4 КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3

НАДЕЖНОСТЬ РЕЗЕРВИРОВАННОГО ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА ПРИ ОГРАНИЧЕННОМ ВОССТАНОВЛЕНИИ

В.А. Богатырев, С.М. Алексанков, Д.В. Демидов, В.Ф. Беззубов

Предложены марковские модели надежности дублированных вычислительных комплексов, позволяющие учесть влияние на нестационарный коэффициент готовности ограниченных возможностей восстановления, вызванных недопустимостью потери данных и прерываний вычислительного процесса во время восстановления.

Ключевые слова: надежность, отказоустойчивость, доступность, дублированный вычислительный комплекс, резервирование, нестационарный коэффициент готовности.

Введение

Высокая надежность, отказоустойчивость и безопасность систем критического применения, в частности, функционирующих в реальном времени, реализуется за счет резервировании основных подсистем, в том числе средств хранения, обработки и передачи данных.

Безопасность систем критического применения достигается при минимизации возможностей возникновения опасных отказов и последствий от их возникновения. Функциональная безопасность систем связана с минимизацией частоты и последствий отказов в выполнении отдельных функций системы, в том числе связанных с безопасностью [1, 2]. Обеспечение функциональной безопасности в значительной мере определяется информационной безопасностью и, прежде всего, связано с минимизацией риска потери данных (в том числе формируемых в ходе вычислительного процесса) при отказах системы, вызванных внешними или внутренними причинами, в том числе в результате злонамеренных воздействий.

В системах критического применения используемые вычислительные узлы, как правило, строятся на основе дублированных или троированных вычислительных комплексов. Возможности сохранения данных после отказов дублированных вычислительных комплексов (ДВК) во многом определяются организацией средств комплексирования и доступа к памяти.

Для достижения высокой отказоустойчивости, функциональной и информационной безопасности при сохранении устойчивости вычислительного процесса средства комплексирования ДВК должны обеспечивать доступность информационных ресурсов (памяти) обоих полукомплексов, даже при отказах процессоров одного из них, тем самым сохраняя возможности функционирования (или данных) в режиме деградации. Формирование работоспособной структуры в ряде случаев требует реконфигурации с целью использования в вычислительном процессе сохраненных ресурсов обоих полукомплексов. В настоящее время достаточно хорошо исследованы модели надежности дублированных систем [3–5], в том числе восстанавливаемых дублированных систем при различных дисциплинах ограниченного восстановления, под которым понимается восстановление при образовании очереди на восстановление отказавших узлов.

Потенциал обеспечения надежности управляющих вычислительных систем во многом определяется особенностями прикладных процессов, в ряде случаев ограничивающих возможности восстановления системы после отказов.

В связи с высоким вниманием к анализу безопасности и функциональной надежности систем критического применения, в том числе систем, критичных к нарушениям доступности и целостности информационных ресурсов, представляется актуальным исследование их надежности. Модели надежности таких систем должны учитывать срывы вычислительного процесса и (или) потерю стратегически важной информации, потенциально приводящие к катастрофическим последствиям, после которых восстановление вычислительной системы теряет смысл. Модели надежности указанного класса систем, помимо оценки традиционных показателей надежности, должны находить вероятности опасных состояний, при которых возможны срыв критичных вычислительных (управляющих) процессов и невосполнимая потеря критически важных данных.

В работе предложены марковские модели надежности восстанавливаемых ДВК, отличающиеся возможностью учета ограниченного восстановления, при невосполнимой потере накопленных данных (результатов вычислений) или при недопустимости прерываний вычислительного (управляющего) процесса во время процесса восстановления системы.

Задачи исследования

В работе решается задача оценки надежности ДВК с учетом ограниченного восстановления после отказов. Типовая структура дублированного вычислительного комплекса, представленная на рис. 1, состоит из двух полукомплексов, каждый из которых содержит процессор (ЦП) и память (М). Доступ ЦП к

ресурсам сопряженного полукомплекса обеспечивается средствами комплексирования (адаптером сопряжения – АС) [6–7].

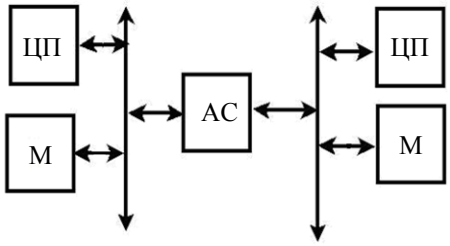

Рис. 1. Структура дублированного вычислительного комплекса

Средства комплексирования должны обеспечивать доступ к памяти сопряженного полукомплекса с целью сохранения информационных ресурсов (результатов решения прикладных задач) даже при отказах одного из дублированных ЦП. Таким образом, для информационно безопасного, отказоустойчивого функционирования комплекса АС должен обеспечивать прямой доступ к памяти двух полукомплексов.

Надежность ДВК в определенной мере зависит от ограничений восстановления системы после отказов, определяемых особенностями прикладных процессов [8, 9].

Рассмотрим ограничения восстановления комплекса. Оно нереализуемо в случаях, когда:

- потеря данных недопустима, а перерывы вычислительного процесса во время восстановления допустимы (*S*1);
- потеря данных и перерывы вычислительного процесса во время восстановления недопустимы (*S*2);
- потеря данных и перерывы вычислительного процесса во время восстановления допустимы (*S*3).

Потеря данных происходит, когда при информационной зависимости прикладных функциональных задач, решаемых вычислительной системой, отказывает память в двух полукомплексах, что приводит к невозможности выполнения задач, т.е. к отказу системы, при котором ее восстановление невозможно.

Перерывы вычислительного процесса во время восстановления недопустимы, например, для управляющих систем, работающих в реальном времени, при этом будем считать, что для поддержки вычислений достаточно работоспособности хотя бы одного ЦП при доступности для него памяти хотя бы в одном полукомплексе. При отказе одного ЦП доступ исправного ЦП к памяти другого (сопряженного) полукомплекса должен поддерживаться средствами комплексирования по прямому доступу.

Случай ограничения восстановления, когда потеря данных недопустима, а перерывы вычислительного процесса во время восстановления допустимы, не рассматривается, так как при отказе памяти в двух полукомплексах вычислительный процесс не реализуем, и при потере данных в обоих полукомплексах их восстановление считается невозможным.

Модели надежности с учетом ограничений восстановления

При построении марковской модели [3] надежности восстанавливаемого ДВК с учетом отмеченных ограничений восстановления (*S*1–*S*3) будем считать, что в каждый момент времени восстанавливается только один узел. Будем считать известными интенсивности отказа процессора – λ_0, памяти – λ_1, адаптера (средств комплексирования) – λ_2, а интенсивность восстановления любого узла равна μ. При достижении состояния, при котором вычислительный процесс в соответствии с перечисленными условиями (*S*1–*S*3) восстановить не удается, считается, что достигнуто невосстанавливаемое состояние (состояния полного отказа системы), когда выполнение потока прикладных задач невозможно.

Марковские модели надежности ДВК для различных случаев ограниченного восстановления после отказов *S*1–*S*3 приведены на рис. 2–4, на которых выделены состояния:

- работоспособные, при которых вычисления реализуемы;
- отказа, при которых восстановление системы возможно;
- отказа, при которых восстановление системы невозможно.

На графах переходов (рис. 2–4) вершины, представляющие состояния системы, пронумерованы (*A*0–*A*17 для рис. 2; *B*0–*B*17 для рис. 3; *C*0–*C*14 для рис. 4). В поле вершин графов представлены изображения, поясняющие состояния ДВК, в соответствии с рис. 1, при этом отказавшие узлы перечеркнуты. Переходы (ребра) графов, обозначенные сплошными линиями, соответствуют отказам, а пунктирные – восстановлениям. На графе для всех переходов указаны соответствующие им интенсивности отказов λ_0, λ_1, λ_2 и восстановлений μ.

Для варианта ограниченного восстановления *S*1 признаком невосстанавливаемого состояния является отказ блоков памяти двух полукомплексов (состояния *A*4, *A*5, *A*7, *A*8, *A*10, *A*11, *A*12, *A*15, *A*16, *A*17 неработоспособны, среди них состояния *A*5, *A*8, *A*11, *A*16, *A*17 – невосстанавливаемые, неработоспособные состояния на рис. 2–4 затемнены).

Для варианта ограниченного восстановления *S*2 невосстанавливаемое состояние возникает при отказе двух блоков памяти или двух процессоров. Для варианта *S*2, при исправности АС, способность выполнения вычислительного процесса во время восстановления сохраняется, если исправен хотя бы один ЦП и один узел памяти, а при отказе АС – если одновременно исправны ЦП и модуль памяти одного полукомплекса. Для систем, соответствующих рис. 3, все неработоспособные состояния (*B*4, *B*5, *B*7, *B*8, *B*10, *B*11, *B*15, *B*16, *B*17) являются невосстанавливаемыми.

Для варианта восстановления *S*3 все состояния являются восстанавливаемыми (к неработоспособным состояниям относятся *C*4, *C*5, *C*7, *C*8, *C*12, *C*13, *C*14), т.е. ограничений по восстановлению, обусловленных определенными сочетаниями отказов узлов, нет.

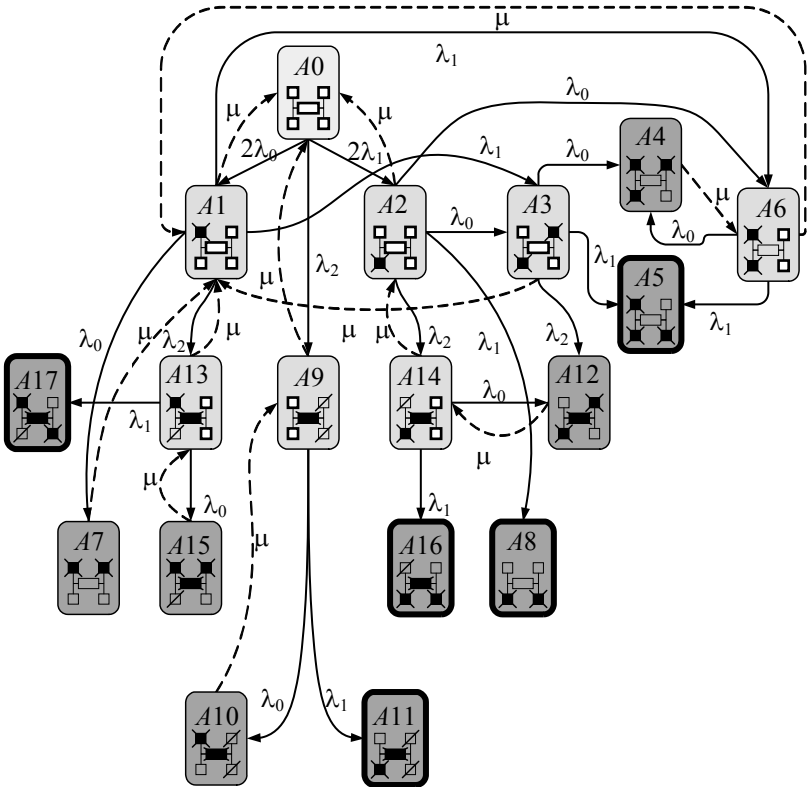

Рис. 2. Граф переходов для марковской модели ДВК при ограничении восстановления *S*1

Для вычисления вероятности нахождения системы в работоспособном состоянии по графам, представленным на рис. 2–4, в соответствии с известными правилами [3] составляется система дифференциальных уравнений, решение которой позволяет найти вероятности всех состояний ДВК, в том числе работоспособных.

Надежность ДВК охарактеризуем нестационарным коэффициентом готовности $K(t)$, который определяется как вероятность того, что в заданный момент времени t система находится в одном из работоспособных состояний. Коэффициент $K(t)$ вычисляется при суммировании вероятностей всех работоспособных состояний. Заметим, что нестационарный коэффициент готовности (функция готовности) $K(t)$ при возможностях восстановления, соответствующих *S*3 (когда все состояния допускают восстановления), с увеличением t стремится к стационарному коэффициенту готовности. При вариантах ограничений восстановления *S*1 и *S*2 (когда есть состояния, для которых восстановление системы после отказов не производится) с увеличением t вероятность работоспособного состояния системы стремится к нулю.

С учетом сформулированных условий работоспособности состояний ДВК для вариантов *S*1–*S*3 ограничений восстанавливаемости системы нестационарные коэффициенты готовности вычисляются как

$$K_{S1}(t) = p_{A0}(t) + p_{A1}(t) + p_{A2}(t) + p_{A3}(t) + p_{A6}(t) + p_{A9}(t) + p_{A13}(t) + p_{A14}(t),$$

$$K_{S2}(t) = p_{B0}(t) + p_{B1}(t) + p_{B2}(t) + p_{B3}(t) + p_{B6}(t) + p_{B9}(t) + p_{B13}(t) + p_{B14}(t),$$

$$K_{S3}(t) = p_{C0}(t) + p_{C1}(t) + p_{C2}(t) + p_{C3}(t) + p_{C6}(t) + p_{C9}(t) + p_{C10}(t) + p_{C11}(t),$$

где $p_{A0}(t), p_{A1}(t), ..., p_{A14}(t)$, $p_{B0}(t), p_{B1}(t), ..., p_{B14}(t)$, $p_{C0}(t), p_{C1}(t), ..., p_{C11}(t)$ соответствуют вероятностям состояний *A*0, *A*1, ..., *A*14 системы *S*1 (рис. 2), состояний *B*0, *B*1, …, *B*14 системы *S*2 (рис. 3) и состояний *C*0, *C*1, …, *C*14 системы *S*3 (рис. 4).

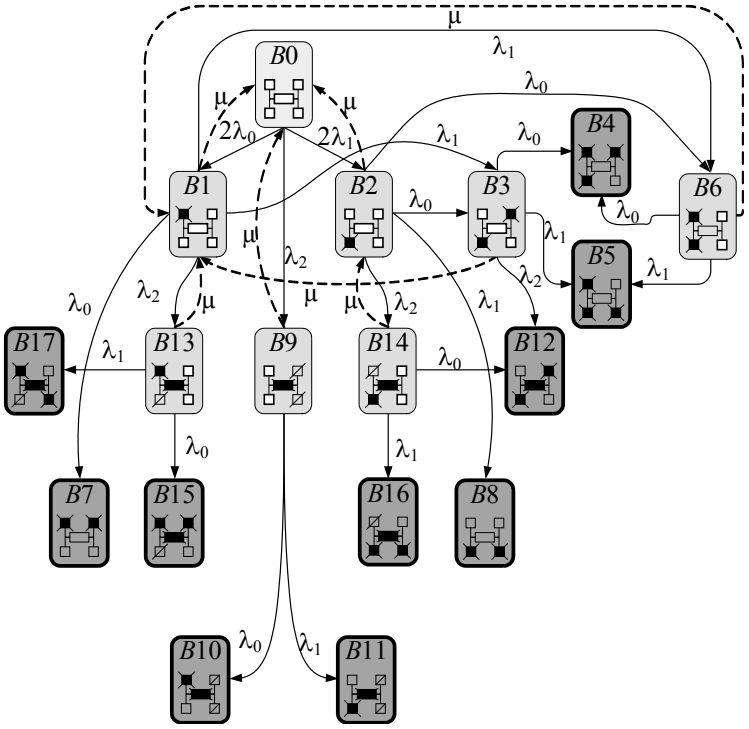

Рис. 3. Граф переходов для марковской модели ДВК при ограничении восстановления *S*2

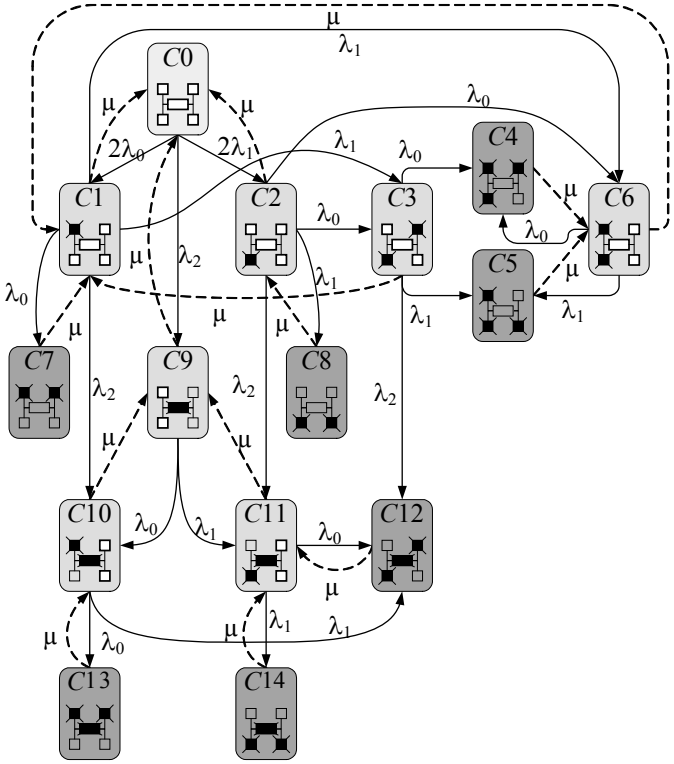

Рис. 4. Граф переходов для марковской модели ДВК при ограничении восстановления *S*3

Вероятность отказа для систем *S*1–*S*4 вычисляется как $1-K_{S1}, 1-K_{S2}, 1-K_{S3}$.

Предложенные модели позволяют вычислить вероятности опасных состояний. Так, вероятность потери информационных ресурсов для систем *S*1 определяется как

$$K_{aS1}(t) = p_{A5}(t) + p_{A8}(t) + p_{A11}(t) + p_{A16}(t) + p_{A17}(t),$$

а вероятность неопасного (восстанавливаемого) отказа – как

$$K_{bS1}(t) = p_{A5}(t) + p_{A8}(t) + p_{A11}(t) + p_{A16}(t) + p_{A17}(t) + p_{A7}(t) + p_{A10}(t) + p_{A12}(t) + p_{A15}(t).$$

Для системы S2 вероятность опасных состояний вычисляется как $1-K_{S2}$.

Результаты расчетов

Результаты расчета нестационарного коэффициента готовности $K(t)$ для рассматриваемых вариантов $S1$–$S3$ ограниченного восстановления дублированных комплексов после отказов представлены на рис. 5. Расчеты проведены для случая $\lambda_0 = 0{,}8\cdot10^{-4}$, $\lambda_1 = 0{,}5\cdot10^{-4}$, $\lambda_2 = 0{,}3\cdot10^{-4}$ 1/ч и $\mu = 1$ 1/ч. Кривые 1–3 соответствуют вариантам $S1$–$S3$ ограничений восстанавливаемости после отказов.

Расчеты выполнены в системе компьютерной математики Mathcad-15 путем решении системы дифференциальных уравнений, составленных по графам на рис. 2–4 по методу Рунге–Кутты.

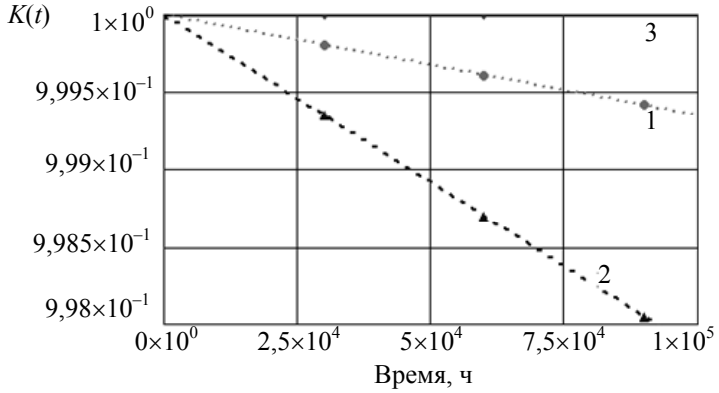

Рис. 5. Нестационарный коэффициент готовности для вариантов ограниченного восстановления дублированных комплексов после отказов. Кривые 1–3 соответствуют вариантам ограничений восстанавливаемости $S1$–$S3$

Расчеты подтверждают существенность влияния ограничений восстанавливаемости после отказов на надежность вычислительных комплексов. Таким образом, при оценке надежности и безопасности критически важных систем рекомендуется использование предлагаемых моделей, позволяющих учесть особенности ограниченного восстановления при невосполнимой потере информационных ресурсов и при прерывании критически важных вычислительных процессов при восстановлении.

Современные информационные управляющие системы, как правило, представляют собой распределенные системы, в которых множество узлов обработки и хранения данных объединяются в кластеры, связанные через многоуровневую сеть. В системах критического применения в качестве базовых узлов могут использоваться дублированные вычислительные комплексы, при оценке надежности и безопасности которых могут применяться предлагаемые в настоящей работе модели как части системы [10–14].

Заключение

Предложены марковские модели дублированных вычислительных комплексов, позволяющие учесть влияние на надежность ограниченности возможностей восстановления при недопустимости потери данных и прерываний вычислительного процесса во время восстановления.

Представленные модели надежности могут быть использованы при прогнозировании надежности и выборе вариантов построения резервированных вычислительных комплексов защищенных систем критического применения, в том числе работающих в распределенных системах реального времени.

Работа выполнена на кафедре вычислительной техники НИУ ИТМО в рамках НИР «Разработка методов и средств системотехнического проектирования информационных и управляющих вычислительных систем распределенной архитектуры».

Литература

1. ГОСТ Р МЭК 61508-2-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам. – Введ. 01.09.2008. – М.: Стандартинформ, 2008. − 68 с.
2. ГОСТ Р МЭК 61508-4-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. – Введ. 01.06.2008. – М.: Стандартинформ, 2008. − 27 с.
3. Половко А.М., Гуров С.В. Основы теории надежности. – СПб: БХВ-Петербург, 2006. – 704 с.
4. Shunji Osaki, Toshihiko Nishio. Reliability Evaluation of Some Fault-Tolerant Computer Architectures. – Springer-Verlag, Berlin Heidelberg, New York, 1980. –129 p.
5. Sorin D. Fault Tolerant Computer Architecture. – Morgan & Claypool, 2009. – 116 p.
6. Богатырев В.А., Башкова С.А., Беззубов В.Ф., Полякова А.В., Котельникова Е.Ю., Голубев И.Ю. Надежность дублированных вычислительных комплексов // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 6 (76). – С. 74–78.

7. Богатырев В.А., Демидов Д.В., Алексанков С.М. Оценка надежности дублированных комплексов с учетом контроля // Materiali VII mezinarodni vedecko-prakticka konference Aktyalni vymozenosti vedy. – 2011. Чехия, Прага 27.06.2011–05.07.2011. – Прага: Education and science, 2011. – С. 57–58.
8. Bogatyrev V.A. Exchange of Duplicated Computing Complexes in Fault Tolerant Systems // Automatic Control and Computer Sciences. – 2011. – V. 46. – № 5. – P. 268–276.
9. Богатырев В.А., Бибиков С.В. Оценка функциональной безопасности систем, связанных с безопасностью // Технико-технологические проблемы сервиса. – 2011. – № 4. – С. 45–47.
10. Богатырев В.А. Надежность вариантов размещения функциональных ресурсов в однородных вычислительных сетях // Электронное моделирование. – 1997. – № 3. – С. 21–27.
11. Богатырев В.А., Богатырев С.В. Объединение резервированных серверов в кластеры высоконадежной компьютерной системы // Информационные технологии. – 2009. – № 6. – С. 41–47.
12. Богатырев В.А. Надежность функционально-распределенных резервированных структур с иерархической конфигурацией узлов // Изв. вузов. Приборостроение. – 2000. – № 4. – С. 67–70.
13. Богатырев В.А. Надежность отказоустойчивых вычислительных систем реального времени, компонуемых из многофункциональных модулей // Информационные технологии. – 2000. – № 10. – С. 11–16.
14. Богатырев В.А. Отказоустойчивые кластеры дублированных вычислительных комплексов // Информационные технологии. – 2012. – № 1. – С. 9–15.

Богатырев Владимир Анатольевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, профессор, Vladimir.bogatyrev@gmail.com

Алексанков Сергей Михайлович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, студент, aleksankov@mail.ru

Демидов Даниил Валентинович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, студент, daniil.demidov@gmail.com

Беззубов Владимир Федорович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, bezzubov_vf@mail.ru