, с целью компрометации SD или с целью реализации атаки на SD. Таким образом, $C(S_C)$ представляет собой процесс противодействия вторжению в систему SD. Поскольку последствием дестабилизации, к которой приводят $V(S_C)$ и $D(S_C)$, является возникновение в S_C противоречивостей и конфликтов, то $C(S_C)$ должен их устранять. Очевидно, что инициация такого осуществляется не только в случае, когда необходимый z_i оказывается невыводимым, но и в случае реализации процессов определения уровня безопасности системы BSD в целом. Эти процессы реализуются в соответствии с алгоритмами обеспечения заданного уровня безопасности системы доступа в целом. Как уже отмечалось, под безопасной системой доступа будем подразумевать тройку $BSD =< P, SD, OD >$.

Катастрофические процессы $K(S_C)$ представляют собой процессы, которым в рамках BSD невозможно противодействовать. Все рассмотренные процессы представляют собой определенные последовательности преобразований, в данном случае, преобразований в S_C. Поскольку дестабилизирующими процессами являются $V(S_C)$ и $D(S_C)$, то формально, для определения $K(S_C)$ можно записать соотношение:

$$\{\{[V(S_C) \& D(S_C)] \vee \Phi[V(S_C), D(S_C)]\} \& \neg C(S_C)\} \to K(S_C),$$

где Ф – функция организации взаимодействия между $V(S_C)$ и $D(S_C)$. Отрицание перед $C(S_C)$ означает, что $C(S_C)$ не может противодействовать санкционированным изменениям в S_C.

Итак, статье рассмотрены вопросы формирования и существования словарей S_C, содержащих описание базовых элементов предметных областей, входящих в состав системы доступа информационной системы. Предложены и формализованы условия исключающие возможности возникновения противоречивости в ситуации, когда две различные предметные области, которые используют различные базовые элементы по отношению друг к другу, обладают максимальными уровнями абстракции.

1. *Герасименко В. А*. Основы защиты информации / *В.А. Герасименко В. А.,А.А. Малкж*. - М.: МГИФ. 1997. - 537 с.
2. *Девянин П.Н.* Модели безопасности компьютерных систем / *П.Н. Девянин.* - М.:"Академия". 2005. - 144 с.
3. *Мельников В.В.* Безопасность информации в автоматизированных системах/ *В.В. Мельников*. - М.: Финансы и статистика, 2006. - 368 с.
4. *Давиденко А. М.* Моделі оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / *А.М. Давиденко* // Матеріали XXIV науково-технічної конференції "Моделювання" Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – Київ: ІПМЕ ім. Г.Є. Пухова НАНУ, 2005. – С. 43.
5. *Давиденко А. Н*. Анализ средств защиты баз данных / *А.Н. Давиденко* // Моделювання та інформаційні технології : зб. наук. пр. – К.: ІПМЕ НАНУ, 2003. – Вип. 20. – С. 137-141.

Поступила 24.01.2011р.

УДК 681

А.А.Владимирский, И.А.Владимирский, И.П.Криворучко, А.А.Криворот, Н.П.Савчук

РАЗРАБОТКА ДИАГНОСТИЧЕСКОГО ЗОНДА ДЗ-1

Диагностический зонд ДЗ-1 (в дальнейшем зонд) предназначен для визуального и параметрического обследования состояния трубопроводов тепловых сетей, проложенных в непроходных каналах.

Различная теледиагностическая аппаратура для визуального обследования технических конструкций известна достаточно широко (см. табл.1). Ввиду большого разнообразия условий применения характеристики этих устройств существенно различаются. В некоторых изделиях присутствует аудиоканал.

При разработке ДЗ-1 учитывалось наличие ряда специфических требований к особенностям эксплуатации зонда и его функциональным возможностям.