УДК 621.039: 004.05

В.И. Дужий

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

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПОДДЕРЖКИ ОЦЕНИВАНИЯ МНОГОВЕРСИОННЫХ СИСТЕМ

Предложена информационная технология поддержки оценивания многоверсионных информационно–управляющих систем, важных для безопасности, позволяющая выполнять оценку таких систем, представленных в виде графовой модели, при помощи метрико-вероятностного метода. Предложенная информационная технология позволяет автоматизировать задачи оценки и выбора многоверсионных проектов путем определения нормированного значения показателя диверсности, который в последующем предлагается использовать для их вероятностной оценки. Предложенная информационная технология может быть использована в полуавтоматическом режиме для решения задач анализа и синтеза в процессе оценки и проектирования многоверсионных систем. Применение данной информационной технологии позволяет оптимизировать применение вносимой в проект диверсности, давая возможность проектировать многоверсионные системы, удовлетворяющие заданным показателям качества.

Ключевые слова: *информационно-управляющие системы, принцип диверсности, архитектурно–технологическая диверсность, показатель диверсности, методика оценки, приоритетный ряд.*

Введение

Информационно-управляющими системами, важными для безопасности (ИУС ВБ), являются системы, функционирование которых не представляет угрозы для окружающей среды, но обеспечивает безопасное функционирование объектов критического применения. По причине потенциальной опасности для окружающей среды и людей таких объектов к их проектированию и эксплуатации предъявляются повышенные требования надежности и функциональной безопасности (ФБ), закрепленные в международных, отраслевых и национальных нормативных документах (IEC 61508:2010, IEC 60880:2006, IAEA NS-G-1.1, НП 306.5.02/3.035: 2000) [1 – 3]. Однако достижение требуемых показателей качества ИУС ВБ затруднено из-за ошибок проектирования и функционирования. Для снижения риска возникновения ошибок при проектировании ИУС ВБ следует соблюдать ряд принципов, основными из которых являются резервирование, принцип диверсности, независимость и др. [1], а спроектированная с соблюдением данных требований система позволяет усилить защиту в глубину (D3) объекта критического применения [4].

Применение резервирования систем позволяет снизить риск возникновения случайных ошибок, возникающих в процессе функционирования аппаратного обеспечения, в то время как внедрение принципа диверсности призвано уменьшить риск появления систематических ошибок, возникших в процессе проектирования и приводящих к отказу по общей причине (ООП) [5]. Реализация принципа резервирования и диверсности позволяет создавать многоканальные многоверсионные системы (МВС), эффективно противостоящие обоим видам ошибок [6]. Однако широкому применению принципа диверсности на практике препятствует ряд нерешенных теоретических и прикладных проблем, основной среди которых является отсутствие эффективной методики оценивания диверсности, позволяющей оценивать и оптимизировать степень диверсности, вносимой в проект, а также определять ее влияние на надежность и ФБ ИУС ВБ. Эффективность применения методики оценивания может быть существенно повышена за счет применения комплекса инструментальных средств поддержки. В общем случае модель представления МВП, методика оценивания, поддержанная инструментальными средствами, составляют информационную технологию оценивания МВП.

Сравнительный анализ некоторых существующих методик оценки МВП рассмотрен в [7].

Постановка задачи. В данной работе предлагается информационная технология оценивания МВП, реализующая методику оценивания, основанную на метрико–вероятностном методе оценки [8] и представлении МВП в виде графовой модели – Graph Model Based Assessment (GMB-A) [9].

Основной раздел

1. Основные положения методики оценивания GMB-A

Методика оценивания GMB–A основана на следующих положениях:

– усовершенствовании известной классификации видов диверсности, представленной в [10, 11], заключающееся в увеличении количества и уточнении видов диверсности, описывающих МВС, что повышает адекватность их представления;

– разделении всех видов диверсности на архитектурные, вносимые в проект разработчиками, и

 © В.И. Дужий

технологические – элементы используемых технологий, выбираемые и используемые в процессе разработки [12];

– представлении технологической диверсности в виде многоуровневой графовой модели (ГМ) – GMB [12], содержащей элементы технологий для каждого вида диверсности; ГМ технологической диверсности может быть представлена в графической или табличной форме; увеличение количества уровней для представления каждого вида диверсности повышает ее чувствительность;

– упорядочении видов диверсности МВП в соответствии со стеком протоколов ИУС ВБ; применение стека протоколов позволяет с единых позиций выполнять оценку МВП, реализованных на различной технологической базе – микропроцессорах, FPGA, аналоговой технике (МП-МП, МП-FPGA, FPGA-FPGA);

– метрической оценке двухверсионной системы при помощи аналитических соотношений, на основании которых определяют значение нормализованного [0,1] показателя диверсности ID (Index Diversity), являющегося метрикой β-фактора, оценивающего технологическую диверсность МВП;

– применении полученной метрики диверсности ID для выполнения последующего вероятностного анализа на основе RBD-диаграмм или при помощи марковских методов для определения показателей надежности и ФБ.

Предложенная методика оценивания GMB-A может быть использована для решения следующих задач:

– анализ существующих (эксплуатируемых) систем, применяемый для их экспертной оценки;

– синтез проектируемых систем, включающий разработку новых и реинжиниринг существующих.

2. Процедуры оценивания и выбора

Процедура оценивания в методике GMB-A включает следующие этапы (рис. 1):

– сбор сведений о существующих технологиях;

– формирование технологического субпрофиля диверсности (ТСПД);

– определение весовых коэффициентов для ТСПД;

– заполнение экспертом опросного листа (check–list), отражающего свойства каждой версии;

– вычисление показателя диверсности ID для каждого вида диверсности при помощи аналитических соотношений;

– вычисление интегральной метрики диверсности МВП μ.

В результате применения процедуры оценки определяют нормированное значение метрики диверсности ID, которое может быть использовано при вероятностном анализе при помощи диаграмм надежности и безопасности (RBD-диаграмм) либо марковских методов (ММ-анализ), с целью определения показателей надежности МВП, основными среди которых является вероятность безотказной работы P и коэффициент готовности K. Эти значения могут быть использованы в процедуре выбора МВП, удовлетворяющего заданным требованиям (рис. 2).

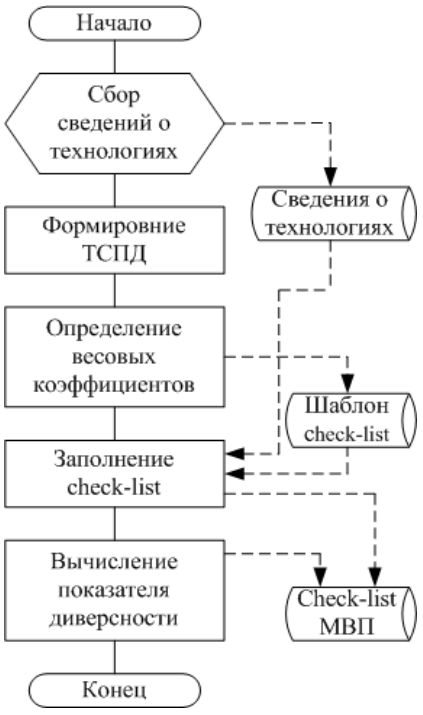

Рис. 1. Методика оценивания GMB-A

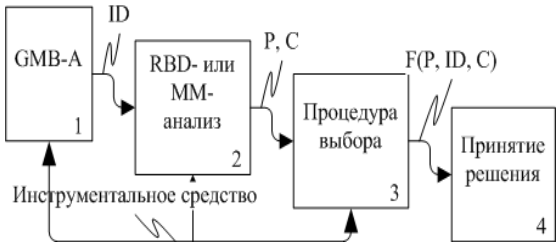

Рис. 2. Связь процедур при выборе видов диверсности

Процедура выбора состоит в решении оптимизационной задачи, цель которой заключается в выборе из исходного множества МВП тех, которые удовлетворяют заданным критериям, с последующим их упорядочением в соответствии с выбранными критериями. Задача выбора МВП математически формулируется следующим образом: задано исходное множество проектов $MP=\{mp_i\}$, имеющие следующие характеристики – показатель диверсности ID_i, вероятность безотказной работы – P_i, стоимость – C_i.

Общая задачи выбора может быть разбита на следующие частные задачи:

– выбрать проект с максимальной ФБ (максимальной диверсностью ID_i) при удовлетворении заданной надежности и минимальной стоимости MP_i, т.е. $P_i > P_{тр}$, $ID_i \rightarrow ID_{max}$, $C_i < C_{тр}$;

– выбрать проект со стоимостью не более заданной при удовлетворении заданной надежности и максимальной ФБ (максимальной диверсностью ID_i), т.е. $P_i > P_{тр}$, $C_i<C_{тр}$, $ID_i \rightarrow ID_{max}$;

– выбрать проект, удовлетворяющий заданной надежности и максимальным значением отношения диверсность/стоимость max (диверсность/стоимость).

Для решения этих задач предлагается использовать *метод приоритетных рядов*, графическое представление которого показано на рис. 3 и 4.

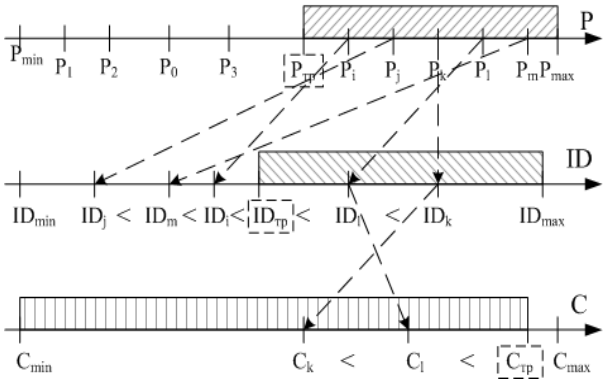

Рис. 3. Решение задачи выбора МВП с максимальной ФБ

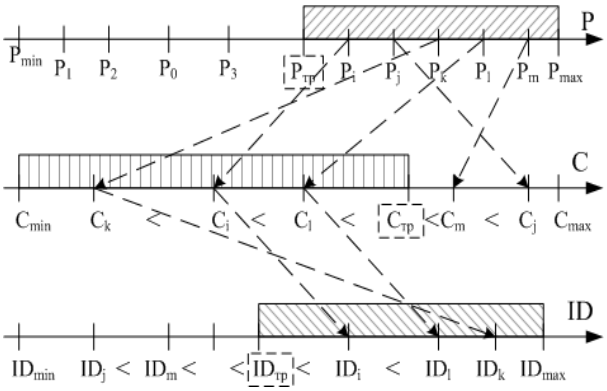

Рис. 4. Решение задачи выбора МВП с требуемой стоимостью и максимальной ФБ

Реализация процедуры выбора при помощи метода приоритетных рядов выполняют в три этапа:

1) все МВП упорядочивают по возрастанию в соответствии со значением первого параметра (показателя надежности P), после чего выбирают те проекты, у которых надежность не менее заданной, $P_i>P_{тр}$;

2) множество МВП, выбранное на этапе 1, упорядочивают по возрастанию в соответствии со значением второго параметра (показателя диверсности ID или стоимости C), после чего выбирают проекты, удовлетворяющие второму условию ($ID_i>ID_{тр}$ или $C_i<C_{тр}$);

3) множество МВП, выбранное на этапе 2, упорядочивают по возрастанию в соответствии со значением третьего параметра (показателя диверсности ID или стоимости C), после чего выбирают проекты, удовлетворяющие третьему условию ($ID_i>ID_{тр}$ или $C_i<C_{тр}$). Из упорядоченного множества выбирают проект с максимальным (ID_{max}) или минимальным (C_{min}) значением третьего параметра.

Следует отметить, что значения, полученные на этапах 2 и 3, могут быть использованы для выбора МВП в соответствии с критерием max(диверсность/стоимость).

Процедура генерации множества версий МВП заключается поиске множества путей из начальных вершин в конечные – поиск по графу в ширину; вершинами графа в ГМ являются элементы технологий, используемые при проектировании МВП, а дуги задают совместимость элементов технологий между собой.

3. Основные элементы информационной технологии оценивания на основе методики GMBA

Применение предложенных процедур – процедуры оценки, выбора и генерации – позволяет решать ряд типовых задач:

– экспертная оценка существующего МВП;

– проектирование нового МВП;

– модернизация существующего одноверсионного проекта.

Учитывая большую размерность исходных данных и связей между технологиями, приводящих к комбинаторному росту множества вариантов МВП, решение приведенных задач существенно осложняется и может быть упрошено за счет применения информационной технологии поддержки, позволяющей решать указанные задачи в полуавтоматическом или автоматическом режиме.

Основной задачей предлагаемой ИТ является оценка и выбор МВП, соответствующих требованиям ФБ, а также разработка инструментальных средств для поддержки процесса такой оценки и выбора, нацеленного на решение типовых задач. Бизнес–процессы решения типовых задач показаны на рис. 5. Из рисунка видно, что типовые процедуры оценки, анализа и выбора (блоки 3, 4, 5) присутствуют в обоих процессах, а в бизнес-процессе проектирования новой МВС дополнительно используются процедуры генерации множества версий и формирования двухверсионного процесса из них (блоки 1, 2 рис. 5, б).

Для поддержки ИТ проектирования и оценивания МВС ИУС ВБ предлагается использовать информационную систему, поддерживающую выполнение основных процедур бизнес–процессов типовых задач (рис. 6).

Каждый бизнес-процесс реализуется одним модулем, при этом полученные данные с выхода одного модуля передаются в другой и сохраняются в базе данных (БД). Последовательное выполнение соответствующих модулей позволяет реализовать бизнес-процессы основных задач. Модуль "Формирование ТСПД" предназначен для создания опросного листа

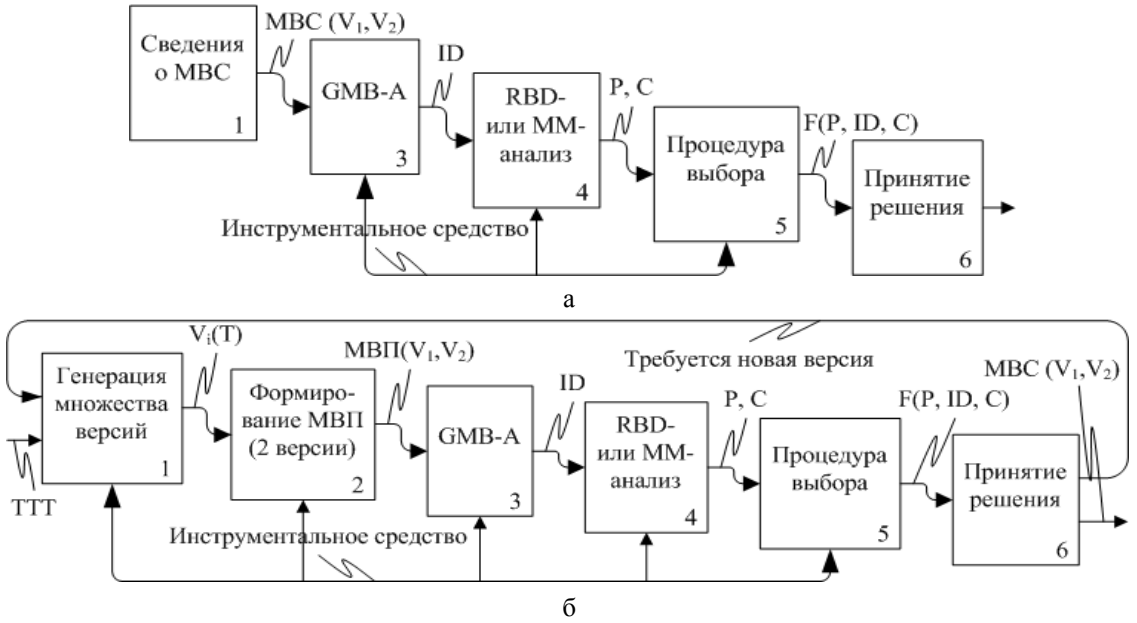

Рис. 5. Бизнес-процессы типовых задач, решаемых при помощи метода GMB-A:
а – оценка существующей МВС, б – проектирование новой МВС

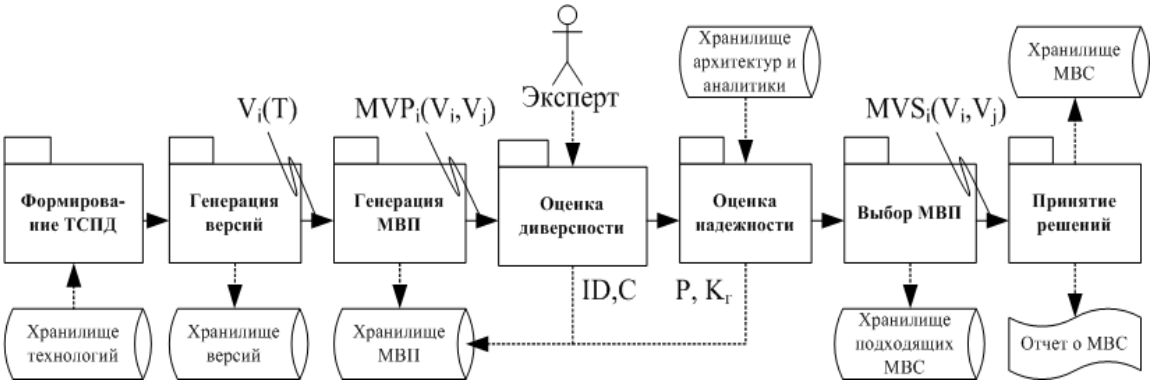

Рис. 6. Информационная система поддержки оценивания и проектирования МВС ИУС ВБ

(chek-list), который будет использован экспертом для фиксации свойств каждой версии МВП. Входными данными для данного модуля являются:

– выбираемый или генерируемый список объединенных и ранжированных видов/подвидов/под–подвидов диверсности, представляющих стек протоколов используемых технологий;

– назначаемые или генерируемые весовые коэффициенты для видов диверсности;

– допустимые связи между элементами технологий, позволяющие уменьшить размерность исходного множества МВП и получить реализуемые на практике проекты.

В результате выполнения данного модуля будет сформирован шаблон многоуровневого опросного листа, в котором свойства конкретного МВП определяются экспертом при выполнении модуля "Оценка диверсности", а его параметры – будут заполнены позднее в результате выполнения последующих модулей.

Модуль "Оценка диверсности" принимает шаблон многоуровневого опросного листа, предоставляет его эксперту для заполнения свойств каждой версии МВП, после чего в автоматическом режиме вычисляется показатель диверсности ID и стоимости C, которые сохраняются для соответствующего проекта в БД.

Модуль "Оценка надежности" вычисляет показатели вероятности безотказной работы P и коэффициент готовности $K_г$, которые также заносятся БД для конкретного МВП. Аналитические соотношения, характерные для данной аппаратной реализации (1oo1, 1oo2, 2oo3 и т.д.), выбираются из соответствующей БД.

Модуль "Выбор МВП" выбирает МВП, удовлетворяющие заданным показателям качества, применяя метод приоритетных рядов, и сохраняет отобранные проекты в БД.

Окончательное принятие решения о соответствии полученных проектов заданным требованиям принимается руководством проектов совместно с экспертами, при этом вся необходимая информация сохраняется в БД и может быть опубликована. Ре-

шением этих задач занимается модуль "Принятие решения".

Рассмотренные модули позволяют выполнять бизнес-процессы, характерные для оценки и выбора имеющегося МВП. Для генерации множества новых проектов необходимы модули "Генерация версий" и "Генерация МВП". Модуль "Генерация версий" выполняет полный перебор элементов технологий с учетом допустимых связей между ними, формируя исходное множество версий $V_i(T)$. Модуль "Генерация МВП" выбирает из исходного множества версий все возможные пары, тем самым формируя исходное множество проектов MVP_i, с которым в дальнейшем работает эксперт.

Приведенная ИТ позволяет автоматизировать процессы оценки и проектирования МВС ИУС ВБ, удовлетворяющих заданным показателям качества и может быть использована на практике для решения задач анализ и синтеза таких систем.

Заключение

Рассмотрена ИТ поддержки методики оценивания МВП GMB-A. Данная методика является более адекватной и чувствительной по сравнению с известными.

Предложена ИТ, позволяющая в полуавтоматическом режиме определять нормированный показатель диверсности МВП, который далее может быть использован для определения показателя надежности и ФБ.

Предложенная ИТ поддержки оценивания МВП позволяет расширить исходное множество вариантов для оценивания и ускорить процесс их оценивания, что позволяет оптимизировать разработку и экспертную оценку МВП с целью оптимизации применения внесенной диверсности в соответствии с заданными критериями качества.

Данная ИТ оценивания МВП может быть использована на этапе проектирования и экспертной оценки ИУС ВБ, позволяя получить более адекватную и чувствительную оценку вносимой в проект диверсности.

Список литературы

1. IEC 61508-1 Ed.2.0:2010. Functional safety of electrical/electronic/ programmable electronic safete-related system – Part 1: General requirements [Текст]. – Vienna: International Electrotechnical Commission, 2010. – 61 p.

2. IEC 60880-2:2000. Software for computers important to safety for nuclear power plants - Part 2: Software aspects of defense against common cause failures, use of software tools and of pre-developed software [Текст]. – Vienna: International Electrotechnical Commission, 2000. – 79 p.

3. НП 306.5.02/3.035-2000. Требования по ядерной и радиационной безопасности к информационным и управляющим системам, важным для безопасности атомных станций [Текст]. Введ. 2000-03-28. – К.: Гос. администрация ядерного регулирования Украины, 2000.

4. Jonson, G. The INSAG Defense in Depth Concept and D-in-D&D in I&C [Текст] / G. Jonson // Proceedings of 7th ANS Topical Meeting on NPIC-HMIT, Las Vegas, USA, November, 2010.

5. Hokstad, P. Common Cause Failure Modeling: Status and Trends [Текст] / P. Hokstad, M. Rausand // Misra, K.B. (ed.). Handbook of Performability Engineering. – Springer, 2008.

6. Siora, A. Research and Production Corporation RADIY: History, Results and Development Vectors [Текст] / A. Siora, V. Sklyar // Critical Infrastructure Safety and Security First International Workshop (CrlSS–DESSERT), Kharkiv, Ukraine, 2011. – V. 1, P. 67-72.

7. Kharchenko, V. Comparative analysis of diversity assessment techniques for Multi-version NPP I&C Systems [Текст] / V. Kharchenko, A. Volkoviy, V. Sklyar, V. Duzhyi // Proceedings of the 21th International Conference on Nuclear Engineering, Chengdu, China, July 29-August 2, 2013. – CD-ROM, pub. ICONE19-16367.

8. Kharchenko, V. Metric-Probabilistic Assessment of Multi-Version Systems: Some Models and Techniques [Текст] / V. Kharchenko, A. Volkoviy, A. Siora, V. Duzhyi // Zamojski, W. et. al. (eds). Dependable Computer Systems: Advances in Intelligent and Soft Computing. – Springer, Volume 97/2011, 2011. – P. 87-100.

9. Kharchenko, V. Diversity Assessment of Multi-Version NPP I&C Systems: NUREG7007 and CLB-BASED Techniques [Текст] / V. Kharchenko, V. Duzhyi, V. Sklyar, A. Volkoviy // Proceedings of the IEEE East-West Design & Test Symposium (EWDTS), Rostov-on-Don, Russia, September 27-30, 2013. – CD-ROM, pap. 114.

10. Wood, R. Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems [Текст] / R. Wood, R. Belles, M. Cetiner et.al. // NUREG/CR-7007, ORNL/TM-2009/302. – NRC Job Code N6176, 2009. – 225 p.

11. U.S. Nuclear Regulatory Commission. Method for Performing Diversity and Defense-in-Depth. Analyses of Reactor Protection Systems [Текст]. NUREG/CR-6303, Washington, D.C., December, 1994 (UCRL-ID-119239).

12. Дужий, В.И. Концептуальная модель ИУС с архитектурно-технологической диверсностью [Текст] / В.І. Дужий, В.С. Харченко // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Випуск 87. "Проблеми енергозабезпечення та енергозбереження в АПК України". – Х.: ХНТУСГ, 2009. – С. 128-131.

Поступила в редколлегию 8.11.2013

Рецензент: д-р техн. наук, проф. В.С. Харченко, Харьковский национальный аэрокосмический университет "ХАИ", Харьков.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТРИМКИ ОЦІНЮВАННЯ БАГАТОВЕРСІЙНИХ СИСТЕМ

В.І. Дужий

Запропоновано інформаційну технологію підтримки оцінювання багатоверсійних інформаційно-управляючих систем важливих для безпеки, що дозволяє виконувати оцінку таких систем, представлених у вигляді графовой моделі, за допомогою метрико-імовірнісного методу. Запропонована інформаційна технологія дозволяє автоматизувати процес оцінки і вибору багатоверсійних проектів шляхом визначення нормованого значення показника диверсності, який у подальшому пропонується використовувати для їх імовірнісної оцінки. Запропонована інформаційна технологія може бути

використана в напівавтоматичному режимі для вирішення завдань аналізу і синтезу в процесі оцінки і проектування багатоверсійних систем. Застосування даної інформаційної технології дозволяє оптимізувати внесення в проект диверсності, що дозволяє проектувати багатоверсійні системи, які задовольняють заданим показникам якості.

Ключові слова: *інформаційно-управляючи системи, принцип диверсности, архітектурно-технологічна диверсність, показник диверсності, методика оцінювання, пріоритетний ряд.*

INFORMATION TECHNOLOGY TO SUPPORT OF MULTI-VERSION SYSTEMS ASSESSMENT

V.I. Duzhyi

A proposed information technology facilitates assessment of multi-version control systems in safety-critical domains. It provides a quality evaluation applying a special metric-based probabilistic method to the graph model of a system. The proposed technology allows effective automation of the assessment process and helps to select multi-version projects based on calculated normalized diversity indicators. Those indicators can be further used for the probabilistic phase of the assessment. This technology can be also used in a half-automated mode to perform analysis and synthesis during design of multi-version systems. Using this technology optimizes the diversity injection into the project that helps to design multi-version systems with stated quality requirements.

Keywords: *information control systems, a diversity technique, design- and technology-aimed diversity, diversity indicator, assessment technique, prioritization.*