УДК 621.3.019.3

А.В. ФЕДУХИН[*], Ар.А. МУХА[*], Н.В. СЕСПЕДЕС ГАРСИЯ[*]

ДОКАЗАТЕЛЬСТВО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

[*]Институт проблем математических машин и систем НАН Украины, Киев, Украина

Анотація. *Стаття присвячена питанням безпеки комп'ютерних систем критичного застосування. Розглянуто способи доказу функціональної безпеки, наводяться необхідні поняття і визначення.*
Ключові слова: *функціональна безпека, програма забезпечення безпеки комп'ютерних систем.*

Аннотация. *Статья посвящена вопросам безопасности компьютерных систем критического применения. Рассмотрены способы доказательства функциональной безопасности, приводятся необходимые понятия и определения.*
Ключевые слова: *функциональная безопасность, программа обеспечения безопасности компьютерных систем.*

Abstract. *The article is devoted to the security questions of computer systems of critical applications. The methods of functional safety proof were considered, the necessary concepts and definitions are given.*
Keywords: *functional safety, security assurance program of computer systems.*

1. Введение

Требования гарантоспособности предъявляются прежде всего к компьютерным системам критического применения, для которых требование безопасности приобретает наиболее важное значение. Безопасность в обычном понимании этого слова трактуется как сохранность человека, объекта, груза, окружающей среды. Однако в технике этому термину придается и более широкое понятие [1]. Например, под «безопасной компьютерной системой» подразумевается не только наличие ее собственной безопасности как технического объекта, но и наличие безопасности результатов ее работы (расчетов, управляющих команд, информации и т.д.). В зависимости от отрасли применения компьютерных систем (КС) понятие безопасности конкретизируется в соответствии с конкретными ее задачами и особенностями. На сегодняшний день трудно найти область человеческой деятельности, где бы не требовались КС высокой надежности и безопасности [2].

Безопасность КС критического применения можно разделить на внешнюю и внутреннюю. Внешняя безопасность связана с сохранностью компьютерной системы как технического объекта и может нарушаться из-за внешних причин (разрушающего влияния окружающей среды или действий человека). Внутренняя безопасность – это свойство объекта не являться источником опасности по отношению к внешним объектам (человеку, окружающей среде). Внутренняя безопасность рассматривается как составляющая надежности и безопасности в связи с тем, что отказы элементов КС, которые нарушают безопасность, одновременно приводят к нарушению надежности.

Функциональная безопасность (ФБ) (functional safety) – основная часть общей безопасности КС, обеспечивающая отсутствие неприемлемого уровня риска как функционированию самой системы, так и здоровью людей, их собственности или окружающей среде. ФБ является очень важным атрибутом для систем критического использования, связанных с безопасностью людей и окружающей среды обитания человека (системы энергетики, хи-

ISSN 1028-9763. Математичні машини і системи, 2016, № 3

мической промышленности, транспорта и т.д.). Целью управления ФБ является минимизация неприемлемого уровня риска нанесения вреда здоровью людей (непосредственно или косвенно – через нанесение ущерба собственности или окружающей среде). Цель обеспечения ФБ считается достигнутой, когда каждая функция обеспечения ФБ системы осуществляется эффективно и обеспечивает выполнение требуемых показателей.

В работе предлагается методология доказательства безопасности КС критического применения, базирующаяся на методологии доказательства безопасности электронных систем железнодорожной автоматики, разработанной коллективом ученых Петербургского государственного университета путей сообщения (ПГУПС) под руководством профессоров Сапожникова В.А. и Сапожникова Вл.А. [3].

2. Основные способы доказательства функциональной безопасности

Можно выделить следующие основные способы доказательства ФБ КС:

- экспертный – на основе экспертизы технической и конструкторской документации;
- расчетный – на основе аналитических расчетов;
- имитационный – эксперименты с машинными моделями;
- экспериментальный испытательный – экспериментальные испытания с опытной системой (лабораторные испытания);
- натурный испытательный – испытания системы в полевых условиях на стадии пусконаладочных работ и периода приработки системы, сертификационные испытания;
- информационный – сбор статистических данных об отказах в процессе длительной эксплуатации одной системы или некоторого числа однотипных систем.

Данные способы перечислены в порядке последовательного их применения и в то же время они расположены в порядке возрастания достоверности оценки ФБ. Экспертные и расчетные методы проводятся на основании утвержденных методик и аналитических моделей, касающихся методологии построения безопасных КС в соответствующих областях их применения. Различные виды испытаний на безопасность проводятся на основании утвержденных программ и методик испытаний.

3. Экспертные методы

Эти методы применяются на начальных этапах разработки КС – при разработке технических предложений, технического задания, при эскизном проектировании.

Независимые эксперты должны оценить концепцию ФБ, принятую разработчиками данной КС, критерии опасных отказов, требования и показатели ФБ, предлагаемые технические решения. Эксперты проверяют технические решения на соответствие утвержденным правилам построения безопасных схем с учетом возможных отказов. Объективность экспертизы определяется личным опытом экспертов, их знаниями в соответствующей области техники.

Основные задачи, которые должны решать эксперты на различных стадиях разработки и проектирования КС, следующие:

- оценка концепции безопасности на стадии технических предложений;
- оценка принятых норм и требований ФБ на стадии технического задания;
- оценка уровня ФБ выбранного варианта системы на стадии эскизного проектирования;
- оценка принятых технических решений и списка опасных отказов на стадии технического проекта;
- оценка достигнутого проектного уровня ФБ на стадии рабочего проекта.

4. Расчетные методы

Расчетные методы используются разработчиками КС для обоснования предполагаемого уровня ФБ при техническом и рабочем проектировании (проектная оценка ФБ). При этом точность расчетов, степень их детализации могут быть различными на разных этапах разработки КС.

Результаты проектной оценки ФБ КС необходимы для выбора того или иного вида резервированной структуры и обоснования мероприятий по диагностированию программных и технических средств (определение необходимых требований по полноте и глубине контроля).

На этапе технических предложений выполняется предварительный расчет ФБ. При этом используется метод, который учитывает только отказы основной и резервной аппаратуры. Контрольные устройства предполагаются абсолютно надежными, поскольку они еще не разработаны. Не учитываются также процессы восстановления и ошибки проектирования и изготовления. Таким образом, предварительный расчет оценивает ФБ выбранной структуры КС в сравнении с ФБ других возможных структур. Полученные при этом значения показателей ФБ можно предварительно считать верхними оценками. Реальные оценки, с одной стороны, уменьшаются при учете указанных отказов и ошибок, но, с другой стороны, увеличиваются при учете процесса восстановления. При этом рассматриваются достаточно простые структурные схемы КС.

На этапе технического задания и эскизного проектирования уточняется ФБ выбранного варианта построения КС. В этом случае учитываются отказы внешних контрольных устройств. Эти устройства обычно выполняются в виде элементов с несимметричными отказами или самопроверяемых элементов, на которые возлагается основная задача по обеспечению ФБ.

Учет процесса восстановления и реальных условий и режимов эксплуатации целесообразно осуществлять на этапе технического проекта, когда будут определены основные эксплуатационные свойства КС и режимы ее обслуживания. В этом случае при уточненном расчете ФБ используют вероятностно-физические методы исследования безопасности и надежности систем [4].

Если появляются данные по ошибкам проектирования и изготовления (в результате эксплуатационных испытаний нескольких систем), то выполняют наиболее точный окончательный расчет ФБ.

Расчетные методы оценки ФБ, как правило, опираются на расчетные методы оценки надежности систем – предварительный, уточненный и окончательный расчеты надежности [5]. В дальнейшем после имитационных и испытательных методов (экспериментальных и натурных) исследования надежности системы и при наличии ограниченной статистики отказов расчет надежности уточняют [6].

5. Имитационные методы

Экспертные и расчетные методы оценки ФБ не могут претендовать на высокую достоверность, если не будут подкреплены данными, полученными при испытаниях разрабатываемой КС. Первым этапом таких испытаний являются испытания машинных моделей КС (машинное моделирование системы). При этом сама КС еще может быть не создана, но должны быть выбраны технические средства, методы контроля и разработано алгоритмическое и программное обеспечение.

Машинное моделирование (виртуальные испытания) КС по сравнению с другими видами испытаний позволяет:

- обеспечивать ускоренные оценки характеристик системы в машинном времени;
- создать во время моделирования все множество возможных технологических

ситуаций;

• имитировать большое число отказов аппаратных и программных средств, что не осуществимо при физических испытаниях системы;

• организовать процедуры верификации программного обеспечения;

• корректировать списки опасных отказов.

Можно выделить следующие виды машинного моделирования систем. Исследование технологических алгоритмов на безопасность – проверка выполнения всех условий ФБ в данном технологическом процессе путем создания всевозможных штатных и нештатных (но вероятных) технологических ситуаций. Реакция системы на эти ситуации сравнивается с эталонной реакцией. Данное моделирование является одновременно и тестированием программного обеспечения.

Исследование работы безопасных схем контроля – проверка безопасности внешних схем контроля (схем сравнения, мажоритарных схем, фиксаторов ошибок, тестеров и др.). Эти схемы несут основную ответственность за ФБ системы, и поэтому данное моделирование является наиболее важным. В процессе моделирования проводятся три вида экспериментов:

• искажение входных сигналов (амплитуда, фаза, длительность, частота и т.п.);

• внесение отказов из заданного списка и определение реакции схемы на эти отказы;

• анализ работы схем при разбросе временных параметров элементов (проверка отсутствия явления состязаний в цифровых схемах).

Доказательство отсутствия опасных отказов в этих экспериментах возможно прямым методом перечисления анализируемых ситуаций.

Моделирование отказов и сбоев программно-технического комплекса (ПТК) – наиболее сложный вид моделирования, выполняется с помощью специальной имитационной машинной модели ПТК с внесением отказов и сбоев при выполнении прикладных программ. Этот вид моделирования позволяет оценить выбранную концепцию безопасности. Моделирование работы прикладного программного обеспечения (ППО) проводится, если ППО обладает специальными свойствами по обнаружению или маскировке ошибок, например, самопроверяемые и диверситетные программы. При проведении моделирования системных функций проверяется безопасность КС при выполнении таких системных функций, как рестарт, необратимость перехода в защитное состояние, реконфигурация структуры, восстановление вычислительного процесса и т.п.

Важным направлением имитационных методов оценки ФБ КС являются методы моделирования надежности систем. Данные методы позволяют на этапах проектирования системы выбрать наиболее надежный вариант исполнения, удовлетворяющий всем требованиям нормативных документов [7–10].

6. Экспериментальные испытательные методы

После разработки КС и создания опытного образца выполняют его экспериментальные испытания в лабораторных условиях. Цель испытаний – проверка безопасности функционирования всех составных элементов КС в комплексе и взаимодействии.

Лабораторные испытания (ЛИ) проводятся с помощью генератора входных технологических ситуаций и имитаторов объектов управления и контроля по специальным программам.

Длительность ЛИ колеблется, обычно, от одного месяца до года. Это позволяет собрать определенные статистические данные об отказах и сбоях. Эти данные могут быть использованы для уточнения аналитических расчетов безопасности. ЛИ проводятся с учетом влияния колебания питающего напряжения, электромагнитных, климатических и механических воздействий, возможных в условиях эксплуатации, на безопас-

ность опытного образца.

В рамках проведения ЛИ проводятся контрольные и определительные испытания на надежность, наиболее эффективными среди которых являются ускоренные испытания в форсированных режимах [11–14].

7. Натурные испытательные методы

После успешного завершения ЛИ КС устанавливается на объекте, где выполняются ее испытания в реальных полевых условиях – натурные испытания. Если при этом на объекте имеется старая система, то целесообразно включить новую КС параллельно со старой. Сравнение работы двух систем позволяет гарантированно зафиксировать случаи возникновения опасных отказов.

КС испытывают в течение одного – двух лет (в зависимости от сложности системы и уровня требований безопасности к ней), после чего проводятся сертификационные испытания. На КС выдается сертификат функциональной безопасности, система может быть рекомендована для применения. С этого начинается постоянная ее эксплуатация.

8. Информационные методы

В процессе постоянной эксплуатации продолжаются мероприятия по обеспечению ФБ КС в соответствии с программой обеспечения безопасности (ПОБ). Важным мероприятием является сбор статистических данных об отказах системы, включая опасные отказы. Поскольку опасные отказы редки, то сбор статистических данных возможен только при длительной эксплуатации одной КС или при определенном времени эксплуатации нескольких экземпляров системы. Полученные при этом данные наиболее объективно характеризуют ФБ КС. Они могут быть использованы для окончательных расчетов показателей ФБ [15].

9. Программа обеспечения безопасности

В современных инновационных проектах КС уделяется большое внимание последовательному выполнению требований к безопасности на всех этапах их разработки: от постановки задачи до приемки их в эксплуатацию.

Основанием для внедрения разработанной КС является одобрение ее приемочной комиссией. Основное правило приемки заключается в полной содержательной проверке КС путем контроля третьей стороной, независимой от разработчика и продавца. Для успешного выполнения задачи обеспечения безопасности КС независимый контролер курирует вопросы, связанные с безопасностью на всех стадиях создания КС.

Наряду с техническим заданием (ТЗ), ПОБ КС является одним из основных документов, используемых при доказательстве безопасности КС. Такая программа должна представлять собой составную часть программы обеспечения гарантоспособности КС (ПОГ) и являться необходимым документом для сертификации безопасности КС [16, 17].

Актуальность создания ПОБ состоит в том, что свойства КС обеспечивать безопасность закладываются при разработке, изготовлении и эксплуатации. Поэтому для обеспечения безопасности необходимо учесть в ПОБ все этапы жизненного цикла системы. Каждый из этапов создания КС должен заканчиваться отчетом о выполнении соответствующей части ПОБ.

В ПОБ должны быть отражены основные методы решения задач обеспечения безопасности, а именно:

- структурные и конструктивные решения;
- методы реализации стратегии отказобезопасности;

• способы выведения системы из внештатных ситуаций (состояния защитного и опасного отказов и т.д.).

ПОБ должна представлять собой совокупность организационных, конструкторских, технологических и методических мероприятий, охватывающих все этапы жизненного цикла КС и распространяющихся на все технические средства, влияющие на безопасность функционирования системы (средства прогнозирования, обнаружения и распознавания опасных отказов, оповещение о них обслуживающего персонала и т. п.). В ней следует предусмотреть определение требований по безопасности к КС в целом и к ее составным частям.

ПОБ должна предусматривать расчеты, моделирование и всесторонние испытания КС и ее элементов, а также определять состав, последовательность, организацию, методические основы, содержание и этапы выполнения мероприятий, обеспечивающих заданный уровень безопасности системы и проводимых на всех стадиях жизненного цикла КС.

ПОБ должна включать в себя следующие данные и материалы:

• список нормативно-технических и методических документов, в соответствии с которыми разработана ПОБ и которые подлежат использованию в процессе реализации программы;

• состав и основные функциональные, информационные и эксплуатационные характеристики системы (при необходимости даются характеристики подсистем КС), которые являются определяющими для безопасности функционирования, а также анализ поведения КС в работоспособном состоянии и в состояниях защитного и опасного отказов, характеристика предполагаемых условий эксплуатации;

• количественные и качественные показатели ФБ КС, заданные в ТЗ и нормируемые действующими нормативно-техническими документами, методы получения проектной оценки ФБ и надежности, исходные условия при которых должны определяться и подтверждаться показатели безопасности;

• основную концепцию, методы и средства обеспечения ФБ КС в целом и ее составных частей, общую модель безопасного функционирования системы;

• мероприятия по обеспечению ФБ, проводимые на всех этапах разработки, серийного производства и эксплуатации КС, и сроки их проведения;

• отчетные материалы о результатах выполнения каждого мероприятия, список исполнителей и сроки их выполнения;

• основания для корректировки программы, исполнителей корректировки и сроки ее проведения, а также порядок обмена информацией об этом между заинтересованными сторонами.

ПОБ может быть оформлена в виде отдельного документа, увязанного с ПОГ и программой обеспечения надежности КС (ПОН) и программами испытаний или в виде составной части ПОГ.

ПОБ должна разрабатывать независимая организация, аттестованная на проведение работ по безопасности КС совместно с разработчиком, изготовителем и заказчиком системы соответственно этапу ее жизненного цикла. ПОБ является одним из основных документов, используемых при сертификации безопасности КС. Разработка и выполнение такой программы обеспечивает необходимый уровень безопасности вновь создаваемых КС. Отчетным документом о результатах выполнения программы на этапе разработки является документ «Доказательство безопасности».

Документ «Доказательство безопасности» должен содержать следующие разделы:

• вводные замечания;

• нормативные документы, используемые для доказательства безопасности;

• характеристику объекта;

• доказательство работоспособности;
• методы доказательства безопасности;
• реальные ограничения;
• программу и методику испытаний;
• характеристику испытательной аппаратуры;
• подтверждение безопасности, результаты испытаний и экспертизы;
• заключение по безопасности;
• список использованной литературы.

В разделе «Методы доказательства безопасности» приводятся перечень методов доказательства ФБ и цели использования применяемых методов доказательства ФБ. Применяемые методы используются для доказательства:

• выполнения концепции безопасности разработанной КС;
• выполнения количественных и качественных требований ФБ, установленных в нормативной документации;
• перехода КС в защитное состояние при появлении отказов или сбоев;
• независимости отказов в структурно-резервированных каналах;
• полноты диагностирования заданного класса отказов с заданной достоверностью (отсутствие накопления отказов);
• обеспечения необратимого защитного (выключенного) состояния отказавших (неисправных) элементов, блоков или каналов КС;
• требуемой эффективности программных и аппаратных средств контроля;
• защищенности от опасных отказов КС при неисправности источников питания, отказах программного обеспечения, отказах и сбоях входных и выходных элементов, перенапряжениях, влиянии климатических и механических факторов.

В разделе «Реальные ограничения» определяются границы применения каждого из используемых методов доказательства безопасности, например, допущения при расчете показателей безопасности, учитываемый класс повреждений, полнота и достоверность испытаний.

В разделе «Подтверждение безопасности, результаты испытаний и экспертизы» приводятся протоколы и акты различных видов испытаний и экспертные заключения. В этом разделе требуется доказать, что соблюдается основной принцип безопасности – одиночный отказ не должен приводить КС в опасное состояние. Это доказательство осуществляется на основании перечня отказов, возможных в данном типе аппаратуры.

После первого отказа может возникнуть второй, третий и т.д. В зависимости от концепции обеспечения безопасности безопасная реакция системы в целом может обеспечиваться даже в случае отказа двух или более конструктивных элементов.

В микроэлектронных системах, как правило, используют концепцию быстрого обнаружения за допустимый интервал времени отдельного отказа. Возникновение двух и более отказов за рассматриваемый интервал времени должно иметь вероятность не выше установленной в нормативной документации для конкретного типа аппаратуры. Вероятность такого события определяется на основании расчетов или моделирования.

При анализе влияния на КС одиночных отказов важными факторами для безопасности являются независимость отказов и сбоев. Если это требование нарушается, то необходимо считаться с множественными отказами и сбоями, которые не обнаруживаются средствами контроля (тестовыми программами, компараторами, контрольными схемами и т.п.).

Для обеспечения независимости отказов каналы обработки информации проектируются независимыми разработчиками (диверситетное проектирование), питаются от разных источников напряжения, используют элементы гальванической развязки. Для обеспечения независимости отказов при вводе информации и при обмене информацией между каналами часто используют информационную избыточность (обнаруживающие коды). КС

должна быть защищена от возникновения одинаковых сбоев при воздействии электромагнитных помех. Для этого используют различные фильтры, элементы гальванической развязки, различные конструктивные решения, обеспечивающие независимость сбоев в каналах обработки информации.

В разделе «Подтверждение безопасности, результаты испытаний и экспертизы» также должно быть подтверждено, каким образом и благодаря чему обеспечивается безопасное состояние КС при возникновении отказов, изменении параметров элементов в допустимых пределах, воздействии электромагнитных помех, климатических и механических факторов. В разделе отражаются требования по эксплуатации, относящиеся к обеспечению ФБ.

Доказательство ФБ сложной КС может быть подразделено на доказательства безопасности ее отдельных подсистем. Структура доказательства ФБ должна повторяться для каждой из подсистем, при этом электрические и информационные связи отдельных подсистем дополнительно должны быть проанализированы на безопасность.

10. Заключение

Доказательство ФБ проходит экспертизу в независимых испытательных лабораториях. При положительных результатах экспертизы разработчику выдается заключение (свидетельство) о безопасности КС. После выдачи заключения доказательство ФБ не может быть изменено. Изменения, которые в дальнейшем вносятся в КС и могут влиять на ее ФБ, должны сопровождаться новым доказательством ФБ.

Доказательство ФБ содержит оценку адекватности испытаний условиям эксплуатации, которая зависит от реальных ограничений (класс рассматриваемых отказов, время испытаний, точность измерений и т.д.).

В доказательстве ФБ отдельных частей КС допускается делать ссылки на известные доказательства ФБ при условии полной идентичности части устройства и ее связей этому доказательству.

Доказательство ФБ хранится у разработчиков и в испытательной лаборатории, выдававшей заключение о ФБ КС. Срок хранения документов, подтверждающих ФБ системы, устанавливается соответствующими нормативными документами на КС.

СПИСОК ЛИТЕРАТУРЫ

1. Новая техника и проблема безопасности человека / Е.Е. Ковалев, В.И. Иванов, Б.Я. Пахомов [и др.] // Вопросы философии. – 1981. – № 5. – С. 49 – 59.
2. Федухин А.В. Гарантоспособность компьютерных систем – мода или объективная необходимость / А.В. Федухин, Б.Г. Мудла // Математичні машини і системи. – 2014. – № 4. – С. 179 – 188.
3. ОСТ 32.41–95. Безопасность железнодорожной автоматики и телемеханики. Методы доказательства безопасности систем и устройств железнодорожной автоматики и телемеханики. – СПб.: ПИИТ, 1995. – 95 с.
4. Стрельников В.П. Оценка и прогнозирование надёжности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – К.: Логос, 2002. – 486 с.
5. Федухин А.В. Уточненный расчет надежности электронных устройств на основе *DN*-распределения / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2000. – № 2, 3. – С. 170 – 175.
6. Федухин А.В. Графо-аналитический метод оценки параметров *DN*-распределения в условиях малой статистики отказов / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2012. – № 2. – С. 161 – 167.
7. Федухин А.В. К вопросу о статистическом моделировании надежности / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2006. – № 1. – С. 156 – 163.
8. Федухин А.В. Имитационное моделирование отказоустойчивой резервированной двухканальной системы в интегрированной инструментальной среде Matlab Simulink / А.В. Федухин, Ар.А. Муха // Математичні машини і системи. – 2011. – № 2. – С. 178 – 181.

9. Федухин А.В. Моделирование надежности систем средствами пакета программ RELIABmod / А.В. Федухин, В.П. Пасько // Математичні машини і системи. – 2011. – № 4. – С. 176 – 182.
10. Федухин А.В. Моделирование надежности систем / А.В. Федухин, В.П. Пасько // Методы менеджмента качества. – 2012. – № 3. – С. 50 – 55.
11. Федухин А.В. Методы ускоренной оценки надежности СВТ. Классификация, основные понятия и определения / А.В. Федухин // Математичні машини і системи. – 2001. – № 1, 2. – С. 194 – 204.
12. Федухин А.В. К вопросу ускоренной оценки надежности технических средств информатики по результатам форсированных испытаний / А.В. Федухин // Управляющие системы и машины. – 2003. – № 1. – С. 18 – 24.
13. Федухин А.В. Контрольные испытания СВТ на надежность в форсированных режимах / А.В. Федухин // Математичні машини і системи. – 2002. – № 1. – С. 134 – 140.
14. Федухин А.В. Ускоренные определительные испытания в форсированных режимах / А.В. Федухин // Математичні машини і системи. – 2002. – № 3. – С. 148 – 154.
15. Сапожников В.В. Безопасность железнодорожной автоматики и телемеханики. Статистические данные, экспертные оценки и нормы безопасности / В.В. Сапожников, Вл.В. Сапожников, Л.В. Гавзов // Автоматика, телемеханика и связь. – 1993. – № 10. – С. 17 – 19.
16. ОСТ 32.19–92. Безопасность железнодорожной автоматики и телемеханики. Общие требования к программам обеспечения безопасности. – СПб.: ПИИТ, 1992. – 15 с.
17. Федухин А.В. Пакет прикладних программ GARANTmod в инжиниринге гарантоспособных систем / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2013. – № 3. – С. 178 – 185.

Стаття надійшла до редакції 07.07.2016