

ОТЗЫВ

официального оппонента на диссертацию Новикова Сергея Николаевича «Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи», представленную на соискание ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертации.

Защита информации является одним из обязательных элементов современных телекоммуникационных систем, к которым относится мультисервисная сеть связи (МСС), обеспечивающая пользователям неограниченный спектр приложений с гарантированным качеством обслуживания, в том числе и высокоскоростных, функционирующих в реальном масштабе времени. Пользователи, в данном случае, должны обладать определенными знаниями в области защиты информации и иметь дополнительное специальное криптографическое программно-аппаратное обеспечение, применение которого может быть ограничено вследствие временных, технологических, финансовых или иных затрат.

Диссертация Новикова С.Н. направлена на создание методологических основ и инструментария для реализации защиты информации с использованием технологий сетевого уровня МСС.

Поскольку защита информации в МСС является сложной финансовой, организационной, технической и **научной проблемой**, то можно заключить, что тема и направленность исследования изложенного в диссертации Новикова С.Н., являются актуальными.

Краткий обзор и анализ содержания работы.

Диссертация состоит из введения, шести глав, заключения, приложений списка литературы из 184 наименований.

Введение включает в себя: актуальность темы исследования, степень ее разработанности; цель и решаемые задачи; научную новизну; теоретическую и практическую значимость полученных результатов; методологию и методы исследования; положения, выносимые на защиту; степень достоверности и аprobацию результатов.

Первая глава посвящена анализу основных подходов по обеспечению базовых параметров защиты информации (конфиденциальности, целостности и доступности информации) в МСС.

Автором диссертации предлагается решать проблемы по обеспечению конфиденциальности, целостности и доступности информации за счет привлечения ресурсов МСС (криптографических, канальных и других). Для этого необходимо разработать и исследовать новые методики, методы и алгоритмы, позволяющие решать задачи обеспечения базовых параметров защиты информации с поддержкой качества обслуживания высокоскоростных приложений МСС, функционирующих в реальном масштабе времени. Чему и посвящена **вторая глава** диссертации.

С целью уменьшения времени шифрования и решения проблемы наличия закрытого канала связи конфиденциальность информации предлагается обеспечить за счет многократного асимметричного шифрования ключами меньшей длины. Теоретические результаты и результаты натурного эксперимента подтвердили эффективность данного предположения.

Целостность и доступность информации в МСС предлагается обеспечить за счет организации *n* параллельных соединений между узлом-источником, узлом-получателем (УП) и принятия решения в УП по *n* одновременно принятым сообщениям. Тем самым уменьшается время задержки передачи информации (по сравнению с известными методами, использующими контроль модификации переданной информации и запрос на ее повторную передачу).

Результаты статистического моделирования подтвердили теоретические результаты оценки целостности информации на выходе решающего устройства.

Автором диссертации предложен критерий выбора сетевых ресурсов, учитывающий вероятностно-стоимостные параметры соединений, обеспечивающих доступность и целостность информации в МСС.

В заключении главы делается вывод – реализация разработанных методов защиты информации возможна за счет технологий сетевого уровня модели взаимосвязи открытых систем (протоколов маршрутизации и сигнализации), что позволит обеспечить требуемый уровень информационной безопасности и качество обслуживания высокоскоростных приложений МСС, функционирующих в реальном масштабе времени.

В третьей главе диссертации: приводятся основные термины и определения предметной области «Маршрутизация»; разрабатывается обобщенная функциональная модель маршрутизации в МСС; приводится обзор методов маршрутизации в МСС; разрабатывается новая классификация методов маршрутизации в сетях связи; предлагаются новые методы маршрутизации в МСС («Логико-статистический», «Логико-лавинный», «Логико-лавинно-статистический»).

Предложенная в диссертации классификация методов маршрутизации в отличии от известных позволяет:

- выявить множество вариантов реализации как последовательных, так и параллельных (многопутевых) методов маршрутизации;
- провести целенаправленный анализ и синтез тех методов маршрутизации, которые будут наиболее эффективно функционировать в предполагаемых сетях связи и в заданных условиях.

Четвертая глава посвящена разработке методик и моделей, позволяющих проводить анализ методов маршрутизации с целью выявления тех методов, которые будут наиболее эффективно функционировать в предполагаемых сетях связи и в заданных условиях:

- математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов;

- математическую модель маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи;
 - методику определения плана распределения информации на однородной ячеистой сети связи большой размерности;
 - упрощенную имитационную модель маршрутизации,
- В данной главе так же определены и разработаны пути сокращения вычислительной сложности алгоритмов оценки структурной надежности сети связи методом статистического моделирования:
- уменьшение дисперсии оценок результатов моделирования с сохранением точности;
 - эффективные методы проверки графа сети на связность.

Пятая глава диссертационной работы посвящена анализу результатов моделирования методов маршрутизации для разработанных моделей, включая результаты имитационного моделирования МСС в условиях ограниченных сетевых ресурсов, выполненных с использованием специализированного программного продукта Opnet Modeler v 14.0.

В результате исследования методов маршрутизации в условиях внешних деструктивных воздействий на элементы МСС автору диссертации удалось установить следующее.

1. В условиях практического отсутствия внешнего деструктивного воздействия «Статистические последовательные» методы маршрутизации обеспечивают больший пользовательский сетевой ресурс по сравнению с «Лавинными» методами, следовательно, увеличивают возможность передачи большего объема пользовательской информации;

2. При условии выхода из строя более 20 % ÷ 30 % сетевых ресурсов МСС «Лавинные параллельные» методы маршрутизации по сравнению со «Статистическими» показывают лучшие результаты. Данный результат независимо подтвержден на различных структурах МСС и с применением различных математических и имитационных моделей.

3. В случае невозможности смены «Статистических последовательных» методов маршрутизации на «Лавинные параллельные» в условиях внешних деструктивных воздействий необходимо на этапе проектирования МСС предусматривать не менее 30 % резерва сетевых ресурсов.

Шестая глава диссертации посвящена разработке методик защиты информации за счет технологий сетевого уровня модели взаимосвязи открытых систем без снижения качества обслуживания приложений МСС. Данные методики базируются на разработанных в предыдущих главах: методах обеспечения базовых параметров защиты информации (конфиденциальность, доступность и целостность); методах маршрутизации и проведенных исследований методов маршрутизации в условиях внешних деструктивных воздействий на элементы МСС.

В заключении представлены основные результаты, полученные соискателем, и перспективы дальнейшей разработки темы.

Научная новизна полученных результатов.

В диссертации получены следующие новые научные результаты:

1. Впервые предложена методология, позволяющая обеспечить защиту информации на базе протоколов сетевого уровня мультисервисных сетей связи, включающая:

- подход к обеспечению конфиденциальности информации, который в отличие от аналогов использует многократное асимметричное шифрование ключами меньшей длины, что позволяет уменьшить время шифрования в l^{c-1} раз, где l – количество асимметричных шифрований, c – постоянная, значение которой определяется криптографическими алгоритмами шифрования;
- критерий выбора сетевых ресурсов (маршрутов) с точки зрения обеспечения целостности и доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости;
- способ и алгоритм обеспечения целостности информации, которые в отличие от известных используют параллельные (многопутевые) методы маршрутизации, учитывают вероятностно-стоимостные параметры маршрутов и позволяют уменьшить время задержки передачи информации;
- алгоритм обеспечения доступности информации в мультисервисных сетях связи, отличающийся от известных тем, что параллельные соединения устанавливаются в соответствии с разработанным критерием выбора сетевых ресурсов (маршрутов), позволяющим выбирать маршруты с точки зрения обеспечения доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости.

2. Предложена новая классификация методов маршрутизации, отличающаяся наличием независимых процедур, включающих: формирование плана распределения информации на сети; выбор исходящих трактов передачи информации в узлах коммутации. Классификация позволяет: выявить множество вариантов реализации последовательных и параллельных (многопутевых) методов маршрутизации; провести целенаправленный анализ и синтез методов маршрутизации, которые будут эффективно функционировать в условиях штатной эксплуатации и внешних деструктивных воздействий на элементы мультисервисной сети связи.

3. Предложен новый метод маршрутизации («Гибридный»), отличающийся от известных тем, что в зависимости от степени воздействия внешних деструктивных факторов на мультисервисную сеть связи, используется «Логический», «Статистический» или «Лавинный» методы. Это позволяет сократить объем передаваемой служебной информации в мультисервисной сети связи во время ввода узлов коммутации в эксплуатацию, штатной эксплуатации и в условиях внешних деструктивных воздействий на элементы сети.

4. Инструментарий (методики, математические модели, алгоритмы, программные продукты) для анализа методов маршрутизации в мультисервисных сетях связи, который в отличие от известных, учитывает

входной самоподобный трафик и *внешние деструктивные воздействия* на элементы мультисервисной сети связи и позволяет выявить те методы маршрутизации, которые будут наиболее эффективно функционировать в *условиях штатной эксплуатации и внешних деструктивных воздействий* на элементы сети.

5. Способ проверки графа сети на связность, отличающийся тем, что анализируемый граф «разбивают» на подграфы; каждый подграф проверяют на связность «стягиванием» смежных вершин к первоначально выбранной, до тех пор, пока подграф не представится в виде одиночной точки или множества точек; в результате формируется суперграф, который проверяется на связность «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока суперграф не представится в виде одиночной точки (исходный граф связан) или множества точек (исходный граф не связан); это позволяет уменьшить алгоритмическую сложность решения задачи в \sqrt{S} (S – количество вершин графа) по сравнению с известными способами.

6. Инструментарий (методики, методы, алгоритмы), позволяющий за счет применения предлагаемых:

- параллельных (многопутевых) методов маршрутизации;
- подхода к обеспечению конфиденциальности информации;
- критерия, позволяющего выбирать сетевые ресурсы (маршруты);
- способа обеспечения целостности информации;
- алгоритма обеспечения доступности информации

обеспечить конфиденциальность, целостность, доступность информации и показатели качества обслуживания приложений мультисервисной сети связи.

Теоретическая значимость, полученных Новиковым С.Н. результатов подтверждается тем, что:

- изложены положения, расширяющие набор методов, применяемых при создании защищенных телекоммуникационных систем, в частности, в обеспечении конфиденциальности, целостности и доступности информации за счет использования протоколов сетевого уровня модели взаимосвязи открытых систем без снижения качества обслуживания приложений мультисервисных сетей связи;
- изложены положения, относящиеся к сетевому уровню модели взаимосвязи открытых систем, и выявлены новые методы маршрутизации, эффективно функционирующие в *условиях штатной эксплуатации и внешних деструктивных воздействий* на элементы сети;
- определены факторы, влияющие на уменьшение вероятности отказа в обслуживании заявок за счет применения параллельных (многопутевых) методов маршрутизации в *условиях внешних деструктивных воздействий* на элементы мультисервисных сетей связи;
- проведена модернизация существующих математических моделей маршрутизации, основанная на учете самоподобия входного трафика и

внешних деструктивных воздействий на элементы мультисервисной сети связи.

Практическая ценность результатов подтверждается тем, что:

1. Разработан инструментарий (методики, методы, алгоритмы), позволяющий реализовать конфиденциальность, целостность и доступность информации с обеспечением показателей качества обслуживания приложений мультисервисной сети связи.

2. Многократное асимметричное шифрование ключами меньшей длины позволяет обеспечить конфиденциальность информации при меньшем времени ее шифрования в $l^{c^{-1}}$ раз, где l – количество асимметричных шифрований, c – постоянная, значение которой определяется криптографическими алгоритмами шифрования.

3. Разработан инструментарий (методики, модели, алгоритмы, программные продукты), включающий:

- математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи;

- математическую модель маршрутизации в условиях входного самоподобного трафика и *внешних деструктивных воздействий* на элементы мультисервисной сети связи;

- методику определения плана распределения информации на однородной ячеистой сети связи большой размерности;

- упрощенную имитационную модель маршрутизации в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи.

Инструментарий позволяет выявить методы маршрутизации, которые будут эффективно функционировать в *условиях штатной эксплуатации и внешних деструктивных воздействий* на элементы мультисервисной сети связи.

4. Программная реализация разработанного способа проверки графа сети на связность позволяет уменьшить время решения задачи в \sqrt{S} (S – количество вершин графа) по сравнению с известными способами.

5. Установлено, что в *условиях внешних деструктивных воздействий* на элементы мультисервисной сети связи (выход из строя более 30% элементов) параллельные (многопутевые) методы маршрутизации позволяют (усредненные данные) понизить среднюю вероятность отказа на обслуживание заявок пользователей до 20%.

6. Разработаны рекомендации по применению методов маршрутизации для обеспечения конфиденциальности, целостности и доступности информации в мультисервисных сетях связи.

Реализация и внедрение результатов исследований. Значение полученных результатов исследования для практики подтверждается тем, что:

– в рамках выполнения хоздоговорных НИР, грантов фонда фундаментальных и прикладных, научных исследований СибГУТИ разработаны алгоритмы, математические модели и их программные реализации, документы, поясняющие применение и техническое описание перечисленных алгоритмов и программ

приняты: в гос. фонд алгоритмов и программ СССР; в отраслевой фонд алгоритмов и программ координационного центра информационных технологий министерства образования РФ; объединенный фонд электронных ресурсов «Наука и Образование» института научной информации и мониторинга РАО и внедрены в организациях: ООО «ЦИБ-Сервис» (г.Барнаул) при разработке защищенных телекоммуникационных систем связи; ООО «СИБ» (г. Новосибирск) в разработках защищенной системы видео конференцсвязи в Правительстве Республики Тыва; ООО «Предприятие «Элтекс» (г. Новосибирск) в процесс проектирования и разработки сетевого коммутационного оборудования (коммутаторов и маршрутизаторов), а так же использованы:

ООО «Газпром трансгаз Томск» (г. Томск) при проектировании систем управления сетями связи; в управлении информационного и документационного обеспечения губернатора Иркутской области и Правительства Иркутской области (г. Иркутск) при обеспечении безопасности каналов связи органов государственной власти, имеющих доступ к корпоративной сети передачи данных;

– в рамках выполнения госбюджетных НИР разработаны: обобщенная, функциональная модель маршрутизации в МСС; классификация методов маршрутизации для сетей связи; методы маршрутизации; математическая модель маршрутизации в МСС; методика обеспечения совокупности параметров, обеспечивающих защиту информации (конфиденциальность, целостность и доступность) за счет ресурсов МСС, и внедрены в учебный процесс СибГУТИ при проведении всех видов занятий для студентов специальности «Информационная безопасность телекоммуникационных систем» в дисциплинах «Телекоммуникационные технологии с гарантированным качеством обслуживания», «Моделирование систем», «Защита и мониторинг мультисервисных сетей связи», «Основы проектирования защищенных телекоммуникационных систем», «Живучесть телекоммуникационных систем», в рамках которых издано 3 учебных пособия с грифом УМО,

а так же использованы при подготовке учебно-методических комплексов проекта Европейской Комиссии TEMPUS JEP_26032_2005, в рамках которых издано учебное пособие для студентов магистратуры направления «Телекоммуникации».

Методология и методы исследования.

Для достижения поставленной цели диссертантом использовался математический аппарат теории вероятностей, теории массового

обслуживания, теории графов и статистическое моделирование сложных систем.

Степень достоверности и апробация результатов

Новикова С.Н. подтверждается тем, что результаты получены на сертифицированном оборудовании и программном обеспечении. Показана воспроизводимость результатов исследований в различных условиях. Теория построена на известных, проверяемых данных и фактах, в том числе для предельных случаев, согласуется с опубликованными экспериментальными данными других исследователей по данной тематике. Использованы и обобщены результаты исследований ведущих специалистов в области защиты информации телекоммуникационных систем и управления мультисервисными сетями связи. Установлено количественное совпадение численных результатов, полученных с помощью математического, имитационного моделирования и натурных экспериментов.

Основные результаты работы докладывались и обсуждались на научных конференциях и форумах международного, всероссийского и республиканского уровнях.

Соответствие содержания диссертации содержанию опубликованных работ.

Всего по теме диссертации опубликовано 66 работ, в том числе: 14 статей в научных журналах и изданиях, рекомендованных ВАК РФ; один патент на способ изобретения; 10 свидетельств на программы для электронных вычислительных машин, зарегистрированных в установленном порядке; 6 работ включены в библиографические базы Web of Science и в Scopus; 2 рецензируемых монографии; 4 рецензируемых учебных пособия, в том числе 3 с грифом УМО.

Анализ публикаций соискателя позволяет заключить, что все основные положения и выводы работы достаточно полно отражены в публикациях автора.

Соответствие содержания диссертации содержанию автореферата.

Содержание автореферата диссертации в полной мере отражает содержание диссертации, полученные в ней практические и теоретические результаты и выводы.

Соответствие темы диссертации заявленной научной специальности.

Представленная на рецензирование работа соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по следующим пунктам:

1. Теория и методология обеспечения информационной безопасности и защиты информации.

5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.

6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

9. Модели и методы оценки защищенности информации и информационной безопасности объекта.

13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Личное участие автора в полученных результатах.

В диссертации использованы результаты, в которых Новикову С.Н. принадлежит основная роль в постановке, решении задач и в обобщении полученных результатов. Некоторые из публикаций написаны в соавторстве с аспирантами научной группы автора (Буров А.А., Жарикова В.О., Киселев А.А., Солонская О.И.).

Рекомендации по использованию результатов.

Разработанные методики, методы, алгоритмы, математические модели, программные продукты могут быть использованы для анализа и синтеза систем защиты информации в мультисервисных сетях связи.

Разработанные автором учебно-методические комплексы на основе предлагаемых методик, методов, алгоритмов, математических моделей и программных продуктов, быть использованы для проведения всех видов занятий для студентов и магистрантов специальности «Информационная безопасность телекоммуникационных систем» в ВУЗах телекоммуникационного профиля в дисциплинах: «Основы проектирования защищенных телекоммуникационных систем»; «Основы технической эксплуатации защищенных телекоммуникационных систем»; «Живучесть телекоммуникационных систем»; «Телекоммуникационные технологии с гарантированным качеством обслуживания»; «Моделирование систем».

Замечания к работе.

1. В диссертации (раздел 2.1, стр. 34 – 38) проведено исследование возможности использования многократного асимметричного шифрования ключами меньшей длины с целью уменьшения времени шифрования с сохранением криптостойкости. Теоретически показано и результатами натурного эксперимента подтверждено (на примере шифрования алгоритмом RSA блока данных объемом 1 кБ при изменении длины ключа от 256 бит до 2048 бит и использовании составного 256-битного ключа), что такой подход позволяет получить линейную зависимость времени шифрования от длины «составного» ключа и тем самым значительно сократить время шифрования. Однако *в диссертации не приведены условия, при которых данный подход*

сохраняет криптостойкость по сравнению с асимметричным шифрованием «одним» ключом.

2. В диссертации разработан метод обеспечения целостности информации на сетевом уровне мультисервисных сетей связи (раздел 2.2, стр. 38 – 41), который предусматривает, что между узлом-источником и узлом-получателем организуется n параллельных соединений, по которым передается сообщение. Целостность информации достигается за счет принятия решения в узле-получателе по n принятым символам $x = (x_1, \dots, x_i, \dots, x_n)$.

На практике далеко не всегда пользователи сети имеют более одного канала доступа к узлам коммутации. Следовательно, *реализация, разработанного в диссертации метода обеспечения целостности пользовательской информации, современными сетевыми протоколами возможна не всегда.*

3. При разработке математической модели влияния методов формирования плана распределения информации на объем доступных сетевых ресурсов (раздел 4.2, стр. 80 – 87) автор сделал предположение, что процесс использования (занятия) сетевых ресурсов, необходимых для реализации методов маршрутизации в мультисервисных сетях связи, имеет нелинейную зависимость и в общем случае подчиняется полиномиальному закону (4.3). При этом, средние сетевые ресурсы, доступные для передачи пользовательской информации, определяются выражением (4.5). Математические выражения (4.7) и (4.9) определяют средние сетевые ресурсы, доступные для передачи пользовательской информации для конкретных методов маршрутизации («Лавинного» и «Статистического». *Вместе с тем (4.7) и (4.9) не учитывают структуру сети связи.*

4. При разработке математической модели маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи (раздел 4.3 стр. 88 – 116) автор диссертации предлагает использовать для входного потока пакетов в мультисервисную сеть связи гамма-распределение. При этом отмечает, что «распределения: Вейбулла, гамма, логнормальное, гиперэкспоненциальное и Парето ... дают более точные результаты расчета размеров буферов памяти коммутационного оборудования». Таким образом в диссертации *недостаточно уделено внимания по обоснованию выбора гамма-распределения в качестве входного самоподобного трафика.*

5. В разделе 4.3.3 «Разработка математической модели распределения потока сообщений между транзитными узлами мультисервисной сети связи» на стр. 99 – 101 автором выведено математическое выражение (4.23), позволяющее расчитать вероятности отказа в обслуживании агрегированных потоков сообщений в трактах передачи сообщений между узлами коммутации мультисервисной сети связи для случая, когда параметр Херста лежит в пределах $0,5 < H_{\max} < 1$, что отражает самоподобный характер трафика. *Результаты математического*

моделирования маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы мультисервисной сети связи (раздел 5.3, стр. 146 – 150) представлены для случая, когда $H_{\max} = 0,5$, что не отражает самоподобный характер трафика.

Данные замечания не снижают общей положительной оценки диссертационной работы значимости полученных научно-практических результатов.

Общая оценка диссертационной работы.

Диссертация Новиков Сергея Николаевича представляет собой законченную научную работу, в которой решена научная проблема, имеющая важное хозяйственное значение, внедрение которой вносит значительный вклад в развитие технологий защиты информации в современных телекоммуникационных системах связи. В рамках решения этой проблемы предложена методология защиты информации в мультисервисных сетях связи, отличающаяся тем, что конфиденциальность, целостность и доступность информации обеспечивается за счет технологий сетевого уровня модели взаимосвязи открытых систем (протоколов маршрутизации и сигнализации). Тем самым, на время сеанса связи, для защиты информации пользователям предоставляется возможность привлечения территориально-распределенных ресурсов сети (каналов связи, баз данных, специализированных криптографических, программно-аппаратных комплексов и т.п.) без снижения качества обслуживания высокоскоростных приложений, функционирующих в реальном масштабе времени.

По содержанию диссертационная работа отвечает требованиям «Положения о порядке присуждения ученых степеней» ВАК России, утвержденного постановлением Правительства РФ № 842 от 24.09.2013 г., а ее автор - Новиков Сергей Николаевич заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заведующий кафедрой

прикладной информатики, НИ ТГУ

доктор технических наук,

профессор

Сущенко Сергей Петрович

Подпись С.П.Сущенко удостоверяю:



Сведения подписанта:

Ф.И.О.: Сущенко Сергей Петрович

Должность: Заведующий кафедрой прикладной информатики, декан факультета информатики

Полное и сокращенное наименование места работы:

г. Томск, Национальный исследовательский Томский государственный университет (НИ ТГУ)

Адрес организации:

634050, г. Томск, пр. Ленина, д. 36, корпус 2, ауд. 106

Телефон: 8 (3822) 529-496

E-mail: ssp@inf.tsu.ru

Специальность, по которой защищалась диссертация Сущенко С.П.:

05.13.01 – Управление в технических системах