УДК 681.324

В.В. СКЛЯР

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ОЦЕНКА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ КРИТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ: ЭЛЕМЕНТЫ МЕТОДОЛОГИИ И ФОРМАЛЬНЫЕ МОДЕЛИ

Предложен системный подход к оценке и обеспечению безопасности информационно-управляющих систем технических комплексов критического использования, основанный на применении ER-модели (модели «сущность-связь»).

безопасность информационно-управляющих систем, технические комплексы критического использования

Введение

Роль техногенных аэрокосмических, энергетических, транспортных, коммуникационных, военных, финансовых, промышленных комплексов и их влияние на человеческое общество постоянно возрастает. Одновременно возрастает потенциальный ущерб, который может нанести отказ таких комплексов. Наиболее существенным свойством указанных объектов является безопасность, под которой подразумевается способность объекта достигать приемлемых уровней риска для жизни и здоровья людей, окружающей среды и экономики [1]. Поэтому комплексы, отказы которых представляют собой потенциальную угрозу, называют техническими комплексами критического использования (ТККИ).

Важность проблемы безопасности определяется имеющими место производственными инцидентами с человеческими жертвами. По данным Международной организации труда (International Labour Organization) количество жертв, связанных с производственными инцидентами, в мире составляет примерно 300 тысяч человек в год [2].

Отметим, что определения безопасности из разных источников отличаются друг от друга и до сих пор являются дискуссионными [1].

При формулировании понятия «безопасность ИУС» необходимо исходить из следующего:

– понятие «безопасность ИУС» должно вытекать из более общего понятия «безопасность ТККИ»;

– понятие «безопасность ТККИ» должно соотноситься с интуитивно подразумеваемым понятием «безопасность»;

– безопасность ИУС и ТККИ является одним из свойств этого объекта, находящимся в одном ряду с такими понятиями как надежность, качество, живучесть.

Приведем три определения понятия безопасность.

В «Толковом словаре русского языка» под редакцией Д.И. Ушакова: «Безопасность – отсутствие опасности… Предупреждение опасности, условия, при которых не угрожает опасность» [3].

Согласно «Webster new world dictionary»: «Безопасность – свойство находиться в защищенном состоянии; отсутствие опасности травм и аварий; уверенность» [4].

В сфере обеспечения качества используется определение стандарта ИСО 8402 «Словарь по качеству»: «безопасность – состояние, при котором риск вреда (для персонала) или ущерб ограничен допустимым уровнем».

Все эти определения не противоречат следующему по уровню иерархии понятию безопасность

ТККИ (промышленного предприятия), которое формулируется в ДСТУ 2156-93 «Безопасность промышленных предприятий. Термины и определения» как «свойство предприятия при нормальной эксплуатации и в случае аварии ограничивать воздействие источников опасности на персонал, население и окружающую среду установленными пределами».

Широкое распространение ИУС в различных отраслях техники привело к возникновению понятия «функциональная безопасность систем». Это понятие является ключевым в стандарте Международной электротехнической комиссии МЭК 61508 «Функциональная безопасность электрических, электронных и программируемых электронных систем, важных для безопасности». Понятие функциональной безопасности ИУС относится к совокупности управляемого оборудования и систем управления этим оборудованием и определяется как часть общей безопасности, которая зависит от правильного функционирования ИУС с другими технологическими системами, а также с внешними устройствами для снижения риска [5].

В качестве вывода отметим, что результаты проведенного анализа понятия «безопасность» соответствуют первоначально сформулированному определению безопасности ИУС ТККИ.

На современном этапе развития науки и техники наиболее динамично развиваются информационные технологии. Поэтому, одной из основных тенденций развития ТККИ является повсеместное внедрение компьютерных информационно-управляющих систем (ИУС). Это приводит к тому, что надежность и безопасность ИУС стали играть решающую роль в обеспечении безопасности ТККИ [6]. Например, отказы ИУС являются причиной около 20% аварий ракетно-космической техники [7].

К настоящему времени общая теория безопасности описана в ряде книг, например [8 – 10]. Теория безопасности компьютерных систем критического использования получила развитие в трудах А. Авижениса [11], Ж.-К. Лапри [12], Н. Левенсон [13], В.С. Харченко [14], М.А. Ястребинецкого [15]. В 2004 г. была опубликована монография [1], в которой впервые в отечественной литературе был обобщен опыт оценки и обеспечения безопасности ИУС АЭС.

Однако известные работы посвящены, как правило, отдельным отраслям промышленности, и в них отсутствуют обобщения, позволяющие распространить теоретические положения на ИУС ТККИ безотносительно к прикладной области. Кроме того, требуют детальной проработки методы оценки и обеспечения безопасности программного обеспечения (ПО) и автоматов с программируемой логикой для ИУС ТККИ, разработанных с использованием новейшей элементной базы. Дополнительного развития требуют теоретические аспекты разработки и оценки ИУС ТККИ, построенных на основе многокомпонентных и многоверсионных технологий.

Целью данной публикации является разработка элементов комплексного подхода к решению научной проблемы оценки и обеспечения безопасности цифровых информационно-управляющих систем критического использования.

Общая схема оценки и обеспечения безопасности ИУС ТККИ

В качестве первого шага разработки комплексного подхода к решению сформулированной выше проблемы предлагается общая схема оценки и обеспечения безопасности ИУС ТККИ (рис. 1).

Ниже описаны взаимосвязи между элементами рис. 1.

Исходным пунктом обеспечения безопасности являются требования законодательных и нормативно-технических документов, соблюдение которых является обязательным при осуществлении всех видов деятельности, связанных с потенциально опасностью.

Технические требования к ИУС, важным для безопасности ТККИ, детализированы в стандартах и других нормативно-технических документах (далее для краткости используется термин «стандарты»).

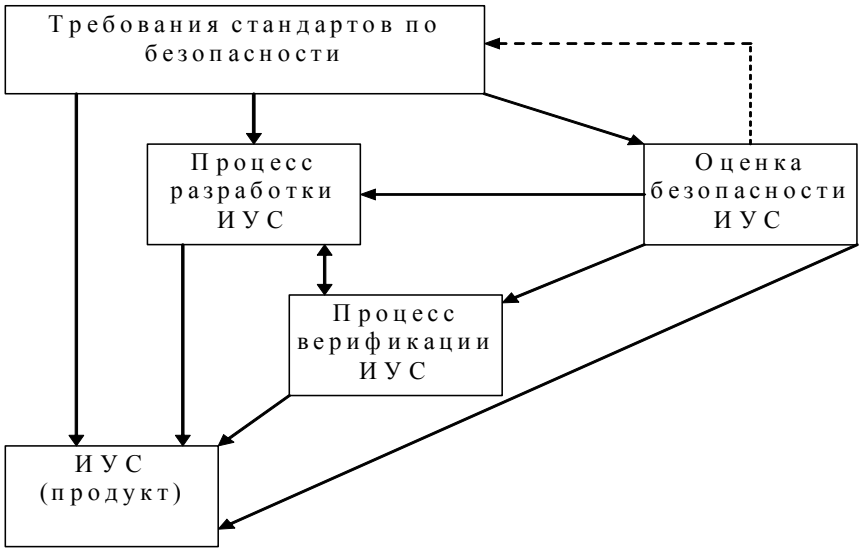

Рис. 1. Общая схема оценки и обеспечения безопасности ИУС ТККИ

Стандарты по безопасности отражают мировой опыт по разработке и эксплуатации ТККИ и содержат так называемые регулирующие требования, соблюдение которых на данном этапе развития науки, техники и технологии признается необходимым и считается достаточным для обеспечения безопасности [1].

Существует две категории стандартов по безопасности:

– стандарты, содержащие требования к ИУС;

– стандарты, содержащие методики оценки ИУС на соответствие требованиям стандартов первой категории.

Требования стандартов к ИУС можно разделить на две большие группы:

– требования к продуктам, т.е. требования непосредственно к ИУС;

– требования к процессам, основными из которых являются взаимосвязанные процессы разработки и верификации ИУС.

Процесс оценки позволяет определить соответствие ИУС требованиям стандартов по безопасности. Оценка ИУС включает как оценку на соответствия требованиям к продуктам, так и на соответствие требованиям к процессам. Учитывая особое значение оценки в общей схеме обеспечении безопасности, обычно ведут речь об оценке и обеспечении безопасности ИУС, как о едином неразрывном процессе.

Процесс оценки, кроме того, является источником усовершенствования стандартов по безопасности, так как позволяет накапливать и анализировать опыт, полученный при работе с ИУС, построенными с использованием новых технических решений. Данный факт отображен на рис. 1 в виде пунктирной стрелки.

Оценка безопасности, выполняемая для ИУС, характеризуется такими свойствами, как сложность, комплексность, многокритериальность, неформализуемость и т.п. В общем случае для оценки конкретной ИУС, как правило, невозможно использовать только один метод оценки. Это приводит к необходимости использования различных методов, технологий, инструментальных средств и т.п., а также к необходимости привлечения специалистов в разных областях знаний для оценки безопасности одной ИУС. Поэтому для ИУС, важных для безопасности, выполняется, как правило, экспертная оценка [1].

Отдельного пояснения требует взаимосвязь процессов разработки и верификации. Процесс верификации – это процесс определения того, удовлетворяют ли программные продукты, которые являются результатом некоторых действий по разработке, требованиям и условиям, наложенным на них предшествующими действиями [16]. Верификация осуществляется при переходе между смежными этапами разработки продукта (как правило, программного продукта) и является обязательным мероприятием для ИУС ТККИ. Это проиллюстрировано на рис. 2.

Разработка является процессом по преобразованию продукта из одного вида в другой. При помощи процесса верификации реализуется обратная связь между продуктами разработки, что позволяет продемонстрировать идентичность продуктов, полученных на разных стадиях разработки, а также их соответствие исходным требованиям. Исходный и конечный продукт, а также процессы разработки и верификации должны подвергаться оценке на соответствие требованиям по безопасности.

Взаимосвязанными составляющими схемы обеспечения безопасности ИУС (рис. 1) являются:

– требования стандартов по безопасности, включая требования к ИУС и их компонентам, а также требования к методам разработки, верификации и оценки;

– процессы разработки и верификации ИУС, а также другие процессы жизненного цикла (ЖЦ);

– продукты разработки (компоненты ИУС).

Таким образом, структурная схема обеспечения безопасности ИУС может быть представлена в виде трехмерного пространства (куба), как на рис. 3.

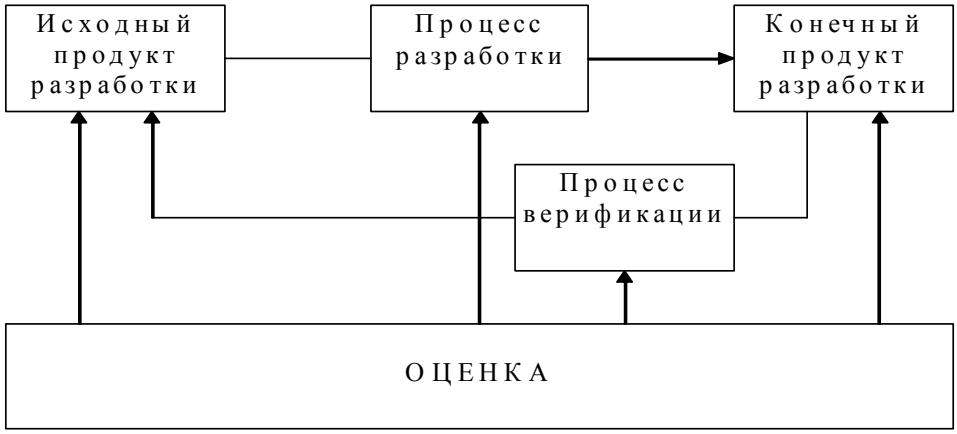

Рис. 2. Взаимосвязь процессов разработки, верификации и оценки ИУС

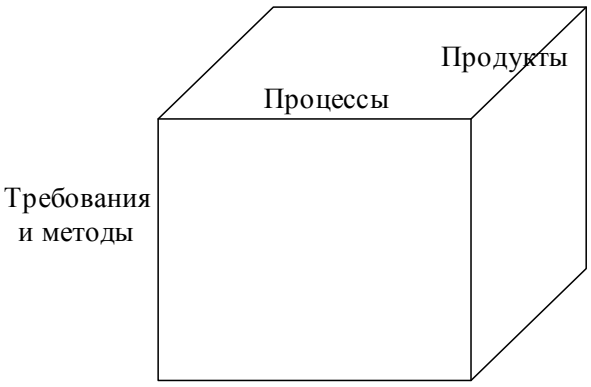

Рис. 3. Структура пространства обеспечения безопасности ИУС, представленная в виде куба «Требования и методы – Процессы – Продукты»

Системная модель оценки и обеспечения безопасности ИУС ТККИ

Системная модель обеспечения и оценки безопасности ИУС ТККИ может быть разработана на основе проведенного анализа общей схемы обеспечения безопасности ИУС ТККИ. Проанализируем подробнее каждую из составляющих пространства обеспечения безопасности ИУС.

Что касается продуктов (компонент ИУС), их состав определяется спецификой конкретной ИУС. Как правило, в любой ИУС можно выделить про-

граммную и аппаратную составляющие, которые, в свою очередь могут иметь сложную структуру.

Для продуктов (программных, аппаратных и системных) необходимо учитывать специфические свойства, влияющие на обеспечения и оценку безопасности. К таким свойствам следует отнести:

– класс безопасности (степень влияния на безопасность ТККИ);

– апробированность;

– тип реализуемой многоверсионности (разнообразия);

– используемую элементную базу (для аппаратных средств);

– используемый язык разработки (для ПО).

Требования стандартов и методы их обеспечения включают:

– непосредственно требования по безопасности к ИУС и их компонентам;

– методы разработки;

– методы верификации;

– методы оценки.

Процессы включают разработку, верификацию, а также другие процессы ЖЦ ИУС (например, управление конфигурацией, обеспечение качества и т.д.). Основную роль в обеспечении безопасности играют процессы разработки и верификации. Каждому из этапов разработки может быть поставлен в соответствие аналогичный этап верификации. Стандартные этапы процессов разработки и верификации ИУС включают [16]: разработку требований, проектирование, реализацию, интеграцию, эксплуатацию и сопровождение.

Такие же этапы могут быть реализованы для программных и аппаратных компонент ИУС. Кроме того, при оценке обеспечения и оценки безопасности ИУС необходимо учитывать специфику прикладной отрасли, в которой применяется ТККИ.

Изложенные выше соображения служат основой для разработки системной модели обеспечения и оценки безопасности ИУС ТККИ. К такой модели выдвигаются следующие требования:

– полнота – модель должна охватывать все аспекты обеспечения и оценки безопасности ИУС ТККИ;

– наглядность – модель должна обеспечивать удобство анализа и восприятия объектов прикладной области;

– универсальность – модель должна учитывать любые свойства входящих в нее объектов;

– практичность – модель должна позволять анализировать конкретные архитектуры ИУС ТККИ и результаты их применения;

– открытость – возможность учета в модели новых теоретических и прикладных результатов;

– автоматизируемость – возможность автоматизации основных операций с моделью, целесообразность которой вытекает из значительной сложности описываемой прикладной области.

Проведенный анализ показал, что наиболее подходящей для описания исследуемой области является модель «сущность-связь» или «Entity-Relationship» (сокращенно ER-модель), широко применяемая для разработки баз данных. Данная модель оперирует следующими базовыми понятиями [17]:

– сущность, с помощью которой моделируется класс однотипных объектов;

– связь – бинарная ассоциация, моделирующая соотношения и взаимодействия между сущностями.

ER-модель для прикладной области оценки и обеспечения безопасности ИУС ТККИ приведена на рис. 4. Для каждой из шести сущностей ER-модели установлен набор атрибутов, состав которых был обсужден выше. Тип всех связей на рис. 4 установлен как «многие-ко-многим» (см. табл. 1). Объекты, включаемые в состав ER-модели, могут иметь сложную многоуровневую структуру, например, представлять собой набор моделей, поддерживающих применение того или иного метода.

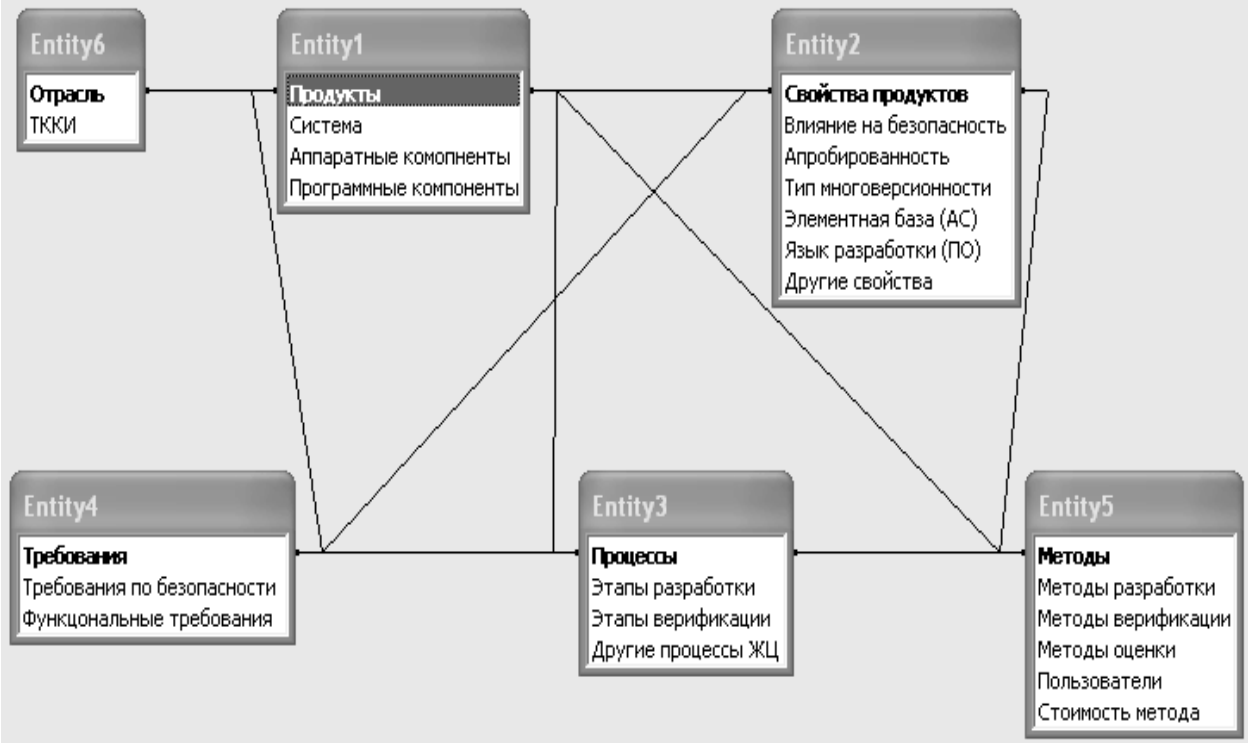

Рис. 4. ER-модель оценки и обеспечения безопасности ИУС

Таблица 1

Структура связей между сущностями ER-модели оценки и обеспечения безопасности ИУС

	Entity1	Entity2	Entity3	Entity4	Entity5	Entity6
Entity1		+	+	+	+	+
Entity2	+			+	+	
Entity3	+			+	+	
Entity4	+	+	+			
Entity5	+	+	+			
Entity6	+					

ER-модель на рис. 4 построена в нотации Microsoft Access. Поскольку в ER-модели имеется значительное количество связей, целесообразно дополнительно привести таблицу связей между сущностями ER-модели. В табл. 1 знаком «+» обозначены те ячейки на пересечении n-х строк и m-х столбцов таблицы, которые соответствуют связям между n-ми и m-ми сущностями.

Применение операций реляционной алгебры для ER-модели оценки и обеспечения безопасности ИУС

Над элементами ER-модели может быть выполнен ряд операций реляционной алгеброй, которая включает в себя операции над отношениями.

Определение 1. n-арным отношением R (множеством кортежей) называют подмножества декартова произведения $D_1 \times D_2 \times ... \times D_n$ множеств атрибутов (доменов) $D_1, D_2, ..., D_n$.

Отношением R в ER-модели оценки и обеспечения безопасности ИУС ТККИ является множество продуктов, соответствующих ИУС либо ее составной части, и относящихся к ним свойств, процессов, методов, требований и отраслей, комбинируемых в любом составе.

Определение 2. Схемой отношения S_R является перечень имен атрибутов данного отношения с указанием домена, которому они относятся: $S_R = (A_1, A_2, ..., A_n)$, $A_i \subseteq D_i$.

Реляционная алгебра включает четыре теоретико-множественные операции (объединение, пересечение, разность и расширенное декартово произведение), а также четыре специальные операции (фильтрация, проектирование, условное соединение и деление). Проведенный анализ показал, что теоретико-множественные операции реляционной алгебры могут быть применены к ER-модели оценки и обеспечения безопасности ИУС ТККИ в полном объеме, а из специальных операций целесообразно применение фильтрации.

Дадим формальное определение и интерпретацию операциям реляционной алгебры, применимой к ER-модели оценки и обеспечения безопасности ИУС ТККИ.

1. Объединение. Результатом данной операции является отношение, содержащее множество кортежей, принадлежащих либо первому, либо второму исходным отношениям, либо обоим отношениям одновременно.

$$R1 \cup R2 = \{ r \mid r \in R1 \vee r \in R2 \},$$

где $R1 = \{ r1 \}$, $R2 = \{ r2 \}$ – исходные отношения;

$r1$, $r2$ – кортежи исходных отношений;

r – кортеж отношения, полученного в результате выполнения операции.

Операция объединения в ER-модели оценки и обеспечения безопасности ИУС ТККИ применяется для интеграции составных компонент и системы в целом из компонент нижнего уровня.

2. Пересечение. Результатом данной операции является отношение, содержащее множество кортежей, принадлежащих и первому, и второму исходным отношениям.

$$R1 \cap R2 = \{ r \mid r \in R1 \wedge r \in R2 \}.$$

Операция пересечения в ER-модели оценки и обеспечения безопасности ИУС ТККИ применяется для выделения в составных компонентах или в системах общих компонент нижнего уровня.

3. Разность. Результатом данной операции является отношение, содержащее множество кортежей, принадлежащих первому, и не принадлежащих второму исходным отношениям.

$$R1 \setminus R2 = \{ r \mid r \in R1 \wedge r \notin R2 \};$$

$$R2 \setminus R1 = \{ r \mid r \in R2 \wedge r \notin R1 \}.$$

В отличие от других теоретико-множественных операций, операция разности не является коммутативной, т.е. ее результат зависит от порядка аргументов. Операция разности в ER-модели оценки и обеспечения безопасности ИУС ТККИ применяется для выделения в составных компонентах или в системах различных компонент нижнего уровня.

4. Расширенное декартово произведение. Результатом данной операции является отношение, со схемой, содержащей схемы исходных отношений, и содержащее множество кортежей, полученных сцеплением каждого кортежа первого исходного отношения с каждым кортежем второго исходного отношения.

$$R1 \otimes R2 = \{ (r1, r2) \mid r1 \in R1 \wedge r2 \in R2 \};$$

$S_{R1} = (A_1, A_2,..., A_n)$, $S_{R2} = (B_1, B_2,..., B_m)$ – схемы исходных отношений;

$S_R = (A_1, A_2,..., A_n, B_1, B_2,..., B_m)$ – схема отношения, полученного в результате выполнения операции.

Операция расширенного декартова произведения в ER-модели оценки и обеспечения безопасности ИУС ТККИ применяется для поиска всего множества вариантов свойств, процессов, методов, требований и отраслей, относящихся к множеству продуктов, соответствующих ИУС либо ее составной части.

5. Фильтрация. Результатом данной операции является отношение, содержащее те кортежи из исходного отношения, для которых истинно условие фильтрации (выбора)

$$R[a(r)] = \{ r \mid r \in R \wedge a(r) = \text{“ИСТИНА”} \},$$

где a – булевское выражение, составленное из термов сравнения с помощью операторов булевой алгебры.

Операция фильтрации в ER-модели оценки и

обеспечения безопасности ИУС ТККИ применяется для поиска отношений, соответствующих определенным условиям применения ИУС.

Следует отметить, что в классической ER-модели отношения, как правило, принадлежат к одной сущности. В разработанной модели отношения являются более динамическими и могут строиться для каждого конкретного случая путем одновременного использования доменов и атрибутов, входящих в состав разных сущностей. Поэтому, для ER-модели оценки и обеспечения безопасности ИУС ТККИ целесообразно применение дополнительной операции, которая не входит в состав операций классической реляционной алгебры. В качестве такой операции предлагается использовать операцию вертикального объединения доменов.

6. Вертикальное объединение. Результатом данной операции является отношение, содержащее множество доменов, принадлежащих либо первому, либо второму исходным отношениям, либо обоим отношениям одновременно

$$R1 \oplus R2 = \{ (r1, r2) \mid r1 \in R1 \vee r2 \in R2 \}.$$

Операция вертикального объединения в ER-модели оценки и обеспечения безопасности ИУС ТККИ применяется для интеграции в составе одного отношения множества продуктов, соответствующих ИУС либо ее составной части, и относящихся к ним свойств, процессов, методов, требований и отраслей.

Исходя из структуры полученной ER-модели для каждой из специфических компонент ИУС, а также для ИУС в целом может быть предложена следующая последовательность действий по оценке и обеспечению безопасности:

– анализ требований стандартов к ИУС и ее компонентам;

– анализ методов разработки ИУС и ее компонент, выбор и применение методов разработки;

– анализ методов верификации ИУС и ее компонент, выбор и применение методов верификации;

– анализ методов оценки ИУС и ее компонент, исходя из процессов их разработки и верификации, выбор и применение методов оценки.

Специфическими продуктами, методология оценки и обеспечения безопасности которых недостаточно освещена в литературе, являются [6]:

– многокомпонентное ПО;

– автоматы с программируемой логикой (АПЛ) на базе программируемых логических интегральных схем (ПЛИС);

– ИУС, разработанные с использованием принципа версионной избыточности;

– ИУС, построенные на основе раннее разработанных программных и аппаратных компонент.

Структура действий по оценке и обеспечению безопасности для каждой из выделенных компонент также может быть описана в терминах ER-модели.

Формализация проблемы оценки и обеспечения безопасности ИУС ТККИ

Исходя из структуры полученной ER-модели в формализованном виде проблема обеспечения и оценки безопасности ИУС ТККИ может быть сформулирована в виде задач анализа и синтеза.

Задача анализа. Имеется ИУС $S = \{HW, SW, A\}$, где HW – характеристики аппаратных средств;

SW – характеристики ПО;

A – архитектура (структура) ИУС.

Для заданной ИУС необходимо выбрать множество методов оценки $D_{ASS} = \{D_{ASSi}\}$, которые обеспечивают для системы наилучшее соотношение

$$\begin{cases} \text{Полнота оценки} \to \max; \\ C \le C_{\text{ДОП.}}, \end{cases}$$

где Полнота оценки – степень охвата действиями по оценке всех процессов жизненного цикла для всех компонент ИУС в зависимости от их свойств и предъявляемых требований по безопасности;

$C_{\text{ДОП.}}$ – заданные (максимально допустимые) затраты на оценку безопасности ИУС.

Задача синтеза. Для ИУС $S = \{HW,SW,A\}$ выбрать множество методов разработки $D_{DEV} = \{D_{DEVi}\}$ и методов верификации $D_{VER} = \{D_{VERi}\}$, которые обеспечивают для системы наилучшее соотношение

$$\begin{cases} \text{Безопасность} \geq \text{Безопасность}_{\text{ДОП.}}; \\ C \to C_{\min}, \end{cases}$$

где $\text{Безопасность}_{\text{ДОП.}}$ – заданный (минимально допустимый) интегральный показатель безопасности ИУС;

C – стоимость ИУС.

Для достижения цели разработки теоретических основ оценки и обеспечения безопасности цифровых ИУС ТККИ должна быть решена совокупность следующих взаимосвязанных задач.

1. Исходной задачей исследования является разработка системной модели обеспечения и оценки безопасности многокомпонентных многоверсионных ИУС, построенных с использованием современных микропроцессоров и программируемой логики. Основой для решения данной задачи является предложенная в настоящей работе ER-модель обеспечения и оценки безопасности ИУС. Решение данной задачи должно включать разработку понятийного аппарата и моделей, позволяющих с единых методологических позиций описать структуру и свойства ИУС и ее компонент, процессы жизненного цикла ИУС, требования к продуктам и процессам, а также методы разработки, верификации и оценки.

Необходимость решения трех следующих задач вытекает из проведенного анализа специфических компонент, применение которых в составе ИУС ТККИ вносит дополнительные риски, и методология оценки и обеспечения безопасности которых недостаточно освещена в известной литературе [6].

2. Разработка методов анализа и синтеза многокомпонентного ПО с учетом требований по безопасности.

3. Разработка методов анализа и синтеза автоматов с программируемой логикой на базе ПЛИС с учетом требований по безопасности.

4. Разработка методов анализа и синтеза многоверсионных многокомпонентных ИУС, построенных на основе ранее разработанных программных и аппаратных компонент, ПЛИС с учетом требований по безопасности.

5. Завершающей задачей, интегрирующей полученные результаты, является разработка информационной технологии поддержки экспертной оценки безопасности ИУС.

Заключение

В статье предложен системный подход к оценке и обеспечению безопасности ИУС ТККИ. Данный подход основан на разработке и применении ER-модели (модели «сущность-связь») оценки и обеспечения безопасности ИУС. Разработанная ER-модель позволяет установить связи между компонентами ИУС, их свойствами, процессами жизненного цикла, требованиями к процессам и продукта, а также методами их разработки, верификации и оценки. Операции с отношениями, входящими в состав ER-модели, основаны на положениях реляционной алгебры.

Проведенное исследование позволило формализовать проблему оценки и обеспечения безопасности ИУС критического использования в виде задач анализа и синтеза. Сформулированы задачи, направленные на разработку теоретических основ оценки и обеспечения безопасности ИУС ТККИ, в том числе, и для компьютерных систем аэрокосмической техники [18, 19].

Дальнейшие исследования по разработке методологии решения научной проблемы оценки и обеспечения безопасности цифровых ИУС ТККИ целесообразно направить на разработку системной модели рисков, возникающих при использовании новых информационных технологий в критических отраслях [6, 18, 19].

Литература

1. Ястребенецкий М.А., Васильченко В.Н., Виноградская С.В. и др. Безопасность атомных станций: информационные и управляющие системы. – К.: Техника, 2004. – 472 с.

2. Takala J. Global estimates of fatal occupational accidents // Proceeding by 16th International Conference of Labour Statistic. – Geneva: International Labour Office. – 1998. – P. 23 – 37.

3. Ушаков Д.И. Толковый словарь русского языка. – М.: ОГИЗ, 1935.– Т. 1.– 1564 с.

4. Webster's new world dictionary. – 3rd college edition. – Prentice hall, 1991.

5. Смит Д., Симпсон К. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов. – М.: Издательский Дом «Технологии», 2004. – 208 с.

6. Харченко В.С., Ястребенецкий М.А., Скляр В.В. Новые информационные технологии и безопасность информационно-управляющих систем АЭС // Ядерная и радиационная безопасность. - 2003.– Т. 6, № 2. – С. 19 – 28.

7. Харченко В.С., Скляр В.В., Тарасюк О.М. Безопасность аэрокосмической техники и надежность компьютерных систем // Авиационно-космическая техника и технология. – 2004. – № 1 (9). – С. 66 – 80.

8. CoVan J. Safety Engineering. – New York: J. Wiley, 1994. – 233 p.

9. King J. Safety in the process industries. – London, Boston: Butterworth-Heinemann, 1990. – 762 p.

10. Vincoli J. Basic guide to system safety. – New York: Van Nostrand Reinhold, 1993. – 194 p.

11. Avizienis A. Fault-tolerance: the survival attribute of digital systems // IEEE Transactions of Computers. – 1978. – V. 66, N 10. – P. 1109 – 1026.

12. Laprie J.-C. Dependability Handbook. LAAS Report n 98-346. – Toulouse: Laboratory for Dependability Engineering, 1998. – 365 p.

13. Leveson N. Safeware: System Safety and Computers. – Addison-Wesley, 1995. – 399 p.

14. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х.: ХВУ, 1996. – 506 с.

15. Ястребенецкий М.А., Иванова Г.М. Надежность автоматизированных систем управления технологическими процессами. – М.: Энергоатомиздат, 1989. – 264 с.

16. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. – Х.: НАКУ «ХАИ», 2004. – 159 с.

17. Карпова Т.С. Базы данных: модели, разработка, реализация. – СПб.: Питер, 2001. – 304 с.

18. Мамедли Э.М., Соболев Н.А. Концепция обеспечения отказоустойчивости СУ и безопасности экипажа «Шаттл» // Зарубежная радиоэлектроника. – 1986. – № 8. – С. 19 – 32; № 9. – С. 21 – 34.

19. Харченко В.С., Скляр В.В., Тарасюк О.М. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций // Радіоелектронні і комп'ютерні системи. – 2003. – № 3. – С. 135 – 149.

Поступила в редакцию 25.10.2005

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко.