УДК 681.3.06

**А.В. ПОТИЙ, И.В. ЛАРГИН, Ю.П. ТКАЧУК**

***Харьковский национальный университет радиоэлектроники, Украина***

# ОПИСАНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В НОТАЦИИ ARIS eEPC

Предлагается способ описания дополнительных атрибутов безопасности информации при моделировании процессов в нотации ARIS eEPC. Обосновываются типы атрибутов безопасности, объекты модели ARIS, которым могут быть присвоены эти атрибуты, а также технические особенности реализации в пакете ARIS.

**безопасность информации, атрибуты, ARIS eEPC, группа атрибутов, тип атрибута**

## Введение

Теория моделирования технических систем и процессов в 20-м веке убедительно доказала свою эффективность и практическую значимость. Этого нельзя сказать о моделировании экономических систем и процессов. Достижения в области математики и быстрое развитие средств вычислительной техники существенно расширили возможности создания и развития новых высокоэффективных теорий моделирования [1]. В настоящее время примеров практического использования моделей экономических систем в мировой практике немного, а в украинской действительности они пока единичны. Но заказчик, например, автоматизированной системы управления предприятием или системы автоматизации технологических процессов желает “увидеть” и скорректировать будущую систему до того, как он оплатит ее изготовление и она будет реализована физически. А для этого необходимо моделирование проектируемой системы. Наличие комплексной модели предприятия является основой для выполнения следующих работ: проведения анализа, оценки и внесения предложений по совершенствованию деятельности предприятия; разработки автоматизированной системы управления предприятием; разработки системного проекта и внедрения корпоративной информационной системы (КИС), поддерживающей систему управления; подготовки и проведения процедуры сертификации предприятия в соответствии с требованиями международных стандартов качества серии ИСО 9000 и т. д.

Наибольшую перспективу имеют комплексные (интегрированные) методологии моделирования бизнес-систем и бизнес-процессов (БП), к которым относится ARIS-методология, позволяющая в зависимости от целей проектирования выбирать соответствующие модели.

Методология помогает охватить и учесть все важные этапы, шаги и моменты моделирования. Более того, методология обеспечивает организационную поддержку, позволяющую скоординировать работу больших коллективов разработчиков. ARIS-методологию используют для описания деятельности предприятия.

Инструментарий ARIS используется для описания бизнес-процессов компании. Результатом описания является набор взаимосвязанных моделей ARIS [1, 2].

Основной предпосылкой написания этой статьи послужил недостаток ARIS, который заключается в отсутствии атрибутов, характеризующих требования по обеспечению безопасности информации в моделируемой системе. К таковым относятся требования

по обеспечению конфиденциальность, целостность, доступность информации.

В данной статье рассматриваются базовые атрибуты среды ARIS, способ добавления новых атрибутов, характеризующих требования по обеспечению безопасности информации, а также объекты, которым могут быть присвоены данные атрибуты, на примере модели событийной цепочки процесса (ARIS eEPC).

## 1. Характеристика атрибутов в нотации ARIS eEPC

Каждый объект ARIS обладает собственным набором атрибутов, при помощи которых можно задать количественные и качественные характеристики моделируемых элементов системы. *Атрибутом* называется необходимое, существенное, неотъемлемое свойство объекта [2].

Атрибуты позволяют записывать и модифицировать характеристики моделей. Они организованы в иерархическую древовидную структуру папок, что обеспечивает их быстрый обзор и позволяет сравнивать значения атрибутов, размещенных в смежных столбцах. Например, можно просмотреть значения атрибутов сразу нескольких объектов и сравнить их. Родственные по смыслу типы атрибутов объединены в папки, состав которых зависит от типа модели, объекта или связи.

Атрибуты имеют следующие элементы ARIS: пользователи (User); группы пользователей (User Group); папки(Groups); базы данных (Databases); модели (Models); объекты (Objects); связи (Relationships); языки (Languages); шрифты (Font formats); текст произвольной формы (Free Form Text) [2].

Отметим некоторые типы атрибутов, содержащиеся в главной папке. К стандартным атрибутам относятся:

– атрибут *Name (Имя)* позволяет давать имя сущности;

– атрибут *Identifier (Идентификатор)* содержит уникальное имя сущности (например, 21.77, ABC.31);

– атрибут *Full name (Полное имя)* задает полное имя для соответствующей сущности.

Для более полного текстового описания сущности используются атрибуты *Description/Definition (Описание/Определение)* и *Remark/Example (Замечание/Пример).*

Некоторые атрибуты заполняются автоматически, например:

– тип элемента (*Type);*

– время создания (*Time of generations);*

– автор *(Created by)* последнего изменения*(Last change);*

– последний пользователь *(Last user).*

Остальные атрибуты определяются исследователем.

Число атрибутов, особенно для объектов, весьма велико и может достигать нескольких десятков. Для того чтобы при моделировании получить понятные и модифицируемые результаты, необходимо решить, какие типы атрибутов будут заполнены в моделях, объектах и связях. На выбор тех или иных типов атрибутов в значительной степени влияют цели моделирования.

Рассмотрим основные элементы модели ARIS eEPC и базовые атрибуты, применяемые к объектам данной модели [2].

Нотации ARIS eEPC (Extended Event Driven Process Chain) представляют собой расширенную нотацию описания цепочки процесса, управляемого событиями. Определим следующие основные объекты, используемые в рамках нотации [1 – 3]:

- функция (Function) – объект служит для описания функций (процедур, работ), выполняемых подразделениями (сотрудниками) предприятия;
- событие (Event) – объект служит для описания реальных состояний системы, влияющих и управляющих выполнением функций;

- организационная единица (Organizational Unit) – объект обозначает различные организационные звенья компании (например, отдел);
- документ (Document) – объект, отражающий реальные носители информации, например бумажный документ;
- прикладная система (Application system) – объект отражает реальную прикладную систему, используемую в рамках выполнения технологии функции;
- кластер информации (Cluster) – объект характеризует данные как набор сущностей и связей между ними. Используется для создания моделей данных;

Кроме того, на объектах определены типы отношений и логические операции “И”, “ИЛИ”, исключающие “ИЛИ”.

## 2. Способ добавления новых атрибутов

Несмотря на то, что количество атрибутов в ARIS Toolset достаточно велико, возникла необходимость добавления новых атрибутов, характеризующих требования или свойства безопасности информации. Далее будем называть такие атрибуты атрибутами безопасности.

Для решения этой задачи необходимо ответить на три вопроса:

– какие атрибуты безопасности необходимо добавить?

– каким образом это возможно осуществить?

– как новые атрибуты можно применить на практике?

Бизнес-процессы и бизнес-системы, моделируемые в среде ARIS, имеют дело с обработкой информационных потоков. В ходе моделирования необходимо определить требования по обеспечению безопасности информации. Под безопасностью информации (БИ) понимают – состояние информации, в котором обеспечивается сохранение определенных политикой безопасности свойств информации [4]. К этим свойствам относятся конфиденциальность, доступность, целостность и наблюдаемость:

- конфиденциальность (англ. confidentiality) информации – свойство информации, которое заключается в том, что информация не может быть получена неавторизованным пользователем и/или процессом;
- целостность (англ. integrity) информации – свойство системы, которое заключается в том, что каждый ее компонент не может быть устранен, модифицирован или прибавлен с нарушением политики безопасности;
- доступность (англ. availability) – свойство ресурса информации, которое заключается в том, что пользователь и/или процесс, который владеет соответствующими полномочиями, может использовать ресурс в соответствии с правилами, установленными политикой безопасности, не ожидая дольше заданного (малого) промежутка времени, т.е когда он находится в виде, необходимом пользователю, в месте, необходимом пользователю, и в то время, когда он ему необходим [4].

Также определённый интерес представляет такой компонент как категория доступа (англ. security clearance).

Реализация функций безопасности информации оказывается значительно более дешевой и эффективной, если они встраиваются в информационные системы и сервисы на стадиях задания требований и проектирования. Чем скорее организация примет меры по защите своих информационных систем, тем более дешевыми и эффективными они будут для нее впоследствии. Поэтому вопрос о добавлении группы атрибутов, отвечающих за безопасность информации при проектировании и моделировании различного рода процессов с использованием среды ARIS, является достаточно актуальным.

Данная задача решается с помощью встроенных средств самой среды ARIS. Модуль *ARIS*

*Configuration* позволяет корректировать методы и объекты ARIS, приспосабливая их к требованиям конкретных пользователей или специфических задач.

В нотации ARIS определены так называемые *Free attributes*, с помощью которых можно добавить новые атрибуты. Добавление атрибутов происходит следующим образом.

1. Создается новая группа атрибутов *Security* (безопасность). Это происходит путём переименования любой *Free attribute type group* в закладке *Attribute type groups* (рис. 1).

2. Создание новых атрибутов происходит аналогичным образом в закладке *Attribute types.* Существуют следующие типы *Free attributes:* Boolean, Date, Duration, Float, Integer, Point in time, Text, Time, Values. Для решения нашей задачи наиболее подходящим является тип Values. При использовании типа Values выбор уровня происходит в выпадающем меню, причем уровни задаются в момент создания атрибута и являются одинаковыми для всех элементов использующих данный атрибут. Для удобства использования созданные атрибуты помещаем в группу *Security*. На рис. 2 показано создание атрибута *Confidentiality* (конфиденциальность) используя тип Values.

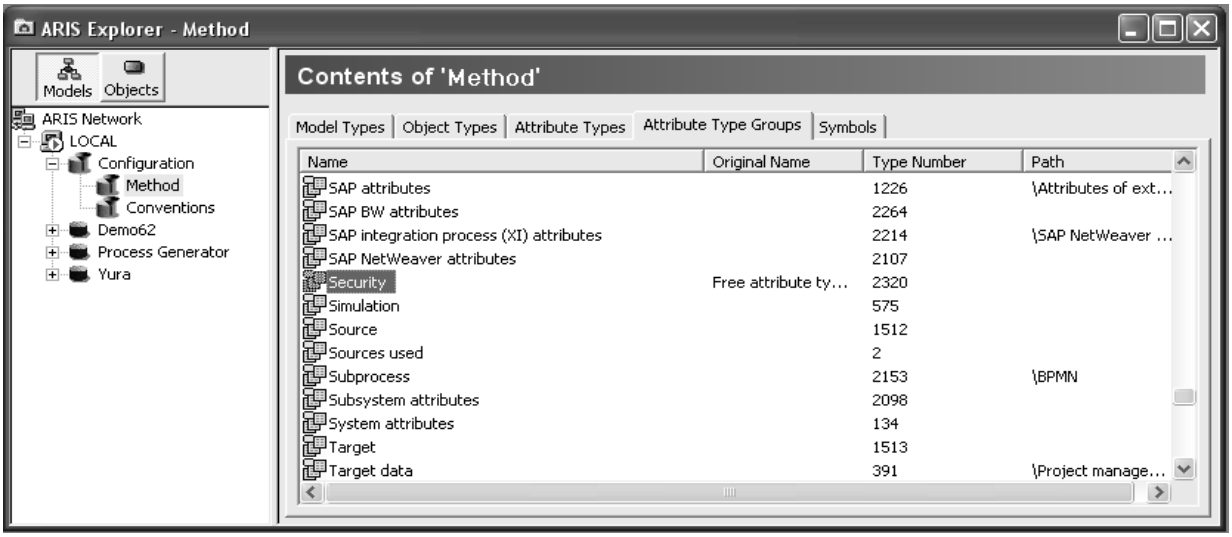


Рис. 1. Создание группы атрибутов

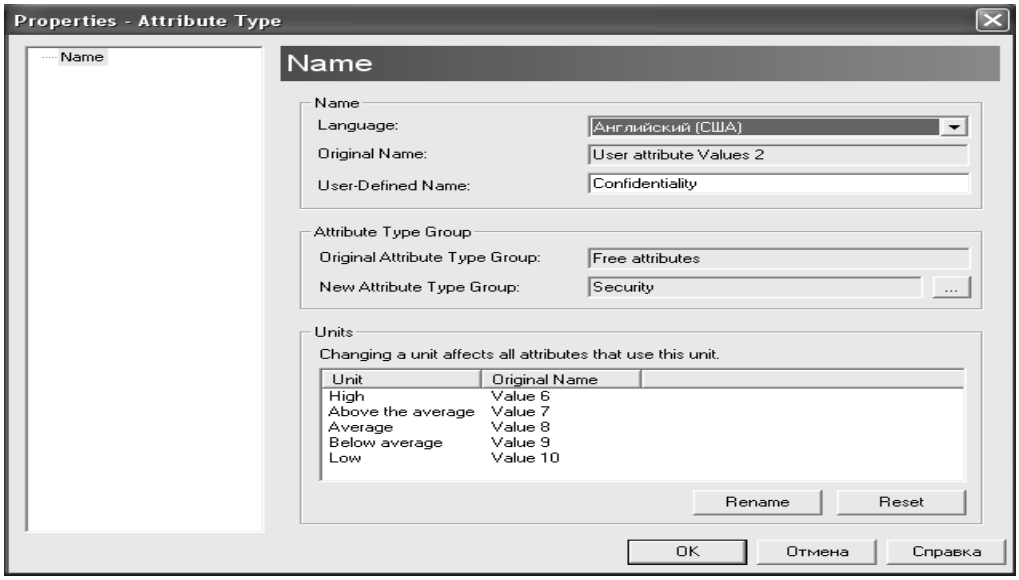


Рис. 2. Атрибут Confidentiality (конфиденциальность) – тип Values

3. В результате создана группа *Security* с атрибутом *Confidentiality* (рис. 3). Аналогичным образом можно добавить атрибуты *Integrity* (целостность) и *Availability* (доступность). Новая группа атрибутов будет доступна для использования во всех моделях ARIS и может быть применена к любому объекту. Используем пятиуровневую шкалу задания уровня требований безопасности (рис. 3).

Таким образом, в среде ARIS мы определили атрибуты безопасности.

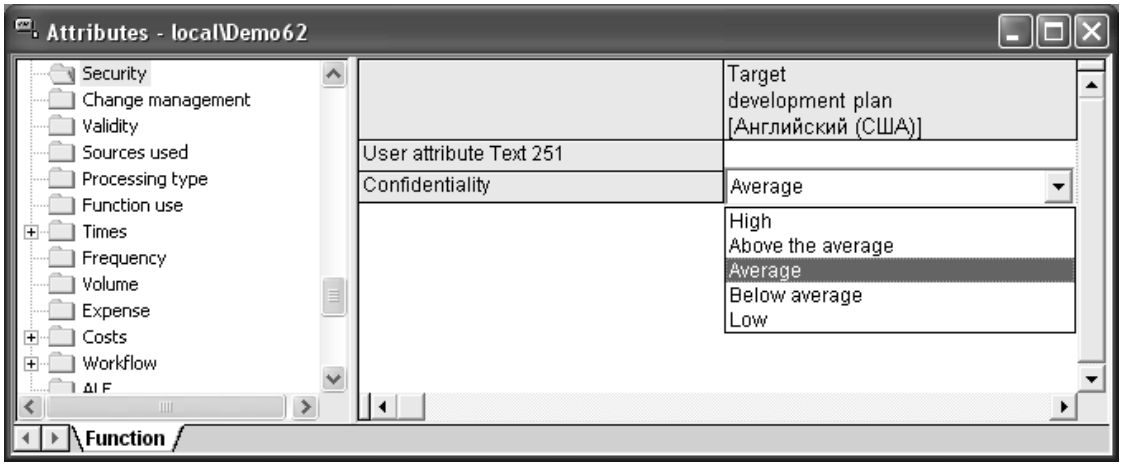


Рис. 3. Окно *Attributes* элемента *Function* модели ARIS eEPC

## 3. Использование атрибутов безопасности на примере модели ARIS eEPC

Возьмем пример eEPC. Определим, какие объекты диаграммы могут обладать атрибутами безопасности. (табл. 1).

Рассмотрим процесс подготовки проекта стратегического развития организации с учетом критериев безопасности информации (рис. 4).

На разных этапах моделирования проекта мы можем наблюдать изменение уровня требований безопасности (табл. 2).

Таблица 1

Атрибуты безопасности объектов

| Тип объекта | | Критерии безопасности информации | | | |
|---|---|---|---|---|---|
| | | Конфиденциальность | Целостность | Доступность | Категория доступа |
| Person type | Тип сотрудника (штатный, внештатный) | – | – | – | + |
| Application system type | Тип прикладной системы | + | + | + | - |
| Function | Функция | + | + | + | – |
| Event | Событие | + | + | + | – |

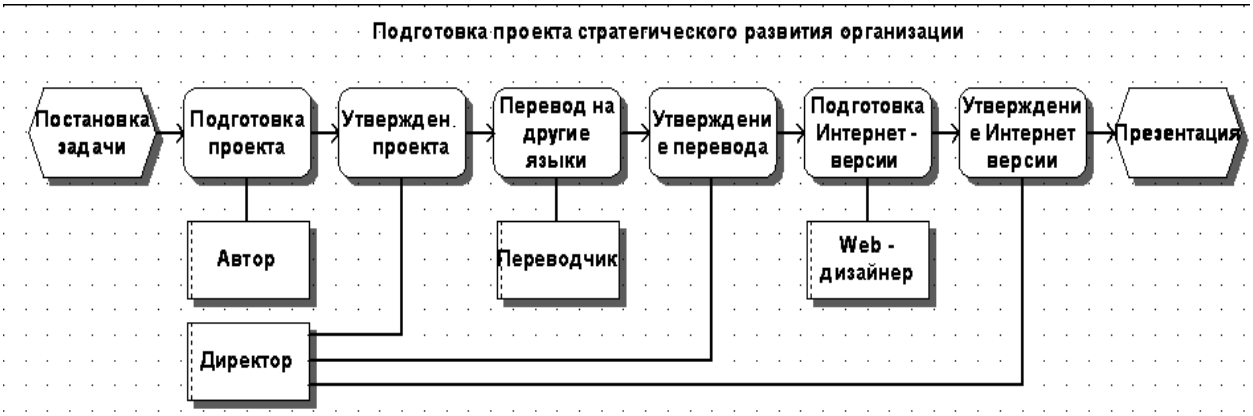


Рис. 4. Пример модели eEPC

Таблица 2

Изменение уровня требований безопасности

| Название атрибута | Название объекта | | | |
|---|---|---|---|---|
| | Подготовка проекта | Перевод на другие языки | Утверждение | Презентация |
| Конфиденциальность | High | High | High | Low |
| Целостность | Low | Low | High | High |
| Доступность | Low | Low | Low | High |

## Заключение

В результате добавления атрибутов безопасности открываются новые возможности работы с ARIS-методологией:

– контроль соответствия безопасности для различных объектов модели;

– при моделировании учитывается динамический характер изменения свойств безопасности;

– с точки зрения формирования требований безопасности при моделировании учитывается жизненный цикл информации;

– в перспективе можно разрабатывать формальную линию проверки соответствия уровня требований и уровня безопасности. Это позволит создать формальный аппарат модели *политики безопасности процесса.*

## Литература

1. Войнов И.В., Пудовкина С.Г., Телегин А.И. Моделирование экономических систем и процессов. Опыт построения ARIS-моделей: Монография. – Челябинск: Изд. Ургу, 2002. – 392 с.

2. Каменева М.С., Громов А.И, Шматалюк А.Е. Моделирование бизнеса. Методология ARIS. – М., 2001. – 333 с.

3. ARIS Method. Version 6. June 2004. Copyright (©) 1997 - 2000 by IDS ScheerAG, Saarbrucken.

4. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в КС від НСД.

*Поступила в редакцию 6.02.2006*

**Рецензент:** д-р техн. наук, проф. И.Д. Горбенко, ЗАО «Институт информационных технологий», Харьков.