Intellectual Technologies on Transport No 3

Интеллектуальные технологии на транспорте № 3

Санкт-Петербург
St. Petersburg
2016

Интеллектуальные технологии на транспорте
№ 3, 2016

Сетевой электронный научный журнал, свободно распространяемый через Интернет.
Публикует статьи на русском и английском языках с результатами исследований и практических достижений в области интеллектуальных технологий и сопутствующих им научных исследований

Журнал основан в 2015 году

Учредитель и издатель

Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» (ФГБОУ ВПО ПГУПС)

Адрес редакции
190031 Санкт-Петербург, Московский пр., 9, ПГУПС
email: itt-pgups@yandex.ru, сайт: http://itt-pgups.ru/

ISSN 2413-2527

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ЭЛ № ФС77-61707 от 07 мая 2015 г.

Журнал зарегистрирован в Российском индексе научного цитирования (РИНЦ)

Intellectual Technologies on Transport
Issue № 3, 2016

Network electronic scientific journal, open access. It publishes articles in Russian and English with the results of research and practical achievements in the field of intelligent technologies and associated research

Founded in 2015

Founder and Publisher

Federal State Educational Institution of Higher Education
«Emperor Alexander I Petersburg State Transport University»

Adress
190031, St. Petersburg, Moskovskiy pr., 9, 2–108
email: itt-pgups@yandex.ru, http://itt-pgups.ru/

ISSN 2413-2527

The journal is registered by the Federal Service for Supervision of Communications and Mass Media, EL №FS77-61707 testimony from May 7, 2015

The journal is registered in the Russian Science Citation Index (RSCI)

Содержание

Contents

Система опережающей подготовки специалистов в области высокоскоростного железнодорожного транспорта

Блажко Л. С., Киселев И. П., Плеханов П. А.
Петербургский государственный университет
путей сообщения Императора Александра I (ПГУПС)
Санкт-Петербург, Россия
dou@pgups.edu

Аннотация. **Статья описывает созданную в ПГУПС уникальную систему опережающей подготовки специалистов в области высокоскоростного железнодорожного транспорта. Представлены зарождение и развитие системы, ее реализация в виде учебной программы для магистров инфраструктуры и эксплуатации высокоскоростных железных дорог.**

Ключевые слова: **высокоскоростной железнодорожный транспорт, система опережающей подготовки специалистов.**

Введение

В последние годы при непосредственном участии авторов данной статьи в ПГУПС создана система опережающей подготовки специалистов в области высокоскоростного железнодорожного транспорта (далее – Система). Цели, достигнутые в ходе ее формирования, прямо вытекают из стратегических задач, поставленных государством в области внедрения инновационных технологий на железнодорожном транспорте. Необходимость создания высокоскоростных железнодорожных магистралей (ВСМ), признанных в мире самым передовым направлением развития железных дорог, обозначена в ряде указов президента России и в Транспортной стратегии страны до 2030 г. [1].

В указе президента России от 16 марта 2010 г. № 21 «О мерах по организации движения высокоскоростного железнодорожного транспорта в Российской Федерации» отмечена необходимость выработать комплекс мер, направленных на обучение и подготовку квалифицированных кадров для организации и обеспечения высокоскоростного железнодорожного движения [2], что в значительной мере и реализовано в предложенной Системе.

Авторы разработали систему в тесной интеграции с производством, в частности с ОАО «РЖД», которое определено единственным исполнителем по осуществлению функций заказчика при проектировании инфраструктуры высокоскоростного железнодорожного транспорта [2], а также в творческом взаимодействии с компаниями, имеющими самые высокие достижения в области ВСМ: Национальным обществом железных дорог Франции, Дойче Банн, Китайскими железными дорогами, компаниями Альстом, Бомбардье, Сименс и другими.

Зарождение и развитие Системы

Отдельные элементы Системы внедряли в учебный процесс Ленинградского института инженеров железнодорожного транспорта (ЛИИЖТ, ныне – ПГУПС) в 1970–1990 гг. Авторы проекта Л. С. Блажко и И. П. Киселев были в числе пионеров в области исследований высокоскоростного железнодорожного транспорта в СССР, одни из первых преподавателей ЛИИЖТ – ПГУПС по данной тематике, о чем свидетельствует их участие в подготовке уникального издания – первой на пространстве бывшего СССР двухтомной монографии «Скоростной и высокоскоростной железнодорожный транспорт» [3]. И. П. Киселев руководил выходом издания, был ответственным за выпуск.

Как цельная Система начала формироваться в начале 2000-х годов и в полном объеме сложилась в 2012–2015 гг. под руководством и при активном личном участии всех трех авторов в рамках международной программы TEMPUS (Трансъевропейской программы академической мобильности для университетов – Trans-European Mobility Programme for University Studies).

В настоящее время в ПГУПС Система охватывает весь цикл подготовки бакалавров, специалистов, магистров, аспирантов, а также послевузовской переподготовки и повышения квалификации – от профориентации школьной молодежи до переподготовки выпускников.

На каждом уровне реализуются свои разработанные в ПГУПС оригинальные просветительские и учебные мероприятия и дисциплины – от общего курса высокоскоростного железнодорожного транспорта до специальных дисциплин и специализаций. Важным элементом является учебный курс ВСМ в рамках так называемой отраслевой составляющей для студентов целевого приема ОАО «РЖД», а также цикл послевузовской переподготовки специалистов объемом 600 часов, реализованный в рамках проекта TEMPUS.

Реализация учебной программы для магистров инфраструктуры и эксплуатации высокоскоростных железных дорог

В проекте TEMPUS при участии авторов данной статьи подготовлена оригинальная учебная программа «Магистр инфраструктуры и эксплуатации высокоскоростных железных дорог для России и Украины» (фр. «Master infrastructure exploitation Grande Vitesse Ferroviaire en Russie et Ukraine», MieGVF). Название условно, поскольку по действующему в Российской Федерации положению, во-первых, обучение по магистерским программам должно продолжаться два учебных года, во-вторых, в перечне направлений подготовки

высшего образования – магистратуры, утвержденном Министерством образования и науки России, нет направления «Высокоскоростной железнодорожный транспорт». Однако это не является непреодолимым препятствием на пути реализации программы MieGVF, поскольку возможны несколько вариантов ее согласования с действующей процедурой обучения в вузе.

Например, по решению ученого совета российского вуза программа может быть принята в качестве программы или дисциплин учебного плана других программ по высокоскоростному железнодорожному транспорту для направлений магистратуры 08.00.00 «Техника и технологии строительства» и 23.00.00 «Техника и технологии наземного транспорта». Также годичная программа под условным названием «Магистратура ВСМ» может быть предложена студентам выпускного курса или специалистам, имеющим диплом об окончании соответствующего вуза в качестве дополнительного профессионального образования по программе переподготовки. Именно этим путем пошли с 2014/2015 учебного года в МИИТе и в ПГУПС.

Результатом проведенных в 2012–2013 гг. предварительных рабочих контактов, встреч, переговоров руководителей, специалистов, железнодорожных организаций и профессоров высших учебных заведений ряда европейских стран был сформирован консорциум, который представил свой проект на международный конкурс и выиграл грант TEMPUS Европейского Союза. В состав консорциума вошли Национальное общество железных дорог Франции (SNCF) [4], имеющее большой опыт в области ВСМ; ОАО «РЖД», активно развивающее в последние годы скоростное движение и приступившее к реализации проекта создания первой в стране ВСМ; Украинские железные дороги, заинтересованные в повышении скорости движения поездов.

В консорциуме также представлены два крупнейших транспортных (железнодорожных) университета России: Петербургский государственный университет путей сообщения Императора Александра I и Московский государственный университет путей сообщения Императора Николая II; университеты Украины: Украинский государственный университет железнодорожного транспорта (г. Харьков), Днепропетровский национальный университет железнодорожного транспорта им. академика В. Лазаряна (г. Днепропетровск). Большое значение для проекта TEMPUS имеет участие в консорциуме одного из старейших и самых престижных технических университетов Европы – Национальной консерватории искусств и ремесел (г. Париж, Франция) [5]. В консорциум также вошли такие авторитетные вузы, как Рижский технический университет (Латвия) и Университет технологий и гуманитарных наук им. Казимира Пулавского в Радоме (Польша).

В рамках работы консорциума, опираясь на анализ мирового опыта и обобщенные теоретические и практические знания в области высокоскоростного железнодорожного транспорта, принята модель годичного обучения с объемом учебных занятий порядка 600–800 академических часов. Подготовка (или переподготовка) в течение одного учебного года была признана соответствующей как потребностям, так и возможностям специалистов-производственников и студентов-старшекурсников технических вузов. В качестве базы для обучения по программе проекта TEMPUS признано необходимым либо наличие у слушателей образования на уровне специалиста-инженера (пятилетнего обучения), либо завершения первого года обучения в магистратуре на базе четырехлетней подготовки бакалавра.

В рамках единого проекта подготовлены две подпрограммы: «Инфраструктура высокоскоростных железных дорог» и «Эксплуатация и подвижной состав высокоскоростных железных дорог». При этом авторы-разработчики отдавали себе отчет, что за рамками проекта еще остаются важные направления, связанные, например, с экологией, экономикой, психологией отбора и подготовки персонала для ВСМ и др.

Структура учебного плана каждой подпрограммы состоит из общей части, включающей основные теоретические и практические положения в области высокоскоростного железнодорожного движения, нормативной базы создания и эксплуатации ВСМ (международной и национальной), социально-экономического анализа проектов ВСМ, управления реализацией проектов и др., и специальной части, различной для каждой подпрограммы.

В качестве законченной логической части (раздела) программы обучения принят так называемый модуль, который может включать две или три европейские зачетные единицы (ECTS – European Credit Transfer System). Содержание модулей разработали эксперты консорциума в составе около 100 профессоров, преподавателей, научных сотрудников вузов, специалистов железнодорожных предприятий и организаций.

Каждый модуль создавался, как минимум, тремя экспертами, входившими в так называемые триномы: эксперты представляли три разные организации (участника) консорциума. Учебно-методические модули – тексты лекций, иллюстративные презентации, контрольные задания и проверочные тесты – подготовлены на русском и английском языках, они представляют собой уникальный материал объемом более 5 тыс. страниц. Представленные модули положительно оценили международные железнодорожные эксперты, специально приглашенные консорциумом для оценки учебно-методического материала.

В дополнение к разработанным модулям профессора ПГУПС при участии специалистов ОАО «РЖД» подготовили и издали к началу занятий слушателей программы TEMPUS учебное пособие «Высокоскоростной железнодорожный транспорт» [6]. Выход в свет этого фундаментального и уникального не только для российской, но и для мировой практики труда (в двух томах общим объемом около 700 стр.), охватывающего весь спектр вопросов по указанной проблематике, само по себе является важным событием в области подготовки железнодорожных кадров. Необходимо отметить, что разделы учебного пособия совпадают с полной учебной программой курса TEMPUS MieGVF.

С сентября 2014 г. по июнь 2015 г. в железнодорожных университетах Санкт-Петербурга, Москвы, Днепропетровска и Харькова по указанной программе обучались 60 слушателей из России и 30 из Украины – студенты выпускных курсов, а также железнодорожные специалисты и менеджеры. Для обучения в российских вузах – МИИТе и ПГУПС – слушателей отбирал на конкурсной основе Департамент управления персоналом ОАО «РЖД» совместно с профессорами и администрацией вузов. Было решено, что в первый учебный год (2014/2015) подпрограмма «Инфраструктура высокоскоростных железных дорог» будет опробована в ПГУПС, а подпрограмма «Эксплуатация и подвижной состав высокоскоростных

железных дорог» – в МИИТе. В 2015/2016 и 2016/2017 учебных годах обучение по этой программе продолжилось.

Опыт реализации программы TEMPUS «Магистр инфраструктуры и эксплуатации высокоскоростных железных дорог для России и Украины» был тщательно рассмотрен в июле 2015 г. в Санкт-Петербурге на международном конгрессе «Инновации и кадры в геополитике железнодорожного транспорта» [7–12]. В рамках этого конгресса, который являлся частью Петербургского международного экономического форума 2015 г., для рассмотрения итогов программы TEMPUS был организован специальный симпозиум, в котором приняли участие представители всех организаций – участников консорциума, а также руководители высокого уровня различных предприятий и организаций железнодорожного транспорта, промышленных и строительных компаний, технических университетов России и ряда европейских стран.

Проект TEMPUS MieGVF был также представлен одним из авторов настоящей статьи на IX всемирном конгрессе по высокоскоростному железнодорожному движению в Токио в июне 2015 г. [13–15]. Результаты первого года обучения с большим интересом и одобрением встречены участниками секции конгресса «Взаимодействие между университетами и сектором высокоскоростного железнодорожного транспорта», посвященной сотрудничеству университетов с железными дорогами в области ВСМ.

Заключение

В настоящее время в ПГУПС обучаются слушатели второго набора, среди которых специалисты ОАО «РЖД» и студенты старших курсов железнодорожных специальностей, имеющие целевые направления на обучение от российских железных дорог. Несомненно, разработанный курс обучения в области высокоскоростного железнодорожного транспорта, включающий уникальный комплект учебно-методического материала на русском и английском языках, представляет интерес для железнодорожников и кадровых служб стран, реализующих или планирующих реализовать проекты ВСМ.

Литература

1. Транспортная стратегия Российской Федерации на период до 2030 года (утв. распоряжением правительства РФ от 22.11.2008 г. № 1734-р).

2. Указ президента РФ от 16.03.2010 г. № 321 «О мерах по организации движения высокоскоростного железнодорожного транспорта в Российской Федерации».

3. Скоростной и высокоскоростной железнодорожный транспорт: в 2 т. / под ред. В. И. Ковалева. – СПб.: Выбор. – Т. 1. – 2001. – 265 с.; т. 2. – 2003. – 448 с.

4. http://www.cnam.fr/ (дата обращения 26.09.2016).

5. http://www.sncf.com/ (дата обращения 26.09.2016).

6. Высокоскоростной железнодорожный транспорт. Общий курс: в 2 т. / под ред. И. П. Киселева. – М.: УМЦ ЖДТ, 2014. – Т. 1. – 308 с.; т. 2. – 372 с.

7. Материалы международного конгресса «Инновации и кадры в геополитике железнодорожного транспорта», 17–18 июня 2015 г., Петербург. гос. ун-т путей сообщения Императора Александра I. – СПб., 2015.

8. Блажко Л. С. Международная программа дополнительного профессионального образования по высокоскоростному железнодорожному транспорту / Л. С. Блажко, И. П. Киселев // Транспорт РФ. – 2015. – № 2 (57). – С. 19–25.

9. Блажко Л. С. Подготовка магистров высокоскоростного железнодорожного транспорта в рамках европейского проекта «TEMPUS» / Л. С. Блажко, И. П. Киселев // Бюл. ОСЖД. – 2015. – № 4–5. – С. 18–25.

10. Киселев И. П. Вузы будут совместно продвигать проекты ВСМ // Гудок. – 2015. – 17 дек.

11. Магистры высокоскоростных магистралей // Гудок. – 2015. – 22 сент.

12. Интеллектуальный ресурс // Гудок. – 2015. – 18 июня.

13. Program of the 9th UIC World Congress on High Speed Rail, July 7–10, 2015, Tokyo Int. Forum. – Tokyo, 2015.

14. UIC 9th World HSR Report // Speedlines. – 2015. – No. 16. – P. 21-24.

15. Hosting the 9th UIC World Congress on High-speed rail // Japan Railway & Transport Review. – 2016. – No. 67. – P. 36-47.

System of Advancing Preparation of High-Speed RailwayExperts

Blazhko L.S., Kiselev I.P.,
Plekhanov P.A.
Emperor Alexander I St. Petersburg State Transport University
Saint-Petersburg, Russia
dou@pgups.edu

Abstract. **The article presents the description created in PGUPS the unique System of advancing preparation of high-speed railway experts. The article contains origin and development of the System, its realization in the form of the education program for masters of an infrastructure and operation of the high-speed railways.**

Keywords: **high-speed railways, system of advancing preparation of experts.**

References

1. Transport strategy of the Russian Federation for the period till 2030 (conf. by the Order of the Government of the Russian Federation, Nov. 22nd, 2008, no. 1734-r).

2. The Decree of the president of the Russian Federation, March 16th, 2010, no. 321 "About measures on the organization of movement of a high-speed railway transport in the Russian Federation".

3. Kovalev V.I. *Skorostnoy i vysokoskorostnoy zheleznodorozhny transport* [Speed and High-Speed Railway Transport], St. Petersburg, Vybor.

4. http://www.cnam.fr/(accessed 26 September 2016).

5. http://www.sncf.com/(accessed 26 September 2016).

6. Kiselev I.P. *Vysokoskorostnoy zheleznodorozhny transport. Obshchiy kurs* [High-Speed Railway Transport. General course], Moscow, UMC ZhDT, 2014.

7. Overview of the International Congress "Innovations And Staff in Railway Transport Geopolitics", June 17-18, 2015, St. Petersburg State Transport University of Emperor Alexander I, St. Petersburg, 2015.

8. Blazhko L.S., Kiselev I.P. The International Program of Additional Professional Education on a High-Speed Railway Transportat [Mezhdunarodnaya programma dopolnitelnogo professionalnogo obrazovaniya po vysokoskorostnomu zheleznodorozhnomu transportu], *Transport Rossiiskoy Federatsii [Transport of Russian Federation]*, 2015, no. 2 (57), pp. 19-25.

9. Blazhko L.S., Kiselev I.P. Preparation of Magisters in High-Speed Railway Transport as Part of the TEMPUS European Project [Podgotovkamagistrovvysokoskorostnogozheleznodorozhnogotransporta v ramkakh evropeyskogo proyekta TEMPUS], *Byulleten OSZHD [OSJD Bulletin]*, 2015, no. 4-5, pp. 18-25.

10. Kiselev I.P. High Schools Will Advance High-Speed Railway Projectsin Common [Vuzy budut sovmestno prodvigat proyekty VSM], *Gudok [Gudok]*, 2015, Dec. 17nd.

11. Magisters of High-Speed Railways [Magistry visokoskorostnykh magistraley], *Gudok [Gudok]*, 2015, Sept. 22nd.

12. Intelligent resource [Intellektualnyi resurs], *Gudok [Gudok]*, 2015, June 18nd.

13. Program of the 9th UIC World Congress on High Speed Rail, July 7-10, 2015, Tokyo Int. Forum, Tokyo, 2015.

14. UIC 9th World HSR Report, Speedlines, November 2015, no. 16, pp. 21-24.

15. Hosting the 9th UIC World Congress on High-speed rail, Japan Railway & Transport Review, March 2016, no. 67, pp. 36-47.

Метод анализа транспортной сети для выявления узких мест

Ахмедиярова А. Т., Утепбергенов И. Т., Касымова Д. Т.
Институт информационных и вычислительных технологий
Алматы, Казахстан
i.utepbergenov@gmail.com

Аннотация. **Разработан алгоритм расчета маршрута в городской транспортной сети, который по входным данным определяет возможность пропуска данного потока между двумя пунктами за время, не превышающее заданное, путем расчета времени проезда по альтернативным маршрутам. Алгоритм основан на определении кратчайшего пути в ориентированном мультиграфе. Также приведены результаты расчета для разных маршрутов, полученные с использованием разработанной программы.**

Ключевые слова: **дорожная сеть города, модель дорожной сети, потоковые данные, пропускная способность, перекресток, ориентированный мультиграф.**

Введение

Чтобы рационально организовать движение транспортных потоков, необходимо оценить максимальный поток в сети, найти наиболее эффективное распределение потока, выявить узкие места и своевременно ликвидировать их. Одновременно нужно оценить суммарные затраты времени транспортных средств при их движении из начального пункта в конечный.

Сегодня имеется обширная литература по изучению и моделированию автотранспортных потоков. Несколько академических журналов посвящены исключительно динамике автомобильного движения. Наиболее авторитетны Transportation Research, Transportation Science, Mathematical Computer Simulation, Operation Research, Automatica, Physical Review E, Physical Reports. Количество публикуемых статей исчисляется сотнями.

Вопросам разработки и исследования эффективности различных методов управления транспортными потоками (ТП), закономерностям их поведения на улично-дорожной сети (УДС) посвящены работы Д. Дрю, Х. Иносе, Т. Хамады, I. Gaishun, Т. Х. Кормена [1–4]. В последние десятилетия в России в практике управления потоками на улично-дорожной сети города накоплен значительный опыт, научные и методологические основы которого обобщены в работах В. В. Зырянова, В. Т. Капитанова, Г. И. Клинковштейна, Ю. А. Кременца, М. П. Печерского, М. В. Яшиной и других [5, 6]. Вопросам нахождения интегрального максимального потока транспортной сети мегаполиса посвящены работы Жогаля С. И., Максимея И. В., Зайченко Ю.П], Полякова К. Ю., Швецова В. И., Сукача Е. И. и других [7–11]. Анализ литературных источников по управлению транспортными потоками [1–6, 11, 12], аналитических моделей исследования операций [7, 8, 13] и теории автоматического управления [8, 9] позволил обосновать возможность применения имитационного моделирования для исследования динамики транспортных потоков региона [11, 14]. На основе данного анализа выявлена актуальность разработки алгоритма расчета маршрута в городской транспортной сети, который по входным данным определяет возможность пропуска данного потока между двумя пунктами за время, не превышающее заданное, путем расчета времени проезда по альтернативным маршрутам.

Постановка задачи

Требуется провести поток M из пункта S в пункт T за время, не превышающее Time. Если это невозможно сделать из-за пробок на дорогах, то выявить эти места и передать на выход. Скорость всех машин усреднена.

Для решения задачи вводятся следующие данные:

1) дорожная сеть города – дороги, перекрестки (обычные), перекрестки со светофорами, кольца;

2) параметры дороги:

а) $Pmax(i,j) \in R^+$ – максимальная пропускная способность дуги (i, j);

б) $Preal(i,j) \in R^+$ – реальный усредненный за период времени Time поток;

в) $zerotime(i,j) \in R^+$ – время прохождения дуги, если на ней нет ни одной машины;

3) $\delta \in (0,1)$ – светофорный параметр (для каждого перекрестка свой), обозначающий, какую часть времени какой свет горит (соответственно, другой свет горит $1 - \delta$ времени);

4) параметры кольца:

а) $Circle\_number \in Z^+$ – число входящих (исходящих) в кольцо дорог;

б) $Circlemax \in R^+$ – максимальная пропускная способность кольца;

в) $Circlereal.1, \ldots, Circlereal.Circle\_number \in R^+$ – реальные усреднённые за период времени Time потоки между 1-й исходящей дорогой и 2-й, между 2-й и 3-й, …, между Circle_number и 1-й;

г) $Circletime.1, \ldots, Circletime.Circle\_number \in R^+$ – по аналогии с zerotime(i, j) и Circlereal;

5) потоковые данные:

а) S – пункт отправки потока;

б) T – пункт принятия потока;

в) $M \in Z^+$ – величина потока (сколько машин подается в точку S);

г) $Time \in R^+$ – время, которое не должен превысить поток из S в T.

Теоретическая модель

В качестве модели используется ориентированный взвешенный мультиграф [4, 11, 12, 14]. Каждая дорога – это

дуга графа, каждый перекрёсток без светофора – вершина. Перекрёсток со светофором и кольцо – это более сложные конструкции, которые, тем не менее, приводятся к первым двум (дорога, перекрёсток без светофора) следующим образом [15, 16].

Перекрёсток со светофором. Изначально перекрёсток без светофора – обычная вершина (за исключением того, что ей приписан параметр δ), которая преобразуется в полный граф K_4, как показано на рис. 1.

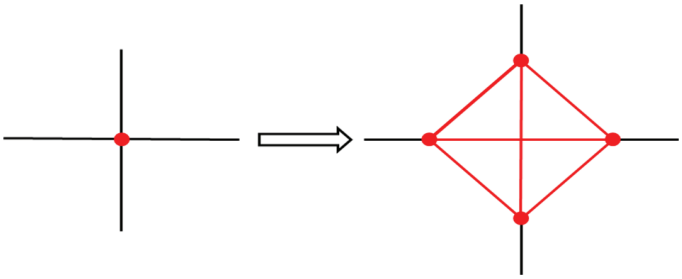


Рис. 1. Преобразование перекрёстка со светофором

Пропускная способность Pmax(i,j) каждой из этих шести дуг равна минимуму пропускной способности инцидентных основных дуг (не красного цвета) [15]. Так как светофор горит δ времени в одну сторону и (1 – δ) – в другую, то, соответственно, реальные пропускные способности будут δ · Pmax и (1 – δ) · Pmax (рис. 2).

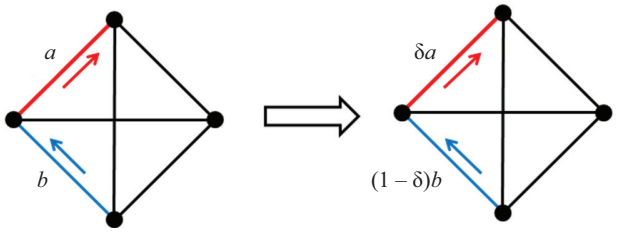


Рис. 2. Пояснение к преобразованию перекрёстка со светофором

Усредненный поток Preal(i,j) каждой дуги равен 0 (будем считать, что машины проходят перекресток мгновенно). Соответственно, zerotime (i,j) из предыдущего предположения тоже равен 0.

Кольцо. Пусть дано кольцо. Тогда его можно преобразовать под предлагаемую модель, как показано на рис. 3.

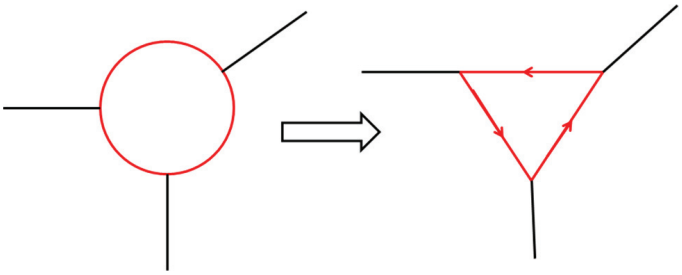


Рис. 3. Преобразование кольца

В результате получим структуру в рамках простых вершин и дуг. В качестве Pmax(i, j) берем Circlemax. В качестве Preal(i, i+1) и zerotime(i, i+1) берем Circlereal.i и Circletime.i, где рассматривается путь между i-й и i+1-й дорогами. Чтобы анализировать движение, нам еще потребуется специальная функция для расчета времени проезда единицы потока по данной дуге [7, 8].

Функция для расчета времени проезда выбранного маршрута. Предлагаемая функция время прохождения единицей потока данного участка (дуги) выглядит следующим образом:

$$h(i, j) = h(Pmax(i, j), Preal(i,j), zerotime(i,j)) \in R^{+}. \quad (1)$$

Она получает на вход пропускную способность дуги, усредненный поток и время, которое бы потребовалось единице потока, чтобы проехать по этой дуге, будь она пуста (нет других машин). Эта функция носит эмпирический характер и может задаваться многими способами. При реализации алгоритма была использована формула [9, 17]

$$h(i, j) = (1 + \frac{Preal(i, j)}{Pmax(i, j)})*zerotime(i, j). \quad (2)$$

Разработка алгоритмов и программ

Предлагаемый алгоритм по входным данным будет проверять возможность пропуска данного потока пунктами (из вершины S в вершину T) за время, не превышающее данное. Алгоритм на выходе будет либо выдавать, что поток проходит, либо – если это невозможно – выявлять пути (Memory.стоимость) и конкретные перекрёстки (список TrafficWay, по структуре аналогичный Memory.путь), на которых возникают заторы, мешающие успешному проезду заданного потока в заданное время.

Алгоритм TrafficWay

1 шаг. Используем алгоритм Mflow, в котором:

а) в качестве начального и конечного пунктов берем вершины S и T;

б) в качестве c_{ij} берем Pmax(i,j);

в) в качестве cost(i,j) берем h (Pmax(i,j), Preal(i,j), zerotime(i,j));

г) в качестве M берем Time.

2 шаг. Преобразуем полученный в предыдущем шаге список в

Memory.стоимость = round (Time – Memory.стоимость) + + 1.

Затем получаем F как сумму всех Memory.стоимость.

3 шаг. Полученный на втором шаге максимальный поток F сравниваем с M:

а) если M <= F, то на выходе алгоритм завершает работу с выводом «Успех»;

б) если M > F, то переходим к 4-му шагу.

4 шаг. Берем первый путь из списка Memory.путь и начинаем по нему идти:

а) берем первую дугу – переходим к пункту «б»;

б) сравниваем Preal(i,j) текущей дуги с суммой Pmax(j,k) всех исходящих из вершины дуг, в которую входит текущая. Если эта сумма больше, чем Preal(i,j) (на рис. 4 a < b + c + d), то переходим к следующей дуге, если такая существует, и повторяем пункт «б»; если не существует, то переходим к пункту «г»; если сумма меньше Preal(i,j), то переходим к пункту «в»;

в) если сумма оказалась меньше, то в список TrafficWay (в строку с номером, аналогичным номеру записи текущего пути в списке Memory.путь) заносим номер вершины, в которую входила текущая дуга;

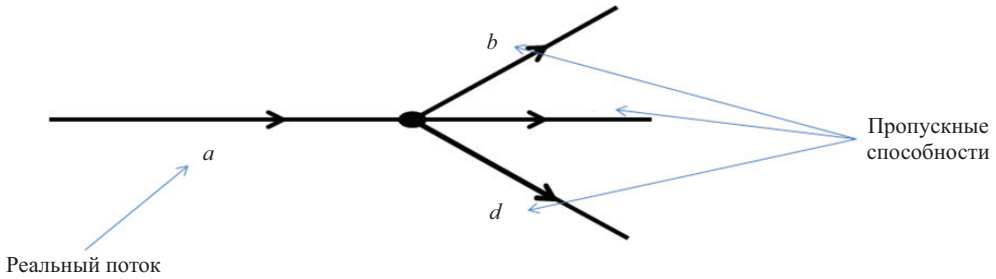


Рис. 4. Пояснение к шагу 4б

г) если следующей дуги в пути не существует, то переходим к шагу 5.

5 шаг. Берем следующий путь и переходим к шагу 4а. Если такого пути нет, то переходим к шагу 6.

6 шаг. Если TrafficWay пуст, то алгоритм завершает свою работу с выходом «Некорректные входные данные». Если TrafficWay содержит записи, то алгоритм также завершает работу и на выходе выдает два списка: Memory.путь – хранит пути и TrafficWay – хранит пробки.

Полученные алгоритмы были реализованы на языке C++. Главное меню программы показано на рис. 5. Входные данные берутся из текстового файла. Программа анализирует транспортную сеть на прохождение по ней потока (рис. 6), ищет пробки и предлагает короткий вариант маршрута.

Если поток не может пройти, то для получения результата, отражающего реальное состояние дорог, при решении связанных задач этот модуль должен быть использован в итеративной связке с другими (устранение пробок, построение развязок). В этом случае нужно, чтобы модуль, строящий развязки, перед подачей модулю, предложенному в данной работе, преобразовал развязку в вид, который понимает модель – обычные дуги, вершины и веса на них.

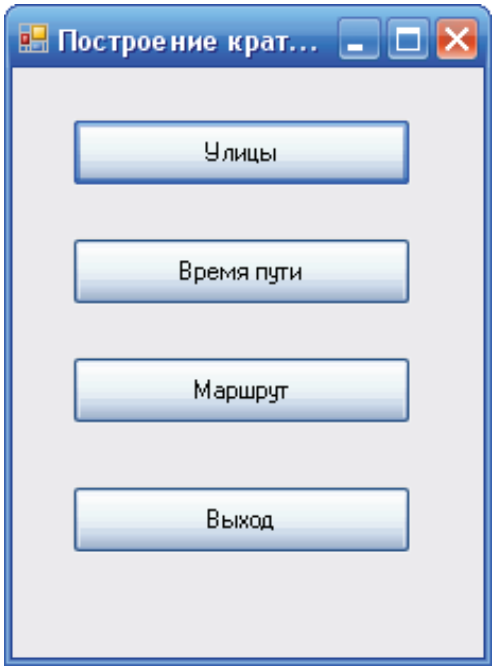


Рис. 5. Главное меню программы

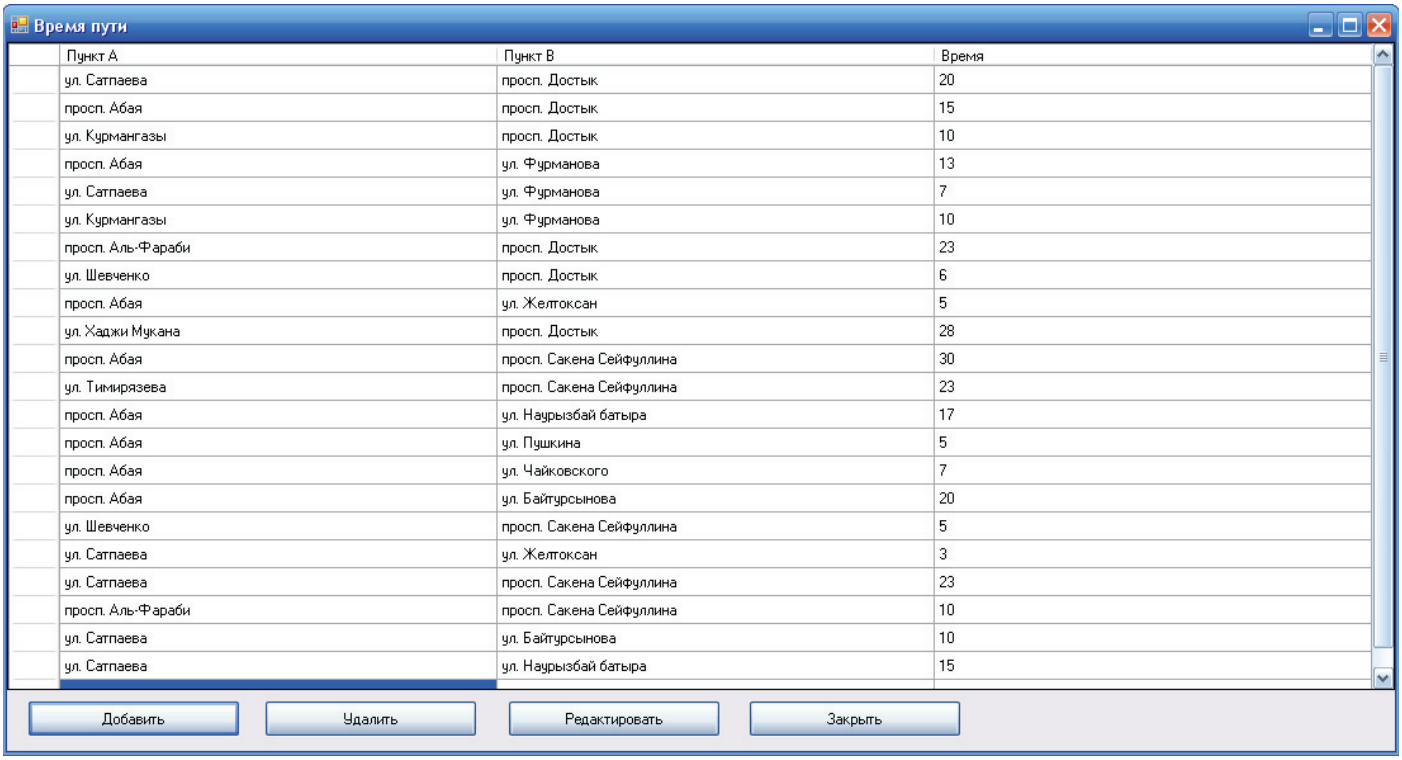


Рис. 6. Окно «Время пути»

Доказательство корректности алгоритма

Утверждение. Алгоритм TrafficWay корректен, его временна́я сложность O ($(n^2 + m^2)$ mC), где n – число вершин графа (V, E), m – число дуг, $C = \max\{Pmax_{ij}\}$.

Доказательство. Данный алгоритм работает по следующему принципу. Сначала он ищет поток, который можно в принципе пустить из пункта S в пункт T за время, не превосходящее Time (так как F был максимальный поток за единицу времени, то чтобы понять, сколько машин успеют пройти за время Time из S в T, нужно было взять Time минус время, потраченное на элементарном пути, плюс еще одна единица, которая успела доехать до T в последний момент), и после того, как нашел его, начинает проверку.

Если входной поток не превысил максимальный, то считаем, что он успевает благополучно пройти из S в T за время Time. Если превысил, то мы предполагаем, что на пути нашего потока встречаются заторы и начиная с четвертого шага начинаем искать их. Для этого поочередно берем пути из списка Memory.путь, который был сформирован еще при выполнении алгоритма Mflow, и по каждому из них идём и проверяем, чтобы реальный (усредненный) поток, входя в вершину, мог весь пройти сквозь нее, т. е. пропускные способности всех исходящих дуг позволяли ему это.

Если, пройдя по всем путям, мы не найдем пробок (TrafficWay будет пуст), то, скорее всего, входные данные (поток M или время Time) были заданы некорректно. Если же пробки найдены, то мы запоминаем с помощью TrafficWay, в каком пути и на каком узле они возникли, после чего передаем на выход эти два списка.

Вычислим временну́ю сложность данного алгоритма по шагам.

Выполнение алгоритма Mflow дает временну́ю сложность O ($(n^2 + m)$ mC). Изменение Memory.стоимость и затем суммирование занимает не более чем O (mC) операций. Далее, когда начинаем проверять все пути (не более чем mC) и на каждом пути сравниваем каждую дугу (не более чем m) с суммой исходящих (не более m), получаем O (m^3C). В итоге получаем O ($n^2mC + m^2C + mC + m^3C$) = O ($(n^2m + m^3 + m + m^2)C$) = O ($(n^2 + m^2)$ mC).

Утверждение доказано.

Вносится время, затрачиваемое на каждом перекрестке. Впоследствии данные используются для построения матрицы смежности.

Заключение

В результате исследования построены:

- алгоритм для определения кратчайшего пути в ориентированном мультиграфе;
- алгоритм Mflow для нахождения максимального потока, стоимость которого не превышает заданную;
- алгоритм TrafficWay для анализа транспортной сети и выявления на ней узких мест.

Доказана корректность алгоритма TrafficWay.

Полученные алгоритмы реализованы на языке C++.

Алгоритм TrafficWay только анализирует транспортную сеть на прохождение по ней потока и ищет пробки. Если поток не может пройти, то для получения результата, отражающего реальное состояние дорог, при решении связанных задач этот модуль должен быть использован в итеративной связке с другими.

Литература

1. Дрю Д. Теория транспортных потоков и управление ими / Д. Дрю. – М.: Транспорт, 1972. – 424 с.
2. Иносэ Х. Управление дорожным движением / Х. Иносэ, Т. Хамада. – М.: Транспорт, 1983. – 248 с.
3. Gaishun I. Investigation of Some Problems of Mathematical Systems Theory for Multistep Processes / I. Gaishun // J. Comput. Syst. Sci. Int. – 2005. – T. 44, Is. 2. – P. 163–166.
4. Кормен Т. Х. Алгоритмы : построение и анализ / Т. Х. Кормен. – 2-е изд. – М.: Вильямс, 2006. – 1296 с.
5. Капитанов В. Т. Управление транспортными потоками в городах / В. Т. Капитанов, Е. Б. Хилажев. – М.: Транспорт, 1985. – 94 с.
6. Клинковштейн Г. И. Организация дорожного движения : учеб. для вузов / Г. И. Клинковштейн. – 5-е изд., перераб. и доп. – М.: Транспорт, 2001. – 247 с.
7. Жогаль С. И. Задачи и модели исследования операций : учеб. пособие / С. И. Жогаль, И. В. Максимей. – Гомель: БелГУТ, 1999.
8. Зайченко Ю. П. Исследование операций : учеб. пособие / Ю. П. Зайченко. – Киев: Слово, 2002. – 320 с.
9. Поляков К. Ю. Теория автоматического управления / К. Ю. Поляков. – СПб., 2008. – С. 4–20.
10. Швецов В. И. Алгоритмы распределения транспортных потоков / В. И. Швецов // Автоматика и телемеханика. – 2009. – № 10. – С. 148–157.
11. Сукач Е. И. Применение имитационного моделирования для исследования динамики транспортных потоков региона / Е. И. Сукач // Изв. Гомел. гос. ун-та им. Ф. Скорины. – 2006. – № 4 (37). – С. 96–99.
12. Chudak F. The traffic equilibrium problem / F. Chudak, D. S. V. Eleuterio. – 2006.
13. Новиков Ф. А. Дискретная математика для программистов / Ф. А. Новиков. – 3-е изд. – СПб.: Питер, 2009. – 384 с.
14. Beckman M. Studies in the economics of transportation / M. Beckman, C. B. McGuire, C. B. Winsten. – CT: Yale Univ. Press, 1956.
15. Попков В. К. Математические модели связности / В. К. Попков. – Новосибирск: Изд-во ИВМиМГ СО РАН, 2006. – 409 с.
16. Фрэнк Г. Сети, связь и потоки / Г. Фрэнк, И. Фриш. – М.: Связь, 1978. – 448 с.
17. Sobol I. M. The Monte Carlo Method / I. M. Sobol. – Moscow: Nauka, 1968. – 64 p.

Problem of Transport Network Analysis for Identifying Bottlenecks

Ahmediyarova A. T., Utepbergenov I. T.,
Kassymova D. T.
Institute of Information and Computing Technologies,
Almaty, Kazakhstan
i.utepbergenov@gmail.com

Abstract: ***The analysis was done and an algorithm was developed for calculating a route in the urban transport network.*** **Based on the input data, this algorithm determines the capability to pass the given flow between two points during the time, not exceeding the given one, by calculating the travel time by alternative routes. The algorithm is based on the determination of the shortest path in the directed multigraph. The calculation results are given for different routes, obtained using the developed program.**

Keywords: **The road network of the city, Model of road network, Flow data, Bandwidth, Crossroads, A directed multigraph.**

References

1. Dryu D. Teoriya transportnyih potokov i upravlenie imi, Moscow, Transport, 1972, 424 p.

2. Inose H., Hamada T. Upravlenie dorozhnyim dvizhe-niem. Moscow, Transport, 1983, 248 p.

3. Gaishun I. Investigation of Some Problems of Mathematical Systems Theory for Multistep Processes, *J. Comput. Syst. Sci. Int.*, 2005, T. 44, Is. 2, pp. 163-166.

4. Kormen T. H. Algoritmyi: postroenie i ana-liz. Moscow, Vilyams, 2006, 1296 p.

5. Kapitanov V. T., Hilazhev E. B. Upravlenie trans-portnyimi potokami v gorodah, Moscow, Transport, 1985, 94 p.

6. Klinkovshteyn G. I. Organizatsiya dorozhnogo dvi-zheniya. Uchebnik dlya vuzov, Moscow, Transport, 2001, 247 p.

7. Zhogal S. I., Maksimey I. V. Zadachi i modeli is-sledovaniya operatsiy. Uchebnoe posobie, Gomel, Bel-GUT, 1999.

8. Zaychenko Yu. P. Issledovanie operatsiy. Kiev, Slovo, 2002, 320 p.

9. Polyakov K.Yu. Teoriya avtomaticheskogo upravleniya. St. Peterburg, 2008, pp. 4-20.

10. Shvetsov V. I. Algoritmyi raspredeleniya trans-portnyih potokov, *Automatics and telemechanics [Avtomatika i telemehanika]*, 2009, no. 10, pp. 148-157.

11. Sukach E. I. Primenenie imitatsionnogo modeliro-vaniya dlya issledovaniya dinamiki transportnyih potokov regiona, *Izvestiya Gomelskogo gosudarstvennogo univer-siteta imeni F. Skorinyi*, 2006, no. 4 (37), pp. 96-99.

12. Chudak F., Eleuterio D. S. V. The traffic equilibrium problem. 2006.

13. Novikov F. A. Diskretnaya matematika dlya programmistov. St. Peterburg, Piter, 2009, 384 p.

14. Beckman M., McGuire C. B., Winsten C. B. Studies in the economics of transportation. CT, Yale Univ. Press, 1956.

15. Popkov V. K. Matematicheskie modeli svyaznosti, Novosibirsk, Izdatelstvo IVMiMG SO RAN, 2006, 409 p.

16. Frenk G., Frish I. Seti, svyaz i potoki. Moscow, Svyaz, 1978, 448 p.

17. Sobol I. M. The Monte Carlo method. Moscow, Nauka, 1968, 64 p.

Многокритериальное управление вагонами на железнодорожном транспорте

Дегтярев В. Г., Ходаковский В. А.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
vdegt@list.ru, hva1104@mail.ru

Аннотация. **В работе рассматриваются методы многокритериального управления вагонами на железнодорожном транспорте: главного элемента, уступок, линейной связки. Эти методы основаны на способах решения транспортной задачи линейного программирования – на методе потенциалов и т. д., а также на методе решения транспортной задачи по критерию времени с нелинейной целевой функцией. Такие подходы к управлению вагонами на железнодорожном транспорте применены впервые. Также в работе предложен новый метод решения задач оптимизации, не уступающий другим по быстродействию и числу итераций.**

Ключевые слова: **целевая функция, критерий оптимальности, управление вагонами, транспортная задача.**

Введение

Методы оптимального управления впервые приложены к решению задач по перемещению железнодорожных вагонов достаточно давно, еще в советское время [1]. Однако тогда это касалось, в первую очередь, подачи порожних вагонов в места их погрузки. Учитывая большую протяженность железных дорог СССР и весьма интенсивные железнодорожные перевозки по всей территории огромной страны, решение этой задачи давало большой экономический выигрыш.

Интерес к этой проблеме возник вновь с капитализацией железных дорог, разделом вагонного парка бывшего СССР между Россией, странами СНГ и Балтии [2] и вызванными этим новыми проблемами. Эти проблемы были связаны как с самим фактом раздела железнодорожного парка между странами и, как следствие, с появлением на железных дорогах России вагонов стран СНГ и Балтии, так и с эксплуатацией вагонов частных компаний. В какой-то мере эти проблемы были решены в работах [3–8]. Следует отметить, что во всех этих работах использовался один критерий оптимальности управления вагонами – стоимости.

В наших работах [6–8] в качестве примеров рассматривались перевозки массовых товаров (леса, нефти, руды и т. д.) из мест их добычи или обработки в места потребления. Так, в пособиях [8, 9] приводятся примеры о перевозке леса из северо-западного региона России в Москву, Одессу и т. д. Стоимость перевозки в основном зависит от расстояния между пунктами отправления и назначения и от некоторых других характеристик, рассчитывается на основе правил, задаваемых ОАО «РЖД». В дальнейшем рассматривались разные варианты постановки и решения транспортной задачи линейного программирования (ЛП) [10–15]. Известны также работы иностранных авторов [16–18].

Математическая постановка задачи

Пусть в пунктах $A_1, A_2, ..., A_m$ находятся вагоны, порожние или с грузами, предназначенные к отправке в пункты $B_1, B_2, ..., B_n$. При этом в пункте A_i находится, соответственно, a_i вагонов. Эти вагоны должны быть поданы в пункты $B_1, B_2, ..., B_n$, причем заявки этих пунктов составляют, соответственно, $b_1, b_2, ..., b_n$ вагонов. В общем случае исходными данными являются: $a_1, a_2, ..., a_m$; $b_1, b_2, ..., b_n$ и другие необходимые для решения задачи данные, например, стоимость перемещения вагонов C_{ij}, время перемещения вагонов t_{ij} и т. д. Транспортная задача по критерию стоимости формулируется следующим образом:

$$\begin{gathered} f_1(X) = \sum_{i=0}^{m}\sum_{j=0}^{n} C_{i,j} X_{i,j} \to \min; \\ \sum_{i=0}^{m} X_{i,j} = a_i; \quad i = 1,2\ldots,m; \\ \sum_{j=0}^{n} X_{i,j} = b_j; \quad j = 1,2\ldots,n; \\ \sum_{i=0}^{m} a_i = \sum_{j=0}^{n} b_j. \end{gathered} \tag{1}$$

Переменная x_{ij} – количество вагонов, перемещаемых из пункта A_i в пункт B_j; матрица X – матрица с элементами x_{ij}. Целевая функция (критерий) $f_1(X)$ – суммарная стоимость перемещения всех вагонов из всех пунктов отправления A_i во все пункты назначения B_j.

Аналогичная транспортная задача по критерию времени имеет вид

$$\begin{gathered} f_2(X) = T = \max_{i,j} t_{i,j} \to \min; \\ \sum_{i=0}^{m} X_{i,j} = a_i; \quad i = 1,2,\ldots,m; \\ \sum_{j=0}^{n} X_{i,j} = b_j; \quad j = 1,2,\ldots,n; \\ \sum_{i=0}^{m} a_i = \sum_{j=0}^{n} b_j. \end{gathered} \tag{2}$$

Целевая функция (критерий) $f_2(X)$ – минимальное время, за которое вагоны перемещаются из всех возможных пунктов отправления A_i во все возможные пункты назначения B_j. Задача (1) является частным случаем задачи ЛП, для нее

разработаны специальные методы решения, более эффективные, чем методы решения любых задач ЛП. Кроме того, в силу специфики задачи (1) размещение исходной информации в памяти компьютера для нее может быть более экономно, чем для задачи ЛП. Короче говоря, решение задачи (1) методами решения транспортных задач более эффективно, чем их решение методами решения задач ЛП.

Задача (2) не является задачей линейного программирования из-за нелинейности целевой функции $f_2(X)$. Однако для решения подобных задач разработаны свои специфические методы. Переходим к задачам многокритериальной оптимизации. Исходная задача многокритериального математического программирования может быть записана в виде

$$\min\{f_1(X) = y_1\}, \min\{f_2(X) = y_2\}, ..., \min\{f_k(X) = y_k\};$$

$$X \in D,$$

где D – область допустимых решений. Существенное отличие этой задачи от традиционной однокритериальной состоит в понятии оптимальности. В однокритериальной задаче под оптимальным понимается решение, обеспечивающее минимальное значение этого одного критерия.

При многих критериях уменьшение одних критериев приводит к увеличению других (редкие исключения не представляют практического интереса), поэтому понятие оптимальности требует принципиальных уточнений. Очевидно, что без дополнительной информации о предпочтениях лица, принимающего решение (ЛПР), бессмысленно говорить об оптимальном решении, тем более, искать его.

Существуют различные формулировки оптимальности в соответствии с конкретными условиями в тех или иных ситуациях. Рассмотрим две ситуации: 1) ЛПР выражает свои предпочтения до начала процесса многокритериальной оптимизации; 2) интерактивное взаимодействие ЛПР с процессом (лицом или лицами) реализации многокритериальной оптимизации.

В первом случае ЛПР может выразить свои предпочтения в различной форме в зависимости от особенностей самого ЛПР, новизны задачи, типа и числа критериев и других факторов, поэтому методы данной группы используют разные представления предпочтений и способы их формализации. Однако все они в конечном итоге сводят многокритериальную задачу к одной или к ряду задач с одним (иногда обобщенным) критерием.

Во втором случае интерактивный процесс решения многокритериальной задачи реализуется путем диалога ЛПР с компьютером. При этом чередуются этапы вычислений, выполняемых компьютером, и корректировки и принятия решений ЛПР. Такая процедура позволяет ЛПР более полно и глубоко оценить взаимосвязь критериев и возможности оптимизируемой системы. Более того, в интерактивном процессе может развиваться формирование предпочтений, компромиссов и даже системы ценностей. Все это облегчает ЛПР нахождение решения, наилучшего с его точки зрения, и повышает уверенность в правильности выбора, поэтому такая технология оказывается более реалистичной, гибкой и приемлемой для руководителей.

Для каждого из этих случаев рассмотрим по одному методу постановки задачи многокритериальной оптимизации. Для первого случая рассмотрим метод главного критерия. Суть метода состоит в том, что ЛПР выделяет главный критерий (далее – $f_1(X)$), а на остальные критерии накладывает требования, чтобы они были не больше задаваемых им пороговых значений t_i. Тогда многокритериальная задача сводится к однокритериальной задаче:

$$f_1(X) \to \min, f_i(X) \le t_i;\ i = 2, 3, ..., m;\ X \in D.$$

Для второго случая рассмотрим метод уступок. Предварительно ЛПР ранжирует критерии по важности. В результате критериям присваиваются номера в порядке убывания важности. После этого начинается основная часть диалога. Решается задача минимизации первого критерия при $X \in D$. Если задача имеет множество оптимальных решений, то на нем ищется решение, наилучшее по второму критерию. Если и оно не единственно, то включается третий критерий, и так до достижения единственного решения.

Иначе говоря, находится лексикографически-оптимальное решение. ЛПР предъявляется полученное решение X^1 со значениями всех критериев. ЛПР анализирует это решение, и если оно его не устраивает, диалог продолжается. ЛПР просят указать, на какую величину он согласен снизить значение первого критерия с тем, чтобы улучшить значение второго. В результате формируется новая задача:

$$f_2(X) \to \min;$$

$$f_1(X) \le f_1 + \Delta_1;\ X \in D, \qquad (3)$$

где Δ_1 – уступка по первому критерию. Снова ищется лексикографическое решение, начиная с задачи (3), и так далее.

Алгоритм решения задачи (на примере)

В табл. 1 в столбце «Запасы» и в строке «Заявки» указаны, соответственно, число вагонов, имеющихся в пунктах отправления $A_i - a_i$, и число вагонов, заявленных в пункты назначения $B_j - b_j$ (числа выделены полужирным шрифтом). Цифры в левом верхнем углу каждой клетки указывают стоимость перевозки вагонов C_{ij} из пункта A_i в пункт B_j, а цифры в правом нижнем углу – время перевозки t_{ij}. Вначале для этого примера решим задачу оптимального управления вагонами по критерию стоимости (1) и задачу оптимального управления по критерию времени (2). Начнем с задачи (1): оставим в табл. 1 только информацию, относящуюся к этой задаче (табл. 2).

Таблица 1

Исходные данные примера

A_i \ B_j	B_1	B_2	B_3	B_4	B_5	Запасы
A_1	40 13	35 8	24 5	27 9	30 10	**25**
A_2	22 8	25 10	25 9	24 11	36 12	**34**
A_3	16 12	30 10	25 8	30 7	18 6	**42**
A_4	44 9	18 7	20 10	32 12	34 8	**23**
Заявки	**21**	**37**	**40**	**11**	**15**	

Таблица 2

Исходные данные по критерию стоимости

A_i \ B_j	B_1	B_2	B_3	B_4	B_5	Запасы
A_1	40	35	24 **25**	27	30	**25**
A_2	22 **21**→	25 **2**↓	25	24 **11**	36	**34**
A_3	16 ↑	30 ←**12**	25 **15**	30	18 **15**	**42**
A_4	44	18 **23**	20	32	34	**23**
Заявки	**21**	**37**	**40**	**11**	**15**	

Для решения транспортной задачи сперва необходимо построить начальный базисный план. Его можно построить методом наименьшей стоимости по строчкам табл. 2 (цифрам, выделенным полужирным шрифтом, в центре клеток). Стоимость всех перевозок в соответствии с этим базисным планом

$$f_1(X) = 24 \cdot 25 + 22 \cdot 21 + 25 \cdot 2 + 24 \cdot 11 + \\ + 30 \cdot 12 + 25 \cdot 15 + 18 \cdot 15 + 18 \cdot 23 = 2795.$$

Для проверки оптимальности этого базисного плана или его улучшения применим наиболее популярный среди специалистов метод потенциалов. Обозначим через v_j потенциалы пунктов назначения B_j, а через u_i – потенциал пунктов отправления. Уравнения для потенциала, составленные на основе базисных клеток табл. 2, имеют вид

$$v_3 - u_1 = 24;\ v_1 - u_2 = 22;\ v_2 - u_2 = 25;\ v_4 - u_2 = 24; \\ v_2 - u_3 = 30;\ v_3 - u_3 = 25;\ v_5 - u_3 = 18;\ v_2 - u_4 = 18. \quad (4)$$

Эта система уравнений имеет одну избыточную переменную, т. е. одну из переменных можно выбрать произвольно (не нарушая единственности значений остальных переменных). Выберем $u_1 = 0$, тогда остальные переменные вычисляются по системе (4):

$$v_3 = 24;\ u_3 = -1;\ v_2 = 29;\ v_5 = 17;$$

$$u_2 = 4;\ v_1 = 26;\ v_4 = 28;\ u_4 = 11.$$

Это позволяет на основе свободных клеток вычислить псевдостоимость: $C_{ij}^* = v_j - u_i$. Они составят: $C_{11}^* = 26$; $C_{12}^* = 29$; $C_{14}^* = 28$; $C_{15}^* = 17$; $C_{23}^* = 20$; $C_{25}^* = 13$; $C_{31}^* = 27$; $C_{34}^* = 29$; $C_{41}^* = 15$; $C_{43}^* = 13$; $C_{44}^* = 17$; $C_{45}^* = 8$.

Условие оптимальности базисного плана имеет вид $C_{ij}^* \le C_{ij}$ (для всех свободных клеток).

В нашем случае это условие выполняется для всех клеток, кроме клеток (1,4) и (3,1). Следовательно, план не является оптимальным, его можно улучшить путем циклической перестановки на основе одной из этих двух клеток. Организуем цикл перемещения на базе свободной клетки (3,1): переместим 12 единиц из клетки (3,2) в клетку (3,1), а для соблюдения баланса – 12 единиц из клетки (2,1) в клетку (2,2).

Этот процесс отражен в табл. 2 стрелками. Получим новый базисный план: $x_{11} = 0$, $x_{12} = 0$, $x_{13} = 25$, $x_{14} = 0$, $x_{15} = 0$, $x_{21} = 9$, $x_{22} = 14$, $x_{23} = 0$, $x_{24} = 11$, $x_{25} = 0$, $x_{31} = 12$, $x_{32} = 0$, $x_{33} = 15$, $x_{34} = 0$, $x_{35} = 15$, $x_{41} = 0$, $x_{42} = 23$, $x_{43} = 0$, $x_{44} = 0$, $x_{45} = 0$. Для этого базисного плана стоимость равна

$$f_1(X) = 24 \cdot 25 + 22 \cdot 9 + 25 \cdot 14 + 24 \cdot 11 + 16 \cdot 12 + 25 \cdot 15 + \\ + 18 \cdot 15 + 18 \cdot 23 = 2663.$$

Как видно, план действительно лучше предыдущего. Проделав еще несколько шагов, получим оптимальный план (в нашем случае – план, соответствующий минимальной стоимости перевозок $X_{\text{стоим}}^{\min}$):

$$X_{\text{стоим}}^{\min} = \begin{pmatrix} 0 & 0 & 25 & 0 & 0 \\ 0 & 14 & 9 & 11 & 0 \\ 21 & 0 & 6 & 0 & 15 \\ 0 & 23 & 0 & 0 & 0 \end{pmatrix}.$$

Для этого плана все условия оптимальности выполняются, а стоимость перевозок $f_1(X_{\text{стоим}}^{\min}) = 2609$.

Переходим к решению задачи по критерию времени. Сохраним в табл. 1 только информацию, относящуюся к этой задаче (табл. 3).

Таблица 3

Исходные данные по критерию времени

A_i \ B_j	B_1	B_2	B_3	B_4	B_5	Запасы
A_1	● 13	8	**25** 5	9	● 10	**25**
A_2	**21** 8	● 10	**13** 9	● 11	● 12	**34**
A_3	● 12	**14** 10	**2** 8	**11** 7	**15** 6	**42**
A_4	9	**23** 7	● 10	● 12	8	**23**
Заявки	**21**	**37**	**40**	**11**	**15**	

Будем решать задачу методом запрещенных клеток. Начальный базисный план задан цифрами, стоящими в верхнем центре клеток и отмеченными полужирным шрифтом. На этом плане наибольшее время $f_2(X) = 10$ и соответствует клетке (3,2).

Попробуем улучшить этот базисный план. Для этого «запретим» перевозки, соответствующие клеткам со временем перевозок ≥ 10. «Запрещенные» клетки помечены символом ●. Для улучшения базисного плана необходимо переместить 14 единиц из клетки (3,2) в другие клетки с меньшим временем перевозки. Этот план улучшить уже невозможно, так как 14 единиц в клетке (3,2), соответствующей максимальному времени 10, невозможно переместить ни в одну клетку с меньшим временем. Итак, оптимальный план по критерию времени ($X_{\text{врем}}^{\min}$) имеет вид

$$X_{\text{врем}}^{\min} = \begin{pmatrix} 0 & 0 & 25 & 0 & 0 \\ 21 & 0 & 13 & 0 & 0 \\ 0 & 14 & 2 & 11 & 15 \\ 0 & 23 & 0 & 0 & 0 \end{pmatrix}.$$

Минимальное время перевозки $f_2(X_{\text{врем}}^{\min}) = 10$.

Как видим, эти два оптимальных плана (по критерию стоимости и по критерию времени) не совпадают. Оценим каждый план с позиций противоположного критерия: $f_1(X_{\text{врем}}^{\min}) = 2871$, что на 10% хуже, чем для $X_{\text{стоим}}^{\min}$; $f_2(X_{\text{совокуп}}^{\min}) = 12$, что на 20% хуже, чем для $X_{\text{врем}}^{\min}$. Ни тот, ни другой вариант может не устроить ЛПР в качестве выбранного им решения, и он захочет рассмотреть какие-то компромиссные варианты. Для этого и служат методы многокритериальной оптимизации.

Сначала применим к этой задаче метод главного элемента. Пусть главным будет критерий стоимости $f_1(X)$ (для железнодорожного транспорта, впрочем, как и для всей российской экономики, это типично), а в качестве порогового значения по второму критерию ЛПР установил величину, равную 11 единицам времени.

Тогда в соответствии с методом главного критерия задача многокритериальной оптимизации формулируется как задача однокритериальной оптимизации:

$$f_1(X) \to \min, f_2(X) \le 11; X \in D.$$

Решая эту задачу и обозначая ее решение через $X^{\min}_{\text{совокуп}}$, получим $X^{\min}_{\text{совокуп}} = \{x_{11}= 0, x_{12}= 0, x_{13}= 25, x_{14}= 0, x_{15}= 0, x_{21}= 21, x_{22}= 2, x_{23}= 0, x_{24}= 11, x_{25}= 0, x_{31}= 0, x_{32}= 12, x_{33}= 15, x_{34}= 0, x_{35}= 15, x_{41}= 0, x_{42}= 23, x_{43}= 0, x_{44}= 0, x_{45}= 0\}$. Для этого плана значения критериев будут равны: $f_1(X^{\min}_{\text{совокуп}}) = 2795$, что лишь на 7% хуже абсолютно оптимального по стоимости; $f_2(X^{\min}_{\text{совокуп}}) = 11$, что лишь на 10% хуже абсолютно оптимального по времени. Таким образом, в совокупности решение $X^{\min}_{\text{совокуп}}$ является лучшим по сравнению и с $X^{\min}_{\text{врем}}$, и с $X^{\min}_{\text{совокуп}}$, так как, не будучи абсолютно оптимальным по каждому из них, оно ближе всего расположено и к тому, и к другому.

Аналогичным образом решается задача многокритериальной оптимизации по методу уступок. Разница состоит лишь в том, что в методе главного критерия ЛПР делает уступки по всем критериям, кроме главного (увеличение $f_1(X)$ в данном примере произошло не потому, что так хотел ЛПР, а потому, что он уступил по второму критерию), а в методе уступок уступки чередуются по всем критериям.

Еще один метод решения

Мы предлагаем еще один метод решения оптимизационных задач подобного типа. Проще всего излагать этот метод на том же конкретном примере оптимального управления вагонами по критерию стоимости, который рассмотрен выше. Исходя из табл. 2, начало алгоритма в пошаговом режиме может выглядеть следующим образом.

1 шаг. Наименьшая стоимость (16) находится в ячейке (3,1), это ячейка первого шага, в нее помещаем наименьшую величину из 21 (первый элемент вектора B) и 42 (первый элемент вектора A), т. е. значение равно **21**.

2 шаг. Второе по величине значение стоимости (18) находится в ячейке (4,2), куда помещаем наименьшую из величин 37 (второй элемент вектора B) и 23 (четвертый элемент вектора A), т. е. итоговое значение равно **23**.

3 шаг. Третье по величине значение стоимости (также 18) находится в ячейке (3,5), куда помещаем наименьшую из величин 15 (пятый элемент вектора B) и 42 (третий элемент вектора A), т. е. итоговое значение **15**.

4 шаг. Четвертое по величине значение стоимости (20) расположено в ячейке (4,3), помещаем здесь наименьшее значение из величин (40–0, так как в третьем столбце все элементы плана все еще равны нулю) и (23–23, поскольку в четвертой строке уже имеется план 23 во втором столбце), итоговое значение **0**.

Далее, поступая аналогично, совершаем еще 4 шага до получения опорного плана.

Требуется минимизировать линейную целевую функцию $f_1(X) = \sum\sum C_{ij}x_{ij}$, которая является суммой всех поэлементных произведений матрицы стоимости C и матрицы плана перевозок X. Для минимизации целевой функции превратим в ней двойное суммирование в суммирование по одному индексу, преобразовав матрицы в векторы путем построчного прочтения матриц:

$$F(Y) = \sum_{k=1}^{mn} \hat{C}_k Y_k,\ \hat{C}_k = sort(V_k);\ V_{k=j+mi} = X_{ij}. \qquad (5)$$

Для минимизации целевой функции (5) необходимо минимизировать затраты на каждом шаге, а значит, выбрать максимальное количество дешевых перевозок, но с учетом ограничений. В пределе, если позволяют ограничения, нужно выбрать только ту перевозку, которая имеет минимальную стоимость. Для доказательства этого утверждения целевую функцию (5) можно записать так:

$$F(X) = a_1x_1 + a_2x_2 + \ldots + a_kx_k \to \min.$$

Тогда если $a_1 \le a_2 \le \ldots a_k$, то для минимизации необходимо обеспечить:

$$x_k = \max(X^k \in D) \le x_{k-1} = \max(X^{k-1} \in D) \le \ldots \le x_1 = \max(X^1 \in D).$$

Следовательно, для решения поставленной задачи необходимо отсортировать вектор стоимости $\hat{C}_k$ в порядке возрастания элементов с запоминанием столбца и строки, где стоял элемент матрицы стоимости до сортировки.

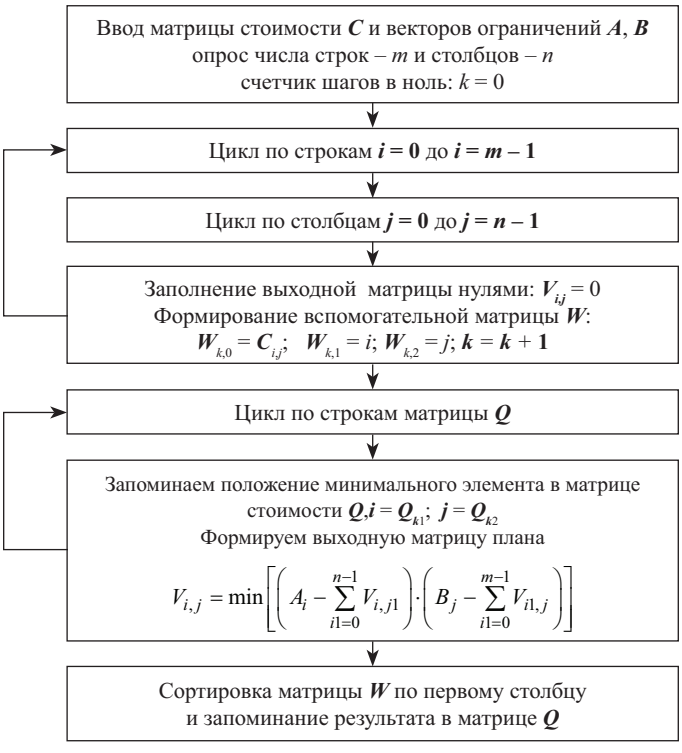
Целевая функция (5) достигнет минимума, если, выбирая стоимость $\hat{C}_k$ начиная с минимальной, определять на каждом k-м шаге такой элемент плана X^k_{ij}, чтобы его значение было максимально возможным, но не превышало ограничений, заданных векторами $\boldsymbol{A}$ и $\boldsymbol{B}$:

$$X^k_{ij} = \min(A_i - \sum_j X^{k-1}_{ij},\ B_j - \sum_i X^{k-1}_{ij}). \qquad (6)$$

Верхний индекс в X^k_{ij} в формуле (6) означает номер шага.

Результаты расчетов в среде Mathcad

Ниже приведен алгоритм оптимизации перевозок по критерию стоимости.



Ниже приведена программа для MathCAD, реализующая приведенный алгоритм.

```
Opt(C, A, B) := | m ← rows(C)
                | n ← cols(C)
                | k ← 0
                | for i ∈ 0..m − 1
                |   for j ∈ 0..n − 1
                |     V_{i,j} ← 0
                |     W_{k,0} ← C_{i,j}
                |     W_{k,1} ← i
                |     W_{k,2} ← j
                |     k ← k + 1
                | Q ← csort(W, 0)
                | for k ∈ 0..m·n − 1
                |   i ← Q_{k,1}
                |   j ← Q_{k,2}
                |   V_{i,j} ← min[(A_i − Σ_{j1=0}^{n−1} V_{i,j1}), (B_j − Σ_{i1=0}^{m−1} V_{i1,j})]
                | V
```

Результаты расчетов на Mathcad

Матрица стоимости

$$C := \begin{pmatrix} 40 & 35 & 24 & 27 & 30 \\ 22 & 25 & 25 & 24 & 36 \\ 16 & 30 & 25 & 30 & 18 \\ 44 & 18 & 20 & 32 & 34 \end{pmatrix}$$

Матрица времени

$$T := \begin{pmatrix} 13 & 8 & 5 & 9 & 10 \\ 8 & 10 & 9 & 11 & 12 \\ 12 & 10 & 8 & 7 & 6 \\ 9 & 7 & 10 & 12 & 8 \end{pmatrix}$$

Начальный план

$$X := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 8 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

m := rows(C) n := cols(C) m = 4 n = 5

Целевая функция по стоимости

$$F1(X) := \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(C_{i,j} \cdot X_{i,j}\right)$$

F1(X) = 555

Целевая функция по времени

$$F2(X) := \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(T_{i,j} \cdot X_{i,j}\right)$$

F2(X) = 184

$$optzena = \begin{pmatrix} 0 & 0 & 25 & 0 & 0 \\ 0 & 14 & 9 & 11 & 0 \\ 21 & 0 & 6 & 0 & 15 \\ 0 & 23 & 0 & 0 & 0 \end{pmatrix}$$

$$optvrem = \begin{pmatrix} 0 & 0 & 25 & 0 & 0 \\ 21 & 13 & 0 & 0 & 0 \\ 0 & 1 & 15 & 11 & 15 \\ 0 & 23 & 0 & 0 & 0 \end{pmatrix}$$

В этих обозначениях матрица optzena соответствует матрице $X^{\min}_{\text{стоим}}$, а матрица optvrem – матрице $X^{\min}_{\text{врем}}$. Как видно, результаты для критерия стоимости по этому методу полностью совпадают с результатами по методу потенциалов. Что же касается критерия времени, то результаты здесь разные, но значения целевых функций также совпадают. Дело в том, что транспортная задача может иметь несколько одинаково оптимальных решений.

Заключение

Многокритериальное управление вагонами на железнодорожном транспорте, насколько нам известно, ранее в научной литературе не рассматривалось. Между тем, такие проблемы могут возникнуть, по крайней мере, по отношению к двум основным в этой отрасли критериям – стоимости и времени. В этой статье такая задача решена. Естественно, для многокритериального управления необходимо знать решение по каждому из критериев отдельно. По критерию стоимости оптимальное управление находится методом потенциалов, по критерию времени – методом запрещенных клеток; компромиссное общее решение – по методу главного элемента.

Примеры показывают, что это компромиссное решение дает результат, позволяющий иметь значения отдельных критериев, достаточно близкие к оптимальным. Иначе говоря, общее оптимальное решение является почти оптимальным по каждому из критериев.

Этот результат можно применять к реальным ситуациям. Критерий стоимости, конечно, является основным при планировании перевозок. Однако в ряде случаев необходимо выполнять перевозки в кратчайшее время, например, скоропортящихся грузов или при доставке грузов в районы боевых действий, когда этот фактор может решать успешность боевых операций, и т. д.

Литература

1. Нестеров Е. П. Транспортные задачи линейного программирования / Е. П. Нестеров. – М.: Транспорт, 1971. – 216 с.

2. Правила эксплуатации, пономерного учета и расчетов за пользование грузовыми вагонами собственности других государств (утв. 24.05.1996 г.). – М.: Марикор, 1996.

3. Гертвальд А. С. Автоматизация планирования резерва вагонов в местах погрузки / А. С. Гертвальд, Л. А. Канарская, Н. Б. Соколов // Вестн. ВНИИЖТа. – 1999. – № 2. – С. 3–8.

4. Тишкин Е. М. Автоматизация управления вагонным парком / Е. М. Тишкин. – М.: Интекст, 2000. – 224 с.

5. Ивницкий В. А. Динамическая оптимизация обеспечения намечаемой погрузки погрузочными ресурсами / В. А. Ивницкий, В. А. Буянов, Н. Б. Соколов // Вестн. ВНИИЖТа. – 2000. – № 5. – С. 28–31.

6. Ковалев В. И. Оптимальное по стоимости управление вагонопотоками с учетом наличия в рабочем парке вагонов как принадлежащих России, так и странам СНГ и Балтии / В. И. Ковалев, В. Г. Дегтярев, С. Ю. Елисеев, А. Т. Осьминин // Вестн. ВНИИЖТа. – 2002. – Вып. 3. – С. 7–11.

7. Ковалев В. И. О моделировании процессов управления вагонопотоками с учетом вагонов других государств / В. И. Ковалев, В. Г. Дегтярев, С. Ю. Елисеев // Изв. ПГУПС. – 2004. – Вып. 2. – С. 16–19.

8. Ковалев В. И. Управление парками вагонов стран СНГ и Балтии на железных дорогах России: учеб. пособие / В. И. Ковалев, С. Ю. Елисеев, В. Г. Дегтярев и др. – М.: Маршрут, 2006. – 243 с.

9. Дегтярев В. Г. Математическое моделирование : учеб. пособие / В. Г. Дегтярев. – СПб.: ПГУПС, 2011. – 105 с.

10. Дегтярев В. Г. Стохастическая транспортная задача по критерию времени / В. Г. Дегтярев, О. Жгун, В. Н. Фоменко // Труды конф. «Математика в вузе». – СПб.: ПГУПС, 2002. – С. 160–162.

11. Дегтярев В. Г. Стохастическая транспортная задача по критерию времени с зависимыми параметрами / В. Г. Дегтярев, О. Жгун, В. Н. Фоменко // Труды конф. «Математика в вузе». – СПб.: ПГУПС, 2003. – С. 144–145.

12. Дегтярев В. Г. Об одном способе решения стохастической транспортной задачи по критерию времени В. Г. Дегтярев, О. Жгун, В. Н. Фоменко // Труды конф. «Математика в вузе». – СПб.: ПГУПС, 2003. – С. 146–147.

13. Дегтярев В. Г. Применение методов транспортной задачи для оптимального регулирования вагонов различных форм собственности / В. Г. Дегтярев // Сб. трудов «Проблемы математической и естественнонаучной подготовки в инженерном образовании». – СПб.: ФГБОУ ВПО ПГУПС, 2013. – С. 66–71.

14. Дегтярев В. Г. Оптимальное управление порожними вагонами различных форм собственности / В. Г. Дегтярев // Труды конф. «Математика в вузе». – СПб., 2012. – С. 135–141.

15. Дегтярев В. Г. Управление вагонами различных компаний и различных типов методами транспортной задачи / В. Г. Дегтярев, В. А. Ходаковский // Сб. трудов «Проблемы математической и естественнонаучной подготовки в инженерном образовании». – СПб.: ФГБОУ ВПО ПГУПС, 2014. – С. 91–96.

16. Sforza A. An Optimization Approach for Decision Support in Railway Traffic Control / Sforza A. // Proc. Multiple Criteria Dessision Support; eds. P. Korhonen, A. Lewandowski, J. Wallenius. – Helsinki: Springer-Verlag, 1989.

17. Tanaka H. Fuzzy Linear Programming Problems with Fuzzy Numbers / H. Tanaka, K. Asai // Fuzzy Sets and System. – 1984. – № 13. – P. 1–10.

18. Archana Khurana J. Multi-index fixed charge bi-criterion transshipment problem / J. Archana Khurana // OPSEARCH. – 2013. – Vol. 50, Is. 2. – P. 229–249.

MultiCriteria Control Cars on a Railways Transportation

Degtyarev V. G., Khodakovsky V. A.
Petersburg State Transport University
Saint-Petersburg, Russia
vdegt@list.ru, hva1104@mail.ru

Abstract. **Methods of the management carriages on the railways with much aims make use of this paper: method of the chief element; method concessions; method of the lines connection. This methods found on the ways of the solution of the problem lines programming (method potentials and other), and too on the method solution of the transports problem with aim minimum time (nonlinear criterion of the optimization). This solutions for the carriages on the railways make for the first time. New method solution of the problems optimization propose too. This method goals of the classic methods.**

Keywords: **function of the aim; criterion of the optimization; management of the carriages; transports problem.**

References

1. Nesterov E. P. *Transportnye zadachi lineynogo programmirovaniya* [Transports problems lines programming], Moscow, Transport, 1971, 216 p.

2. *Pravila ekcpluatatsii, ponomernogo ucheta i raschetov za polzovanie gruzovymi vagonami sobstvennosti drugikh gosudarstv* [Rulls of the exploitation, registration and calculations carriages other States (affirmed 1996, may, 24)], Moscow, Marikor, 1996.

3. Gertwald A. S., Kanarskay L. A., Sokolov N. B. Automatic planning of the reserve carriages in the place loaing. [Avtomatizatsiya planirovaniya rezerva vagonov v mestakh pogruzki], *Conducting VNIIZT*, 1999, no. 2, pp. 3-8.

4. Tishkin E. M. *Avtomatizatsiya upravleniya vagonnym parkom* [Automatic management of the carriages park], Moscow, Intekst, 2000, 224 p.

5. Ivnizkiy V. A., Buyanov V. A., Sokolov N. B. Dynamic optimization guarantee loading of the recourses [Dinamicheskaya optimizatsiya obespecheniya namechaemoy pogruzki pogruzochnymi resursami], *Conducting VNIIZT*, 2000, no. 5, pp. 28-31.

6. Kovalev V. I., Degtyarev V. G., Eliseev S. U., Osminin A. T. Optimizations (on the cost) management of the carriages with calculation of the carriages other States. [Optimalnoe po stoimosti upravlenie vagonopotokami s uchotom nalichiya v rabochem parkevagonov, kak prinadlezhsshikh Rossii. tak i stranam SNG i Baltii], *Conducting VNIIZT*, 2002, no. 3, pp. 7-11.

7. Kovalev V. I., Degtyarev V. G., Eliseev S. U. Modelling management of the carriages with calculation of the carriages other States [O modelirovanii protsessov upravleniya vagonopotokami s uchotom vagonov drugikh gosudarctx], *News PSTU*, 2004, Is. 2, pp. 11-19.

8. Kovalev V. I., Eliseev S. U., Degtyarev V. G. et al. *Upravlenie parkami vagonov stran SNG i Baltii na zheleznykh dorogakh Rossii (ychebnje posobie)* [Management of the parks carriages with calculation of the carriages other States], Moscow, Marshrut, 2006, 243 p.

9. Degtyarev V. G. *Matematicheskoe modelirovanie (uchebnoe posobie)* [Mathematics modelling], St. Petersburg, PSTU, 2011, 105 p.

10. Degtyarev V. G., Zhgun O., Fomenko V. N. Stochastic transports problem on the criterion of the time [Stokhasticheskaya transportnaya zadacha po kriteriyu vremeni] *Works of the conf. "Mathematic in the university"*, St. Petersburg, PSTU, 2002, pp. 160-162.

11. Degtyarev V. G., Zhgun O., Fomenko V. N. Stochastic transports problem on the criterion of the time with depend parametris [Stokhasticheskaya transportnaya zadacha po kriteriyu vremeni s zavisimymi parametrami] *Works of the conf. "Mathematic in the university"*, St. Petersburg, PSTU, 2003, pp. 144-145.

12. Degtyarev V. G., Zhgun O., Fomenko V. N. Method solution stochastic transports problem on the criterion of the time [Ob odnom sposobe resheniya stokhasticheskoy transportnoy zadachi po kriteriyu vremeni] *Works of the conf. "Mathematic in the university"*, St. Petersburg, PSTU, 2003, pp. 146-147.

13. Degtyarev V. G. Optimize management of the carriages difference forms property [Primenenie metodov stokhasticheskoy transportnoy zadachi dlya optimalnogo regulirovaniya vagonov razlichnych form sobstvennosti] *Works of the conf. "Mathematic in the university"*, St. Petersburg, FGBOU VPO PSTU, 2012, pp. 135-141.

14. Degtyarev V. G. Application methods of the transports problem on management of the carriages difference forms property [Optimalnoe upravlenie porozhnimi vagonami razlichnykh form sobstvennosti] *Works of the conf. "Problems natural and scientific teaching in the engineers education"*, St. Petersburg, FGBOU VPO PSTU, 2013, pp. 66-71.

15. Degtyarev V. G., Khodakovsky V. A. Management of the carriages different firms and different types methods of the transports problem [Upravlenie vagonami razlichnykh kompaniy i razlichnykh tipov metodami transportnoy zadachi] *Works of the conf. "Problems natural and scientific teaching in the engineers education"*, St. Petersburg, FGBOU VPO PSTU, 2014, pp. 91-96.

16. Sforza A. An Optimization Approach for Decision Support in Railway Traffic Control, *Proceedings Multiple Criteria Dessision Support*, eds. P. Korhonen, A. Lewandowski, J. Wallenius, Helsinki, Springer-Verlag, 1989.

17. Tanaka H., Asai K. Fuzzy Linear Programming Problems with Fuzzy Numbers, *Fuzzy Sets and System*, 1984, no. 13, pp. 1-10.

18. Archana Khurana J. Multi-index fixed charge bi-criterion transshipment problem, *OPSEARCH*, 2013, Vol, 50, Is. 2, pp. 229-249.

Управление пакетными коммутациями в телематических устройствах с ограниченным буфером и повторными заявками с помощью вероятностного выталкивающего механизма и приоритетного обслуживания первичных заявок

Заяц О. И., Кореневская М. М., Ильяшенко А. С., Мулюха В. А.
Санкт-Петербургский политехнический университет Петра Великого
Санкт-Петербург, РФ
zay.oleg@gmail.com, masha_kor95@mail.ru, ilyashenko.alex@gmail.com, vladimir@mail.neva.ru

Аннотация. **В работе рассматривается однопотоковая система массового обслуживания конечной емкости с абсолютным приоритетом, вероятностным выталкивающим механизмом и повторными требованиями. Дано описание исследуемой модели, получены аналитические выражения для коэффициентов загрузки системы по каждому типу требований. Показан способ сведения модели к модели без повторных требований. Методом производящих функций найдены основные вероятностные характеристики для обоих типов требований. В результате численных расчетов исследовано влияние вероятностей выталкивания и повторного обслуживания на вероятности потерь. Также исследован режим двух случаев: запирания системы и линейного закона потерь в зависимости от вероятности повторного обращения.**

Ключевые слова: **теория массового обслуживания, приоритетные системы, вероятностный выталкивающий механизм, повторные заявки, метод производящих функций.**

Введение

Основной аналитический метод исследования телематических устройств состоит в рассмотрении их как специфических систем массового обслуживания [1]. Для корректного описания реальных сетевых взаимодействий при этом приходится использовать достаточно сложные модели СМО. Во-первых, фактическая структура информационных потоков диктует использование многопотоковых моделей СМО [2]. Во-вторых, частичные потоки должны быть надлежащим образом приоритезированы. Приоритет означает некоторое преимущество в обслуживании, которое предоставляется особо выделенным типам заявок по отношению к остальным типам.

Исследования последних лет показали, что приоритет в обслуживании целесообразно дополнить также приоритетом по постановке в очередь, т. е. соответствующим выталкивающим механизмом. Саму концепцию выталкивающего механизма предложил Г. П. Башарин и начал разрабатывать еще на рубеже 1960–1970-х годов [3]. Однако на первоначальном этапе развития этой теории речь шла только о *детерминированном* выталкивающем механизме. Он дает безусловное право высокоприоритетным требованиям всегда вставать на место низкоприоритетных в накопителе, когда тот бывает переполнен.

Такой выталкивающий механизм лишь отчасти решает задачу управления пакетными коммутациями. На практике часто интенсивность высокоприоритетного трафика существенно ниже, чем низкоприоритетного. При этом возникает следующая дилемма: если включить описанный механизм, то в накопителе будут преобладать высокоприоритетные запросы. Если же от него отказаться, то, напротив, большая часть накопителя будет забита низкоприоритетными запросами. Между тем для эффективной работы телематического устройства необходим рациональный баланс тех и других [2]. Детерминированный механизм не дает возможности тонкой настройки телематического устройства, необходимой для гибкого и эффективного управления им.

В начале 2000-х годов Н. О. Вильчевский выдвинул идею *вероятностного* (*рандомизированного*) выталкивающего механизма, в котором выталкивание происходит по случайному закону с некоторой вероятностью α. Величина α играет роль параметра управления и служит для адаптации телематического устройства к условиям окружающей сетевой среды. В статьях [4, 5] эта идея была реализована для случая двухпотоковой одноканальной марковской СМО с ограниченным накопителем и относительным приоритетом. Уже в самых первых работах по вероятностному выталкивающему механизму была показана его высокая эффективность. Так, в работах [4, 5] приводится числовой пример, в котором введение приоритета уменьшает вероятность потери высокоприоритетных требований всего в 2–3 раза, а дополнение приоритета еще и случайным выталкиванием позволяет за счет увеличения α от 0 до 1 уменьшить эту вероятность потери сразу в 10^{23} раз.

По классификации Г. П. Башарина [2] система, рассмотренная в [4, 5], имеет обозначение $\overrightarrow{M_2} / M / 1 / k / f_1^1$. Первый (векторный) символ в этом обозначении говорит, что на вход системы поступают два простейших потока требований. Второй символ указывает, что обслуживание обоих этих потоков идет по показательному закону с одинаковой

интенсивностью. Третий символ соответствует тому, что имеется лишь один канал обслуживания, а четвертый – что суммарная емкость СМО составляет ровно k требований (одно на обслуживании и k – 1 в накопителе). Последний символ приоритета f_i^j свидетельствует о наличии приоритета первого потока над вторым, причем значение $i = 1$ отмечает относительный приоритет, а значение $j = 1$ – вероятностный выталкивающий механизм.

Авторы данной статьи продолжили исследования, начатые в [4, 5], и разобрали ряд других разновидностей приоритета для СМО класса $\overrightarrow{M_2} / M / 1 / k / f_i^1$, снабженных вероятностным выталкивающим механизмом помимо случая относительного приоритета ($i = 1$). В статьях [6, 7] эта задача решена для случая абсолютного приоритета ($i = 2$), а в работе [8] – применительно к случаю чередующегося приоритета.

В теории массового обслуживания существует ряд усложнений, которые не попали в эту классификацию, однако требуют дополнительного внимания. Одним из таких усложнений является эффект «разогрева» и «охлаждения» модели [9, 10]. Еще один интересный способ усложнения модели – добавление повторных заявок. Во всех упомянутых статьях [2–8] не учитывался важный фактор повторных вызовов. Между тем хорошо известно, что игнорирование этого фактора в телефонных, информационно-вычислительных и телематических системах способно кардинально изменить реальную картину функционирования такого рода систем. Исследованию СМО с повторными вызовами посвящена обширная литература. Достаточно полное представление о современном состоянии работ в этой области дают монография [11] и обзор [12]. Вычислительные и алгоритмические аспекты проблемы подробно разобраны в [13].

В последние годы существенно возрос интерес к исследованию приоритетных систем с повторными требованиями. Здесь следует отметить интересный обзор [14], а также содержательную статью [15]. Изучение таких СМО началось со случая, когда ограничивалась длина очереди только низкоприоритетных требований, высокоприоритетные могли поступать в накопитель в любом количестве [16, 17]. Впоследствии ученые перешли к изучению моделей, в которых ограничение касалось и очереди высокоприоритетных заявок [18–23].

Особо следует отметить работы П. П. Бочарова и его соавторов, посвященные анализу тех приоритетных СМО с повторными требованиями, в которых приоритет по обслуживанию предоставляется первичным требованиям, а при повторном обращении требование превращается в низкоприоритетное [18–20]. Эти задачи чрезвычайно интересны с прикладной точки зрения, но явно недостаточно изучены. Выше отмечалось, что появление повторных заявок способно в корне изменить поведение СМО, в том числе при наличии приоритетов. Это происходит из-за обилия в таких системах вторичных требований, повторно пытающихся попасть в систему. Во многих случаях напрашивается естественное и логичное решение – предоставить преимущество впервые поступившим заявкам. Это имеет место, например, при моделировании узлов коммутации в информационных системах [24].

В нашей статье модель, подобная разобранной в [18–20, 24], изучается в комбинации с вероятностным выталкивающим механизмом. Это позволяет тонко настроить баланс между первичными и вторичными требованиями, что принципиально важно, например, в задачах управления робототехническими комплексами в космических экспериментах, детально описанных в работе [25].

Описание модели СМО

Рассмотрим систему массового обслуживания, на вход которой поступает один-единственный входящий простейший поток требований с интенсивностью $\lambda_{1,0}$. Этот поток будем называть *первичным* потоком заявок. Такие заявки будут иметь в данной системе наивысший приоритет. При функционировании системы с ограниченным накопителем на ее входе могут возникать потери этих первичных требований из-за отсутствия свободных мест в накопителе. В этом случае обычно требования попросту безвозвратно теряются. Однако при рассмотрении систем с повторными заявками у потерянных требований появляется возможность повторно попасть в систему. Именно такие заявки будут формировать еще один – второй – входящий поток в систему, обладающий меньшим приоритетом, чем первичный. Этот поток фактически делает систему двухпотоковой. Более детально поведение *повторных* заявок в системе может быть описано следующим образом.

Первичные требования, которые были потеряны по причине отсутствия свободных мест в накопителе, с вероятностью, равной единице, попадают на *орбиту* повторных требований. В классической постановке задачи о повторных требованиях вероятность попадания с орбиты обратно в систему была равна единице для всех типов требований. Чтобы не допустить забивания орбиты вытесненными из СМО требованиями, введем дополнительный параметр модели – вероятность попадания из орбиты обратно в систему q. Тогда если какое-либо требование ранее было вытеснено из системы и вновь попало туда лишь с орбиты повторных требований, то оно с заданной вероятностью q может еще раз попасть на орбиту, а с вероятностью $1 - q$ безвозвратно потеряться. Схема описанной СМО приведена на рис. 1.

Исследование такой системы можно свести к случаю обычной двухпотокой системы с вероятностным выталкиванием и без повторных заявок. Однако для этого придется использовать интенсивность первичного и вторичного входящих потоков, фактически реализуемую в данной СМО. Рассмотрим процесс получения этих интенсивностей подробнее.

При таком способе организации СМО интенсивность входящих потоков может быть получена как

$$\begin{cases} \lambda_1 = \lambda_{1,0}; \\ \lambda_2 = \lambda_{1rep} + \lambda_{2rep} = \dfrac{\lambda_{1,0} P_{loss}^{(1)}}{1 - P_{loss}^{(1)}} + \dfrac{\lambda_2 q P_{loss}^{(2)}}{1 - q P_{loss}^{(2)}}, \end{cases} \quad (1)$$

где λ_{1rep}, λ_{2rep} – интенсивность потоков первичных и вторичных повторных требований, соответственно; $P_{loss}^{(1)}$ и $P_{loss}^{(2)}$ – вероятность потери требований из первичного и вторичного потоков, соответственно.

Из результатов работ [6, 7] можно сделать вывод, что вероятность потери зависит от четырех параметров: ρ_1, ρ_2, k и α, первые два из которых представляют собой коэффициенты загрузки, соответственно, по высоко- и низкоприоритетному трафику, а третий – суммарную емкость системы.

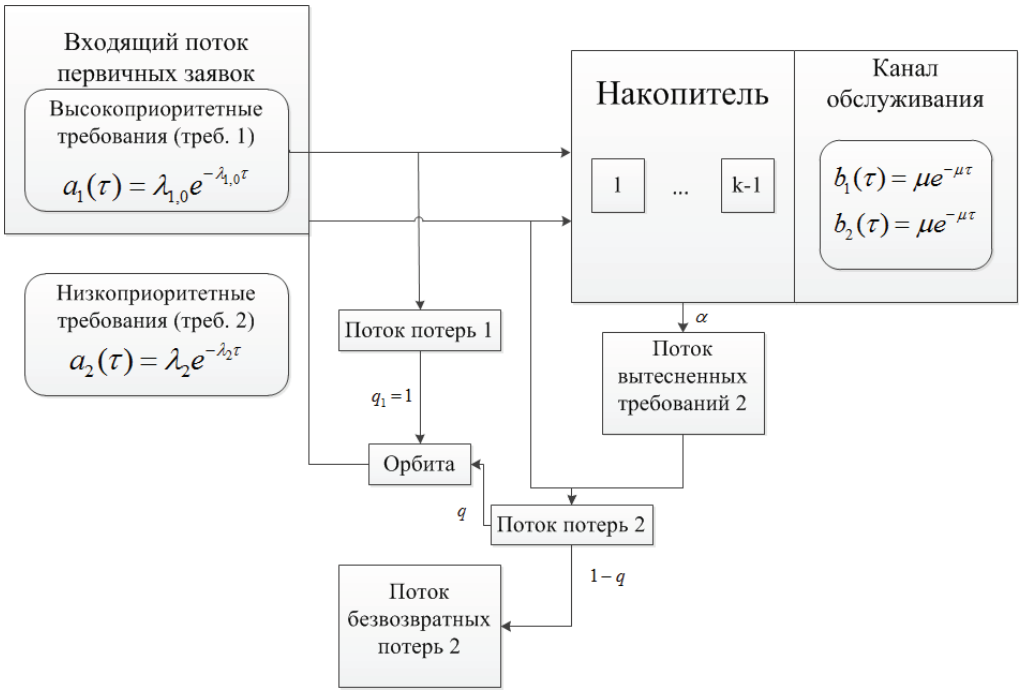


Рис. 1. Схема однопотоковой СМО с повторными заявками

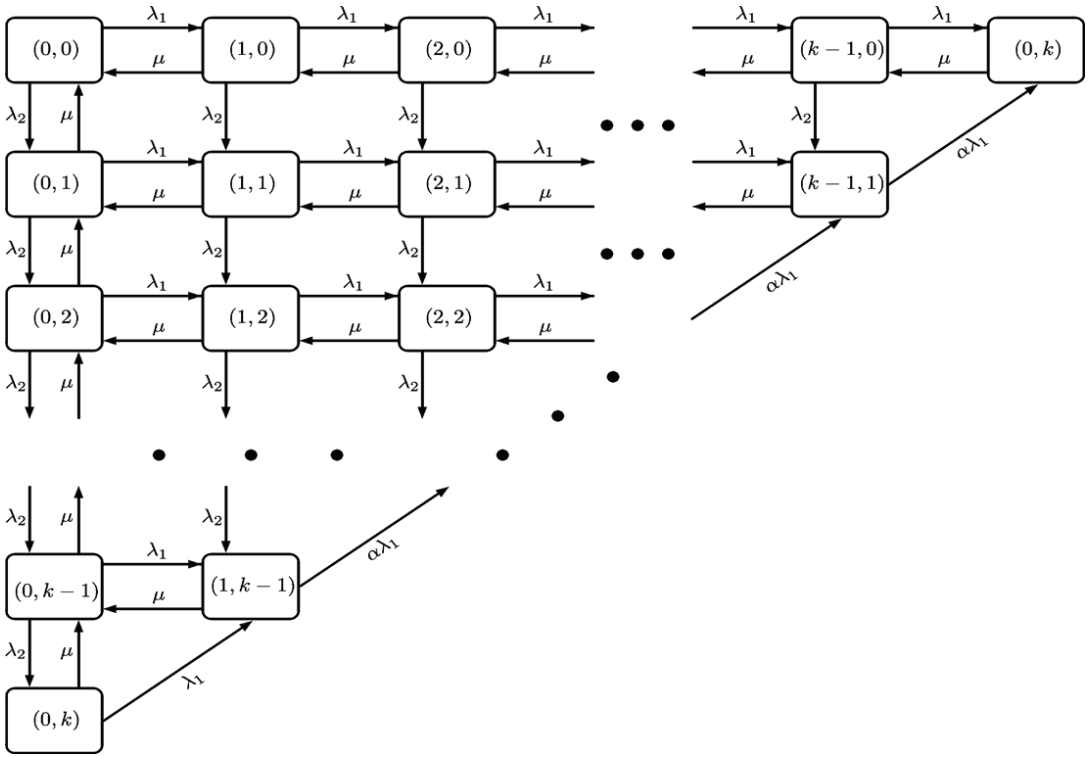


Рис. 2. Размеченный граф состояний для системы с повторными заявками

Тогда для определения коэффициентов загрузки можно использовать систему уравнений, получаемую из уравнений (1) делением их обеих частей на интенсивность обслуживания требований в канале:

$$\begin{cases} \rho_1 = \rho_{1,0}; \\ \rho_2 = \dfrac{\rho_{1,0}\varphi_1(\rho_1,\rho_2,k,\alpha)}{1-\varphi_1(\rho_1,\rho_2,k,\alpha)} * \dfrac{1-q\varphi_2(\rho_1,\rho_2,k,\alpha)}{1-2q\varphi_2(\rho_1,\rho_2,k,\alpha)}. \end{cases} \quad (2)$$

Введенные здесь функции четырех упоминавшихся аргументов задают выражения для вероятностей потери.

С использованием найденных выражений для коэффициентов загрузки (2) и для вероятностей потери, полученных методами работ [6, 7], легко получить численное значение интенсивности вторичного потока (а значит, и коэффициента загрузки по этому потоку), после чего легко находятся конкретные числовые значения для вероятностей потерь тре-

бований в зависимости от всех параметров системы, к которым теперь добавляется еще один – вероятность повторного обращения q.

Метод производящих функций

Для получения аналитических выражений для характеристик исследуемой модели существует ряд методов, применяемых к приоритетным системам массового обслуживания, рассмотренных в работе [26]. Один из них – метод производящих функций, который и будет применен далее.

Рассмотрим систему с вероятностным выталкивающим механизмом, абсолютным приоритетом и повторными заявками в установившемся режиме. Процесс в этой системе будет Марковским. Он является также и эргодическим, что гарантирует существование финальных вероятностей, не зависящих от начального состояния системы. Последние удовлетворяют стационарной системе уравнений Колмогорова.

Введем вначале фазовое пространство этой системы (совокупность всевозможных состояний, в которых она может находиться). Определим его равенством

$$\Omega = \{(i,j): i = \overline{0,k},\ j = \overline{0,k}, 0 \le i + j \le k\}. \qquad (3)$$

Далее определим вероятности состояний:

$$P(i,j;t) = P\{N_1(t) = i, N_2(t) = j, 0 \le i + j \le k\},$$

где $N_q(t)$ – число требований q-го типа в системе в момент времени t.

Введем финальные вероятности этой системы:

$$P_{i,j} = \lim_{t\to\infty} P(i,j;t),\ (i = \overline{0,k},\ j = \overline{0,k}, 0 \le i + j \le k).$$

Тогда по обычным правилам можно построить размеченный граф состояний, описывающий все возможные переходы между состояниями системы из фазового пространства (3). Этот граф представлен на рис. 2.

Воспользуемся приведенным графом состояний и построим систему уравнений Колмогорова для финальных вероятностей. В результате этих действий получим следующую систему линейных уравнений:

$$\begin{aligned}
&-[\lambda_1(1-\delta_{j,k-i}) + \alpha\lambda_1(1-\delta_{i,k})\delta_{j,k-i} + \\
&+ (1-\alpha)\lambda_1\delta_{i,0}\delta_{j,k-i} + \lambda_2(1-\delta_{j,k-i}) + \\
&+ \mu(1-\delta_{i,0}\delta_{j,0})]P_{i,j} + \mu P_{i+1,j} + \mu\delta_{i,0}P_{i,j+1} + \\
&+ \lambda_2 P_{i,j-1} + \lambda_1 P_{i-1,j} + \alpha\lambda_1\delta_{j,k-i}P_{i-1,j+1} + \\
&+ (1-\alpha)\lambda_1\delta_{j,k-i}\delta_{i,1}P_{i-1,j+1} = 0, \\
&(0 \le i \le k; 0 \le j \le k-i).
\end{aligned} \qquad (4)$$

Для удобства записи этих уравнений использован дельта-символ Кронекера, который позволяет привести все уравнения (4) к единообразной форме для произвольных значений индексов i и j.

Уравнения (4) выполняются при всех $i, j \ge 0$, для которых выполняется условие $i + j \le k$. Здесь введено следующее соглашение, которое будет использоваться во всей статье:

$$P_{i,j} \equiv 0, (i < 0, j < 0, i + j > k).$$

Для получения характеристик модели будем использовать метод производящих функций.

Для этого определим производящую функцию финальных вероятностей $P_{i,j}$ из фазового пространства (3) в виде

$$G(u,v) = \sum_{i=0}^{k}\sum_{j=0}^{k-i} P_{i,j}u^i v^j.$$

Для этой производящей функции условие нормировки выглядит следующим образом:

$$G(1,1) = \sum_{i=0}^{k}\sum_{j=0}^{k-i} P_{i,j} = 1.$$

Теперь приступим к получению аналитического выражения для производящей функции. Для этого умножим левую и правую части уравнения (4) на $u^i v^j$ и просуммируем по всем допустимым значениям (i,j). После ряда алгебраических преобразований приходим к искомому уравнению для производящей функции финальных вероятностей:

$$\begin{aligned}
&[\lambda_1 u(1-u) + \lambda_2 u(1-v) + \mu(u-1)]vG(u,v) = \\
&= \mu(u-v)G(0,v) + (1-\alpha)\lambda_1 P_{0,k}v^k u(u-v) + \\
&+\mu u(v-1)G(0,0) + \alpha\lambda_1 u^{k+1}(v-u)P_{k,0} + \\
&+[\alpha\lambda_1(u-v) + \lambda_1(1-u)v + \lambda_2(1-v)v]u\sum_{i=0}^{k} P_{i,k-i}u^i v^{k-i}.
\end{aligned} \qquad (5)$$

Чтобы получить отсюда выражения для искомых вероятностей $P_{i,j}$ при произвольных i и j, необходимо вначале разрешить (5) относительно G, что дает

$$\begin{aligned}
&G(u,v) = \frac{1}{v\rho_1(u-u_1)(u-u_2)}* \\
&*((u-v)G(0,v) + u(u-1)G(0,0) + \\
&+[\alpha\rho_1(u-v) + \rho_1(1-u)v + \rho_2(1-v)v]u\sum_{i=0}^{k} P_{i,k-i}u^i v^{k-i} + \\
&+\alpha\rho_1 u^{k+1}(v-u)P_{k,0} + (1-\alpha)\rho_1 P_{0,k}v^k u(u-v)).
\end{aligned}$$

Здесь u_1, u_2 – корни знаменателя этого выражения, определяемые по формуле

$$u_{1,2} = \frac{[\rho_1 + \rho_2(1-v) + 1] \mp \sqrt{[\rho_1 + \rho_2(1-v) + 1]^2 - 4\rho_1}}{2\rho_1}.$$

Эти корни являются простыми полюсами производящей функции, для дальнейшего решения необходимо разложить выражение для производящей функции по степеням ее аргументов u и v.

Чтобы это сделать, воспользуемся выражениями для тех характеристик системы, которые хорошо известны по исследованиям классической однопотоковой системы класса $M/M/1/k$. Это прежде всего распределение общего числа требований в системе:

$$r_n = \sum_{i=0}^{n} P_{i,n-i} = \sum_{i=0}^{n} P_{n-i,i}. \qquad (6)$$

Подставим в (6) выражение для финальных вероятностейиз работы [7]. Тогда получим систему уравнений, содержащую только наиболее интересующие нас «диагональные» вероятности $p_i = P_{k-i,i}$.

$$r_z = \sum_{j=0}^{z} P_{z-j,j} = p_0 \rho_1^{-1} \zeta_z - \alpha \varphi_z p_{z+1} + \\ + \sum_{j=1}^{z} p_j \xi_{z,j} + p_k (\alpha - 1) \delta_{z,k-1}, (0 \le z \le k-1), \quad (7)$$

где

$$\zeta_z = \sum_{j=0}^{z} \rho_1^{(1-k+z-j)/2} \beta^j (C_{k-z-1}^{j+1} - \rho_1^{1/2} C_{k-z-2}^{j+1}); \quad (8)$$

$$\varphi_z = \rho_1^{(z+1-k)/2} C_{k-1-z}^{1};$$

$$\xi_{z,j} = \sum_{s=j}^{z} \rho_1^{(z-k-s+j)/2} (\rho_1^{-1/2} C_{k-1-z}^{s-j+1} - C_{k-2-z}^{s-j+1}) \beta^{s-j} - \\ - \alpha \rho_1^{(j-k)/2} \beta^{z+1-j} C_{k-1-z}^{z-j+2}.$$

Дополним эту систему уравнением (6), чтобы получить одно недостающее уравнение:

$$r_k = \sum_{i=0}^{k} P_{k-i,i} = \sum_{i=0}^{k} p_i. \quad (9)$$

Данная система имеет квазитреугольную матрицу, для которой процесс решения можно свести к решению системы с треугольной матрицей. Профиль этой матрицы представлен на рис. 3 (при $k = 21$).

Нахождение вероятностных характеристик модели

Одной из самых важных характеристик любой телематической системы является вероятность потери заявки, которая зависит от её типа. Для каждого типа требований вероятность потери может быть найдена по ранее полученным формулам (7)–(9):

$$P_{loss}^{(1)} = q_k + (1-\alpha) \sum_{i=1}^{k-1} p_i; P_{loss}^{(2)} = r_k + \alpha \frac{\rho_1}{\rho_2} \sum_{i=1}^{k-1} p_i + \frac{\rho_1}{\rho_2} p_k.$$

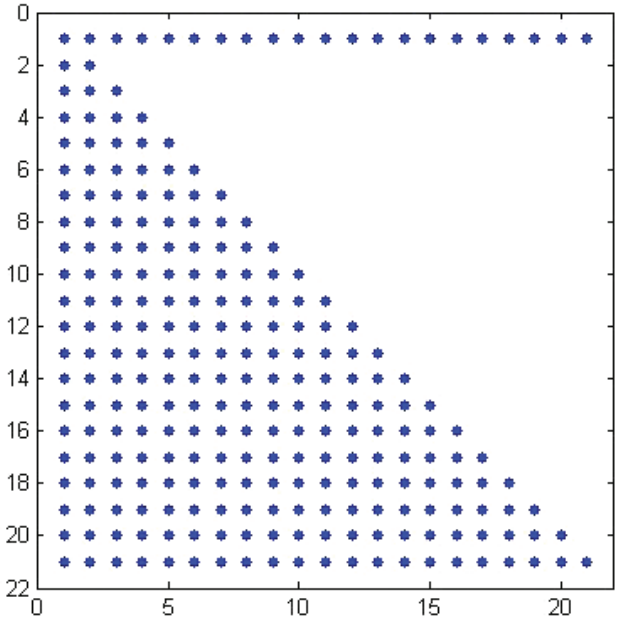


Рис. 3. Профиль матрицы итоговой системы

Численное исследование зависимостей $P_{loss}^{(i)}$ от вероятности выталкивания a дало очень интересные результаты, представленные ниже на графиках.

Рассмотрим зависимость вероятности потерь для двух типов требований в зависимости от параметров a и q при разных значениях коэффициента загрузки ρ_1. Результаты представлены на рис. 4 для высокоприоритетных требований, на рис. 5 – для низкоприоритетных требований в обоих случаях при $\rho_1 = 1.0; 1.6; 2.2; 2.8$.

Из зависимостей на рис. 4 видно, что с ростом коэффициента загрузки системы отдельные кривые из семейства кривых, отвечающих разным значениям параметра q,

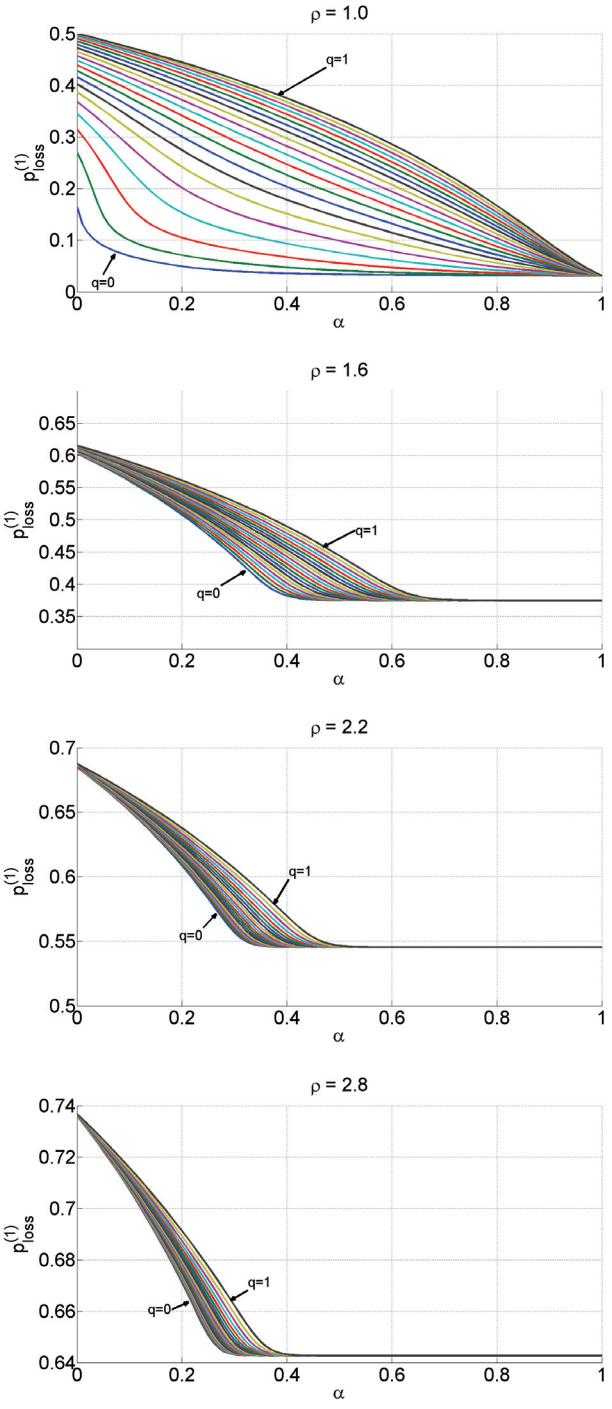


Рис. 4. Зависимость вероятности потерь высокоприоритетных требований от a и q

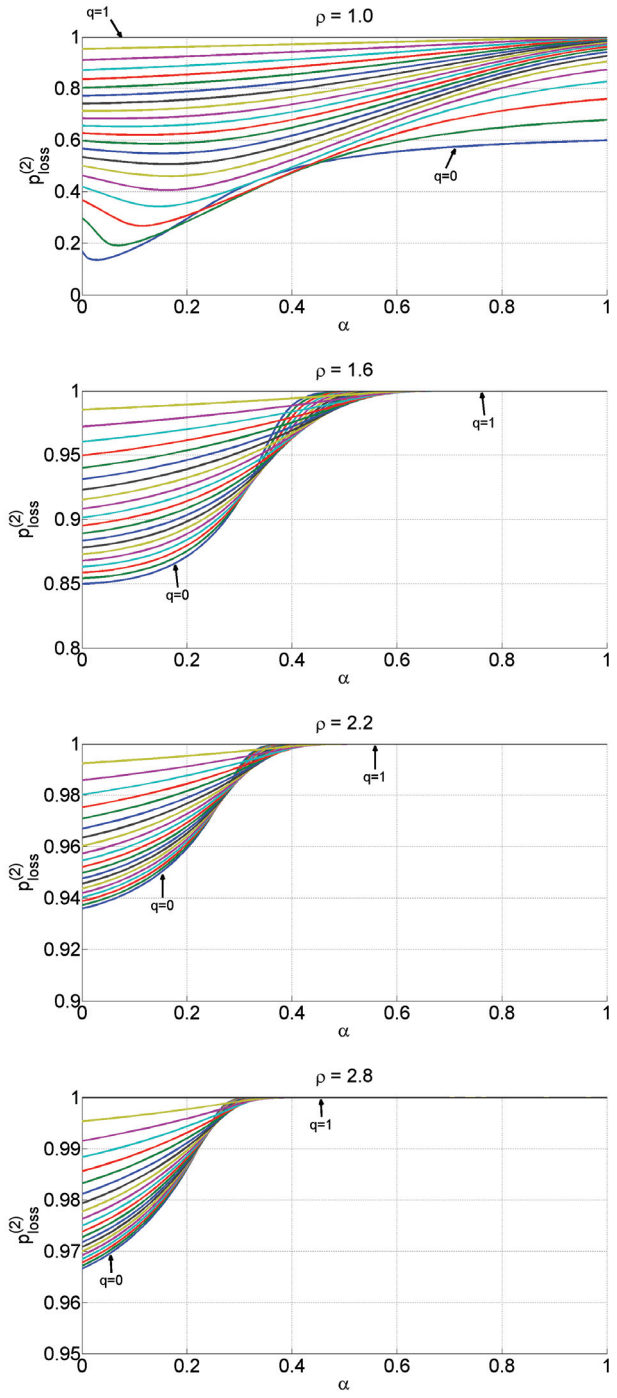


Рис. 5. Зависимость вероятности потерь низкоприоритетных требований от *a* и *q*

сближаются друг с другом, и это говорит о снижении зависимости вероятности потерь от вероятности попадания требования на повторное обслуживание. А поскольку сами кривые несколько приподнимаются вверх, то можно сделать логичный вывод, что вероятность потери при дальнейшем увеличении нагрузки будет только расти.

В работах [6–8] введено понятие областей линейности, в которых при определенных комбинациях коэффициентов загрузки зависимость вероятности потерь от вероятности выталкивания оказывалась близка к линейной. В данном случае такой характер поведения вероятности потерь можно наблюдать только для небольших значений коэффициента загрузки.

Из графиков на рис. 5 видно, что при некоторых значениях параметра *a* удается практически полностью заблокировать систему от попадания в нее низкоприоритетных требований. В работах [6–8] такой эффект назван запиранием системы, причем были найдены области действия подобных эффектов. Для данной системы можно сделать вывод, что при высоких значениях коэффициента загрузки варьирование вероятности попадания требований на повторное обслуживание *q* не оказывает существенного влияния

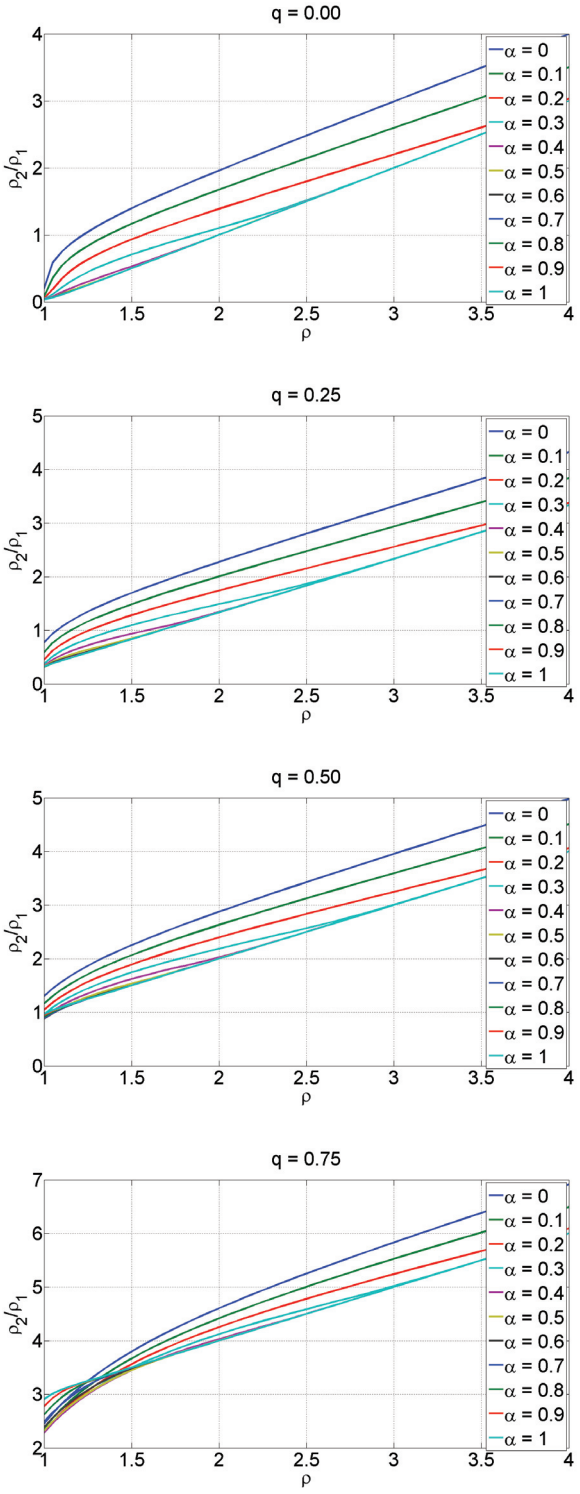


Рис. 6. Зависимость отношения коэффициентов загрузки повторного и первичного потоков при различных *a* и *q*

на проявление этого эффекта. Однако если значения коэффициента загрузки близки к пропускной способности системы, то можно в достаточно широком диапазоне менять вероятности потерь и даже совсем запереть систему от попадания повторных заявок.

Еще одним результатом, представлявшим интерес для приложений, была зависимость отношения между коэффициентами загрузки потоков требований (рис. 6).

Из приведенных зависимостей видно, что при изменении вероятности выталкивания a соотношение между коэффициентами загрузки убывает, т. е. первичный поток начинает преобладать над вторичным. Однако при изменении вероятности попадания потерянного требования на повторное облуживание это соотношение возрастает. Максимальные значения для всех случаев достигаются при $a = 0$ и $q = 1$.

Заключение

В рамках данной работы исследована однопотоковая система с повторными заявками и вероятностным выталкиванием. Получены аналитические выражения для коэффициентов загрузки модели с повторными заявками. Показан способ сведения однопотоковой модели с повторными заявками к двухпотоковой модели без них. Показано применение метода производящих функций для получения вероятностей состояний модели. Также построены численные зависимости вероятностей потери от основных параметров модели. Практически значимыми результатами являются полученные эффекты запирания и линейного закона потерь, которые могут быть использованы для уменьшения вычислительной загрузки на телематические устройства, функционирующие и принимающие решения в режиме реального времени. Предварительные расчеты таких областей, где проявляются эти эффекты, позволят сразу выбирать нужные значения параметров модели вместо их многократного вычисления в реальном времени, что позволит поднять производительность систем и повысить эффективность управления ею.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 15-29-07131 офи_м.

Литература

1. Вишневский В. М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. – М.: Техносфера, 2003.

2. Заяц О. И. Управление пакетными коммутациями в телематических устройствах с ограниченным буфером при наличии абсолютного приоритета и вероятностного выталкивающего механизма / О. И. Заяц, В. С. Заборовский, В. А. Мулюха, А. С. Вербенко // Программная инженерия. – 2012. – № 2. – С. 22–27; № 3. – С. 21–29.

3. Башарин Г. П. Некоторые результаты для систем с приоритетом / Г. П. Башарин // Массовое обслуживание в системах передачи информации. – М.: Наука, 1969. – С. 39–53.

4. Avrachenkov K. E. Randomized push-out disciplines in priority queueing / K. E. Avrachenkov, G. L. Shevlyakov, N. O. Vilchevsky // J. Math. Sci. – 2004. – Vol. 22, no. 4. – P. 3336–3342.

5. Avrachenkov K. E. Priority queueingwith finite buffer size and randomized push – out mechanism / K. E. Avrachenkov, N. O. Vilchevsky, G. L. Shevlyakov // Perform. Eval. – 2005. – Vol. 61, no. 1. – P. 1–16.

6. Ilyashenko A. Further investigations of the priority queueing system with preemptive priority and randomized push–out mechanism / A. Ilyashenko, O. Zayats, V. Muliukha, L. Laboshin // Lect. Notes in Comp. Sci. – 2014. – Vol. 8636. – P. 433–443.

7. Muliukha V. Preemptive queueing system with randomized push-out mechanism / V. Muliukha, A. Ilyashenko, O. Zayats, V. Zaborovsky // Commun. Nonlinear Sci. Numer. Simul. – 2015. – no. 1/3. – P. 147–158.

8. Ilyashenko A. Alternating priorities queueing system with randomized push-out mechanism / A. Ilyashenko, O. Zayats, V. Muliukha, A. Lukashin // Lect. Notes in Comp. Sci. – 2015. – Vol. 9247. – P. 436–445.

9. Гиндин С. И. Численный расчет многоканальной системы массового обслуживания с рекуррентным входящим потоком и «разогревом» / С. И. Гиндин, А. Д. Хомоненко, С. Е. Ададуров // Изв. ПГУПС. – 2013. – Вып. 4 (37). – С. 92–101.

10. Хомоненко А. Д. Моделирование облачных вычислений с использованием многоканальной системы массового обслуживания с «охлаждением» / А. Д. Хомоненко, М. М. Халиль, С. И. Гиндин // XIX междунар. конф. по мягким вычислениям и измерениям (SCM-2016). – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2016. – Т. 1. – С. 247–251.

11. Falin G. I. Retrial queues / G. I. Falin, J. G. Templeton. – L.: Chapman and Hall, 1997.

12. Falin G. I. A survey of retrial queue / G. I. Falin // Queueing Syst. – 1990. – Vol. 7. – P. 127–168.

13. Степанов С. Н. Численные методы расчета систем с повторными вызовами / С. Н. Степанов. – М.: Наука, 1983.

14. Choi B. D. Single server retrial queues with priority calls / B. D. Choi, Y. Chang // Math. Comput. Modell. – 1999. – Vol. 30, no. 1. – P. 7–32.

15. Artalejo J. R. Stationary analysis of a retrial queue with preemptive repeated attempts / J. R. Artalejo, A. N. Dudin, V. I. Klimenok // Oper. Res. Lett. – 2001. – Vol. 28. – P. 173–180.

16. Choi B. D. The M/G/1 retrial queue with Bernoulli schedule / B. D. Choi, K. K. Park // Queueing Syst. – 1990. – Vol. 7. – P. 219–227.

17. Choi B. D. On the virtual waiting time for an M/G/1 retrial queueing systems with two types of calls / B. D. Choi, D. H. Han, G. I. Falin // J. Appl. Math. Stochastics Anal. – 1993. – Vol. 6, no.1. – P. 11–29.

18. Бочаров П. П. Система M/G/1/r с повторными заявками и приоритетным обслуживанием первичных заявок / П. П. Бочаров, О. И. Павлова, Д. А. Пузикова // Вестн. РУДН. – Прикладная математика и информатика. – 1997. – № 1. – С. 37–57.

19. Bocharov P. P. A M/G/1/r retrial queueingsystem with prioritry of primary customers / P. P. Bocharov, O. I. Pavlova, D. A. Puzikova // Math. Comput. Modell. – 1999. – Vol. 30, no. 1. – P. 89–98.

20. Бочаров П. П. Стационарные вероятности состояний системы MAP/G/1/r с повторными заявками и приоритетным обслуживанием первичных заявок / П. П. Бочаров, А. В. Печинкин, Н. Х. Фонг // Автоматика и телемеханика. – 2000. – № 8. – С. 68–78.

21. Choi B. D. MAP1, MAP2/M/c retrial queue with guard channels and its applications to cellar networks / B. D. Choi, Y. Chang, B. Kim // Top. – 1999. – Vol. 7. – P. 231–248.

22. Choi B. D. M/G/1 retrial queueing systems with two types of calls and finite capacity / B. D. Choi, K. B. Choi, Y. N. Lee // Queueing Syst. – 1995. – Vol. 19. – P. 215–229.

23. Choi B. D. The M1, M2/G/1/k retrial queueing systems with priority / B. D. Choi, D. B. Zhu // J. Korean Math. Soc. – 1998. – Vol. 35. – P. 691–712.

24. Агаларов Я. М. Об одном численном методе вычисления стационарных характеристик узла коммутации с повторными передачами / Я. М. Агаларов // Автоматика и телемеханика. – 2011. – № 1. – С. 95–106.

25. Zaborovsky V. Cyber-Physical Approach in a Series of Space Experiments “Kontur” / V. Zaborovsky, V. Muliukha, A. Ilyashenko // Lect. Notes in Comp. Sci. – 2015. – Vol. 9247. – P. 745–758.

26. Рыжиков Ю. И. Расчет многоканальных систем обслуживания с абсолютным и относительным приоритетами на основе инвариантов отношения / Ю. И. Рыжиков, А. Д. Хомоненко // Интеллектуальные технологии на транспорте. – 2015. – № 3. – С. 11–16.

Network Packets Management in Telematic Devices with Retrial, Limited Buffer Size Using Randomized Push-Out Mechanism and Prioritization for Initial Flow

Zayats O. I., Korenevskaya M. M., Ilyashenko A. S., Muliukha V. A.
Peter The Great St.Petersburg Polytechnic University
Saint-Petersburg, Russian Federation
zay.oleg@gmail.com, masha_kor95@mail.ru, ilyashenko.alex@gmail.com, vladimir@mail.neva.ru

Abstract. **In this article considered retrial queueing system with single incoming flows, finite buffer, preemptive priority and randomized push-out mechanism. Provided description of queueing system model, obtained analytical expressions for load coefficients of system for both types of incoming flows and shown method of casting this model to model without retrial. Using generating functions method obtained main probabilistic characteristics of considered model (like loss probabilities) for both types of incoming packets. Obtained theoretical results allowed to study dependences of loss probabilities from model parameters like push-out and retrial probabilities. Also found areas of retrial probability values when model can get closed for low-priority packets or can have linear dependence of loss probability from pushing-out probability.**

Keywords: **priority queueing systems, prioritized system, randomized push-out mechanism, retrial systems, queueing theory.**

References

1. Vishnevsky V. M. *Teoreticheskie osnivy proektirovaniya komputernikh setey* [Theoretical bases of computer networks design.]. Moscow, Tekhnosfera, 2003.

2. Zayats O. I., Zaborovsky V. S., Muliukha V. A., Verbenko A. S. Network packets management in telematic devices with limited buffer size preemptive priority and randomized push-out mechanism. Part 1. [Upravlenie paketnimi kommutaciyami v telemeticheskih ustroystvah s ogranichennim bufferom prinalichii absolutnogo prioriteta i veroyatnostnogo vitalkivayushego mehanizma. Chast' 1], *Programmnaya ingeneria [Program Eng.]*, 2012, no. 2, pp. 22-27; no. 3, pp. 21-29.

3. Basharin G. P. Some results for priority systems [Nekotorierezultatidlyasistem s prioritetom]. *Massovoe obslujivanie v sistemah peredachi infomacii [Queueing theory in data transfer systems]*. Moscow, Nauka, 1969, pp. 39-53.

4. Avrachenkov K. E., Shevlyakov G. L., Vilchevsky N. O. Randomized push-out disciplines in priority queueing, *J. Math. Sci.*, 2004, vol. 22, no. 4, pp. 3336-3342.

5. Avrachenkov K. E., Vilchevsky N. O., Shevlyakov G. L. Priority queueingwith finite buffer size and randomized push – out mechanism, *Perform. Eval.*, 2005, vol. 61, no. 1, pp. 1-16.

6. Ilyashenko A., Zayats O., Muliukha V., Laboshin L. Further investigations of the priority queueing system with preemptive priority and randomized push-out mechanism, *Lect. Notes in Comp. Sci.*, 2014, vol. 8636, pp. 433-443.

7. Muliukha V., Ilyashenko A., Zayats O., Zaborovsky V. Preemptive queueing system with randomized push-out mechanism, *Commun. Nonlinear Sci. Numer. Simul*., 2015, no. 1/3, pp. 147-158.

8. Ilyashenko A., Zayats O., Muliukha V., Lukashin A. Alternating priorities queueing system with randomized push-out mechanism, *Lect. Notes in Comp. Sci.*, 2015, vol. 9247, pp. 436-445.

9. Gindin S. I., Khomonenko A. D., Adadurov S. E. Numerical computations multiflowqueueing system with recurrent flow and heating [Chislenniy raschet mnogokanalnoy sistemi massovogo obslugivaniya s rekurrentnim vhodyashim potokom i razogrevom], *PGUPS News [Izv. Peterburgskogo universiteta putey soobsheniya]*, 2013, no. 4 (37), pp. 92-101.

10. Khomonenko A. D., Khalil M. M., Gindin S. I. Cloud computing modelling with multichannel queueing systems with «cooling» [Modelirovanie oblachnikh vichisleniy s ispolzovaniem mnogokanalnoy sistemi massovogo obslugivaniya s okhlagdeniem]. *XIX Int. Conf. soft Comput. Measurements (SCM-2016)*. 2016, St. Petersburg, St. Petersburg Electrotechnical Univ. "LETI", T. 1, pp. 247-251.

11. Falin G. I., Templeton J. G. Retrial queues. L, Chapman and Hall, 1997.

12. Falin G. I. A survey of retrial queue, *Queueing Syst.*, 1990, vol. 7, pp. 127-168.

13. Stepanov S. N. Chislennie metody rascheta sistem s povtornimi vizovami [Numerical methods in retrial systems]. Moscow, Nauka, 1983.

14. Choi B. D., Chang Y. Single server retrial queues with priority calls, *Math. Comput. Modell.*, 1999, vol. 30, no. 1, pp. 7-32.

15. Artalejo J. R., Dudin A, N., Klimenok V. I. Stationary analysis of a retrial queue with preemptive repeated attempts, *Oper. Res. Lett.*, 2001, vol. 28, pp. 173-180.

16. Choi B. D., Park K. K. The M/G/1 retrial queue with Bernoulli schedule, *Queueing Syst.*, 1990, vol. 7, pp. 219-227.

17. Choi B. D., Han D. H., Falin G. I. On the virtual waiting time for an M/G/1 retrial queueing systems with two types of calls, *J. Appl. Math. Stochastics Anal.*, 1993, vol. 6, no. 1, pp. 11-29.

18. Bocharov P. P., Pavlova O. I., Puzikova D. A. Sistema M/G/1/r s povtornimi zayavkamii prioritetnim obslugivaniem pervichnikh zayavok [Retrial queueing system M/G/1/r with priority of primary customers], *RUDN Bull. Appl. Math. Inf. [Vestnik RUDN. Prikladnaya matematika i informatika]*, 1997, no. 1, pp. 37-57.

19. Bocharov P. P., Pavlova O. I., Puzikova D. A. A M/G/1/r retrial queueing system with prioritry of primary customers, *Math. Comput. Modell.*, 1999, vol. 30, no. 1, pp. 89-98.

20. Bocharov P. P., Pechinkin A. V., PhongN.Kh. Stacionarnie veroyatnosti sostoyaniy sistemi MAP/G/1/r s povtornimi zayavkami i prioritetnim obslugivaniem pervichnikh zayavok [Stationary probabilities od retrial queueing system MAP/G/1/r and priority on primary customers], *Automatics and telemechanics [Avtomatika i telemehanika]*, 2000, no. 8, pp. 68-78.

21. Choi B. D., Chang Y., Kim B. MAP1, MAP2/M/c retrial queue with guard channels and its applications to cellar networks, *Top*, 1999, vol. 7, pp. 231-248.

22. Choi B. D., Choi K. B., Lee Y. N. M/G/1 retrial queueing systems with two types of calls and finite capacity, *Queueing Syst.*, 1995, vol. 19, pp. 215-229.

23. Choi B. D., Zhu D. B. The M1, M2/G/1/k retrial queueing systems with priority, *J. Korean Math. Soc.*, 1998, vol. 35, pp. 691-712.

24. Agalarov Ya. M. Ob odnom chislennom metode vichislen-iya stacionarnih harakteristic uzla kommutacii s povtornimi peredachami [A numerical method for calculating stationary characteristics switching node with retransmissions], *Automatics and Telemechanics [Avtomatika I Telemehanika]*, 2011, no. 1, pp. 95-106.

25. Zaborovsky V., Muliukha V., Ilyashenko A. Cyber-Physical Approach in a Series of Space Experiments “Kontur” *Lect. Notes in Comp. Sci.*, 2015, vol. 9247. pp. 745-758.

26. Ryzhikov Yu. I., Khomonenko A. D. Raschet mnogokanalnikh system obslugivaniya s absolutnim i otnositelnim prioritetami na osnove invariantov otnosheniya [Computational approach for multiflowqueueing systems with preemptive and non-preemptive priorities based on relational invariants], *Intellectual Technologies on Transport [Intellectualnie Tehnologii na Transporte]*, 2015, no. 3, pp. 11-16.

Влияние параметров линейной антенной решетки на возможность выявления отражателей

Кормильцева М. Ф., Чурова В. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
Mariekor@outlook.com, Postkiser@mail.ru

Аннотация. **Рассмотрен принцип и особенности работы ультразвуковых преобразователей с фазированной антенной решеткой (ФАР). Изучены параметры настройки дефектоскопа на ФАР, их влияние на результаты контроля, а именно S-сканы. Различно сфокусированные (цилиндрические, эллиптические, сферические) звуковые пучки обеспечивают лучшую наглядность полезного сигнала на фоне шумов. Приводятся результаты исследование влияния параметров настройки (активной апертуры, фокусного расстояния, угловой разрешающей способности, типа фокусировки) на выявление отражателей в образце с помощью ультразвукового дефектоскопа «HARFANGX-32» и пьезоэлектрического преобразователя на ФАР с призмой.**

Ключевые слова: **неразрушающий контроль, дефектоскопия, ультразвуковой контроль, фазированная решетка, преобразователь.**

Введение

Неотъемлемая часть ультразвукового контроля – правильная подготовка и настройка. В зависимости от характеристик объектов контроля – толщины, материала, особенностей конструкции – выбирают подходящие датчики (в том числе пьезоэлектрические преобразователи – ПЭП). Часто необходимо использовать ПЭП с разными углами ввода для одного объекта для прозвучивания всего сечения шва прямым и однократно отраженным лучами, чтобы выявить различно ориентированные дефекты [1]. Приобретение и содержание (поверка, ремонт и обслуживание) большого количества ПЭП требует значительных затрат. Для решения ряда задач и оптимизации контроля в ультразвуковой дефектоскопии начали применять метод фазированной антенной решетки (ФАР). Приборы на ФАР появились еще в середине 1990-х годов (в медицине используются с начала 1980-х годов), однако только сейчас они вышли за рамки научно-исследовательских программ и их начали внедрять в производство. Главными преимуществами технологии ультразвуковых фазированных решеток являются амплитуда и фаза импульсов возбуждения данного множества отдельных пьезоэлементов в многоэлементном преобразователе, которые управляются компьютером. Пьезоэлементы возбуждаются так, чтобы была возможность управлять параметрами ультразвукового луча (углом, фокусным расстоянием, размером фокусного пятна) с помощью компьютерной программы. Это позволяет обнаруживать дефекты, различно ориентированные относительно акустической оси, тогда как при использовании обычного одноэлементного преобразователя вероятность пропустить дефекты, расположенные под большим углом к акустической оси, больше [2]. Отчеты представляются в виде изображений (сканов), что облегчает понимание результатов контроля для персонала.

Применение при неразрушающем контроле дефектоскопов на основе технологии фазированных решеток значительно повышает качество и надежность контроля, поскольку можно обнаружить сложно ориентированные дефекты и прозвучить больший объем объекта контроля за счет электронного управления ультразвуковыми полями. Дефектоскопы на ФАР могут применяться там, где затруднено получение достоверных результатов с помощью привычного ультразвукового дефектоскопа. Например, при контроле деталей и объектов с крупнозернистой структурой (опор двигателя самолета из литья титана) или большого объема сваренных элементов сложной формы (тавровых сварных швов ребер жесткости при строительстве мостов).

В настоящее время дефектоскопы на ФАР используются для контроля сварных швов (и околошовной зоны), лопастей ветряных турбин, труб и трубопроводов различного диаметра и назначения, в том числе сварных стыков полиэтиленовых газопроводов высокой плотности, для проверки коррозийности. Дефектоскопы на ФАР нашли применение в таких отраслях, как нефтегазовая промышленность (контроль газопроводов и нефтепроводов), авиационная (деталей корпуса самолета, шасси), аэрокосмическая (композитных деталей, сопел ракет), железнодорожная (колес вагонов), мостостроение, добывающая отрасль (тяжелой техники – ковшей, валов, экскаваторов), также их используют для ультразвукового контроля золотых слитков и для обнаружения пустот в пластмассовых деталях [3].

Несмотря на значительные преимущества данного метода по сравнению с использованием обычных ультразвуковых дефектоскопов и одноэлементных преобразователей, дефектоскопы на ФАР используются реже, вероятно, потому, что нет четко сформулированной нормативно-документационной базы для контроля различных объектов с помощью дефектоскопов на фазированных решетках [4–7].

Принцип работы фазированной решетки

Преобразователь с ФАР представляет собой некоторое количество пьезоэлектрических элементов, каждый из которых можно рассматривать как источник сферической волны [8].

Для создания луча с требуемыми параметрами (углом и фокусировкой) эти волновые фронты можно задержать во времени и синхронизировать по фазе и амплитуде – отдельные элементы возбуждаются в несколько различающиеся моменты времени. Волновые фронты от множества узких пьезоэлементов будут интерферировать, создавая суммарный волновой фронт с требуемыми параметрами [9].

При излучении генератор синхроимпульсов посылает сигнал на блок фазовых задержек, который генерирует импульс высокого напряжения заданной длительности и с заданной задержкой, определенной фокальным законом. На каждый элемент решетки поступает один задержанный импульс. Излученные каждым элементом волны при суммировании представляют собой луч, сфокусированный на определенном расстоянии и распространяющийся под конкретным углом. Впоследствии этот луч отражается от дефекта. Сигнал принимается каждым элементом решетки и в соответствии с заданным фокальным законом задерживается во времени. Далее такие задержанные импульсы суммируются и формируют единый импульс, который поступает в устройства приемного тракта [10]. Величина временно́й задержки на элементах фазированной решетки зависит от таких параметров, как тип волны, величина апертуры, требуемый угол и глубина фокусировки.

Особенности ФАР

Известно множество типов фазированной решетки, однако наибольшее распространение получила линейная фазированная решетка благодаря своим преимуществам – простой конструкции, сравнительной легкости изготовления.

Существуют три основных способа управления лучом: электронное сканирование, динамическая фокусировка, секторное сканирование [11]. При электронном сканировании один фокальный закон переключается в пределах группы элементов, сканирование выполняется с постоянным углом и вдоль длинной стороны решетки (этот процесс эквивалентен механическому перемещению обычного одноэлементного преобразователя). При динамической фокусировке по глубине сканирование выполняется посредством изменения фокусного расстояния. Для излучения используется один и тот же импульс, тогда как в режиме приема решетка перефокусируется последовательно на разные значения глубины. При секторном сканировании (азимутальном, угловом) излучение производится одной и той же группой элементов при одном фокусном расстоянии последовательно под разными углами.

Отображения результатов контроля на экране при использовании дефектоскопов на фазированных решетках различны, они представляют собой разные типы разверток, называемых сканами. А-скан – форма представления сигналов в прямоугольной системе координат, где по оси ординат откладывается амплитуда принятых сигналов, а по оси абсцисс – время от цикла зондирования [12]. При механическом сканировании данные собираются при помощи датчиков координат. Затем данные представляются в удобном для анализа виде. Фазированные решетки обычно используют массив сгруппированных А-сканов (который представляет собой В-скан), полученных под разными углами, с использованием множества фокальных законов. Информация, полученная и записанная из одного положения фазированной решетки в виде большого числа А-сканов, представляется в реальном времени в виде секторного S-скана или электронного В-скана. S-скан – это изображение, полученное от пучков, сформированных при изменении угла ввода от меньшего к большему. В-сканом называется изображение, на котором совокупность принятых сигналов отображается точками, принадлежащими сечению объекта контроля в плоскости падения волны и параллельному ей. Как S-, так и В-сканы представляют собой изображение, содержащее информацию о прозвучиваемом материале и несплошностях, находящихся на пути ультразвука по всем направлениям, по которым осуществляется электронное сканирование. Отражение результатов прозвучивания в виде двумерного сечения объекта контроля дает прямое представление о результатах контроля. S-скан дает такие преимущества, как вывод изображения во время сканирования, истинное представление о глубине, двумерное представление контролируемого объема. Для получения лучшего изображения комбинируется линейное и секторное сканирование. Такая комбинация методов дает хорошо распознаваемые образы дефектов.

Комбинация сканов, полученных продольными и поперечными волнами, может быть весьма полезна для обнаружения и измерения размеров дефектов при возможности малых перемещений преобразователя. В этом случае активная часть апертуры преобразователя может перемещаться для получения оптимальных углов озвучивания. Различно сфокусированные звуковые пучки (цилиндрические, эллиптические, сферические) обеспечивают лучшую наглядность полезного сигнала на фоне шумов. При электронном сканировании преобразователь может механически перемещаться, после чего полученные данные можно объединить в общее высокоинформативное изображение дефекта с разных ракурсов. С помощью комбинации секторного электронного сканирования в одной плоскости и механического перемещения преобразователя в другой плоскости можно получить объемное изображение интересующего объекта контроля. Каждое положение преобразователя представляет собой «срез» дефекта в плоскости качания луча. Данные «срезы» можно сравнить с металлографическими срезами при определении реальных размеров и формы дефекта.

Исследование параметров решетки

Было изучено влияние параметров настройки (активной апертуры, фокусного расстояния, угловой разрешающей способности, типа фокусировки) на выявление отражателей в образце (рис. 1) с помощью ультразвукового

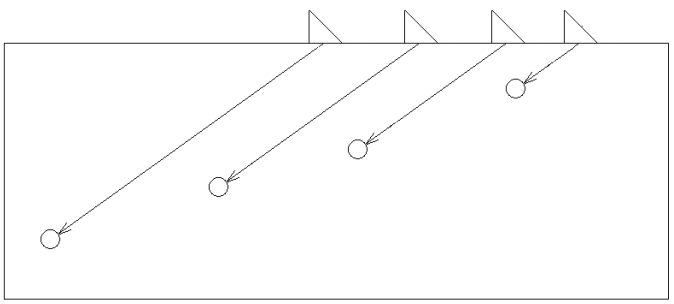


Рис. 1. Схема получения сигналов от отражателей в образце

дефектоскопа «HARFANGX-32» и ПЭП на ФАР с призмой. В ходе работы данные параметры подвергались изменениям, что позволило получить и впоследствии сравнить ряд S-сканов (протоколов), некоторые из них представлены на рис. 2–19.

Изображения фиксировались при прозвучивании углом ввода α, рассчитанным по закону Снеллиуса [13], исходя из известного угла призмы β и скорости распространения ультразвуковых волн в материалах объекта контроля (сталь) и призмы (рексолит):

$$\frac{\sin\alpha}{C_{t2}} = \frac{\sin\beta}{C_{l1}}.$$

При изучении влияния активной апертуры получены три протокола контроля: для 32, 16 и 8 активных элементов апертуры. На рис. 2 и 3 приведены протоколы, записанные при использовании 32 и 8 активных элементов, соответственно.

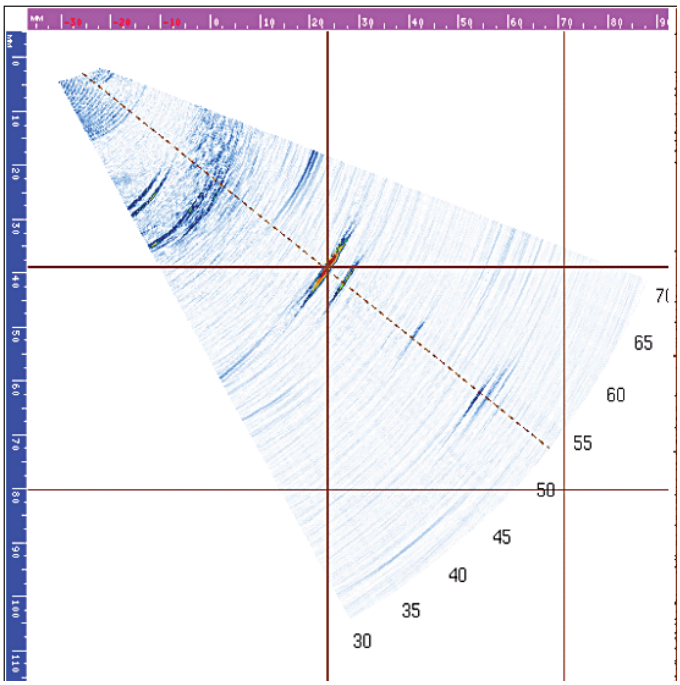


Рис. 2. Изучение влияния активной апертуры (32 активных элемента)

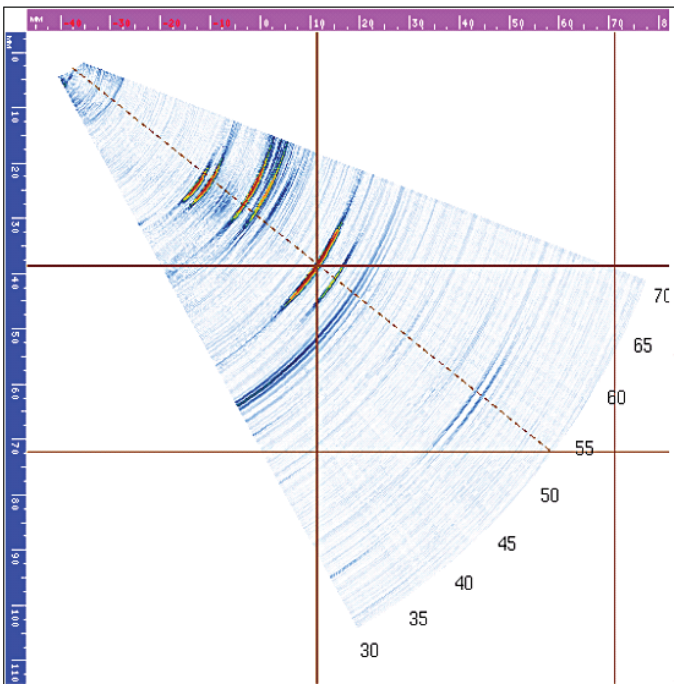


Рис. 3. Изучение влияния активной апертуры (8 активных элементов)

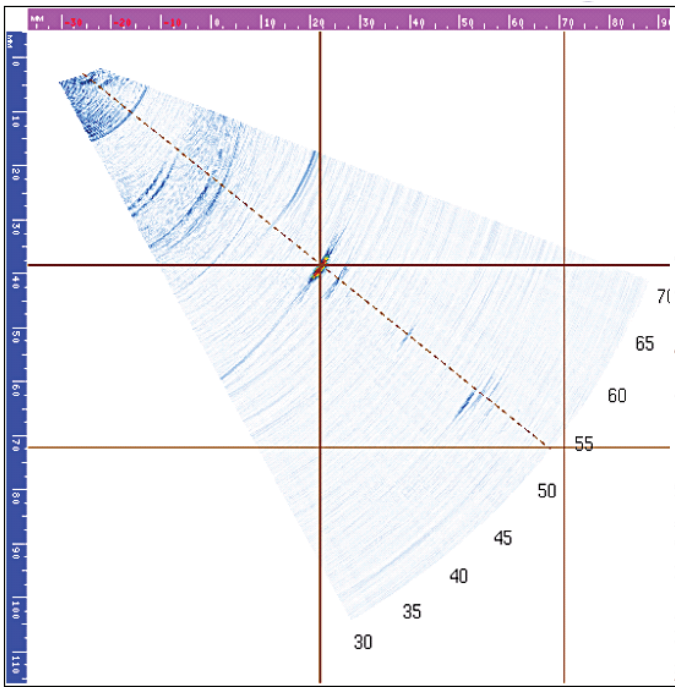


Рис. 4. Изучение влияния типа фокусировки (постоянный путь)

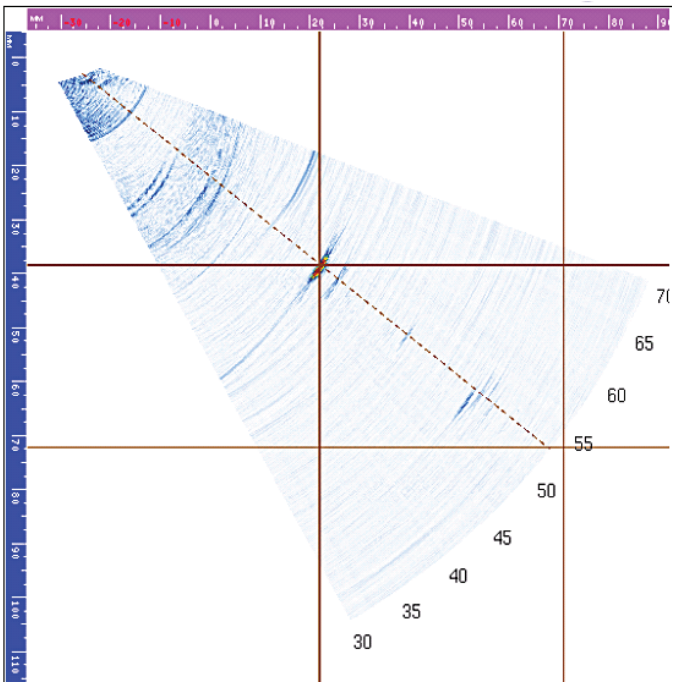


Рис. 5. Изучение влияния типа фокусировки (постоянная глубина)

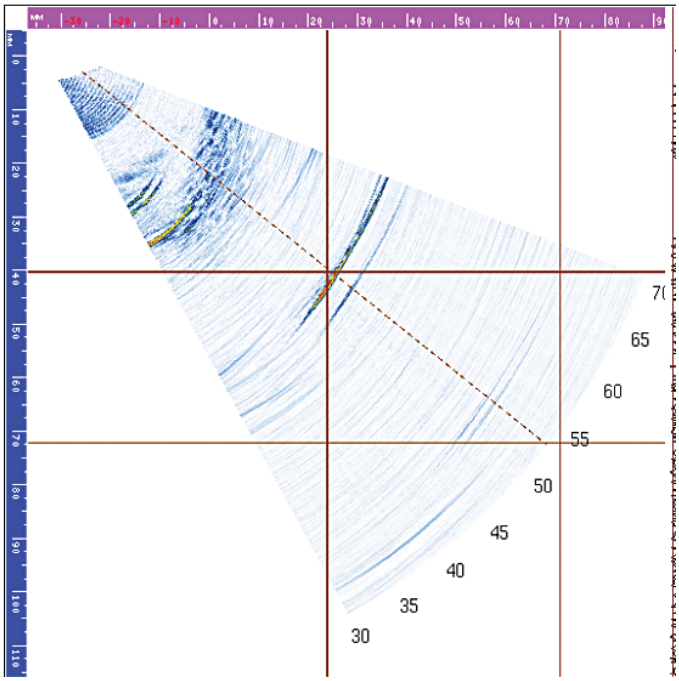


Рис. 6. Изучение влияния типа фокусировки (постоянное смещение)

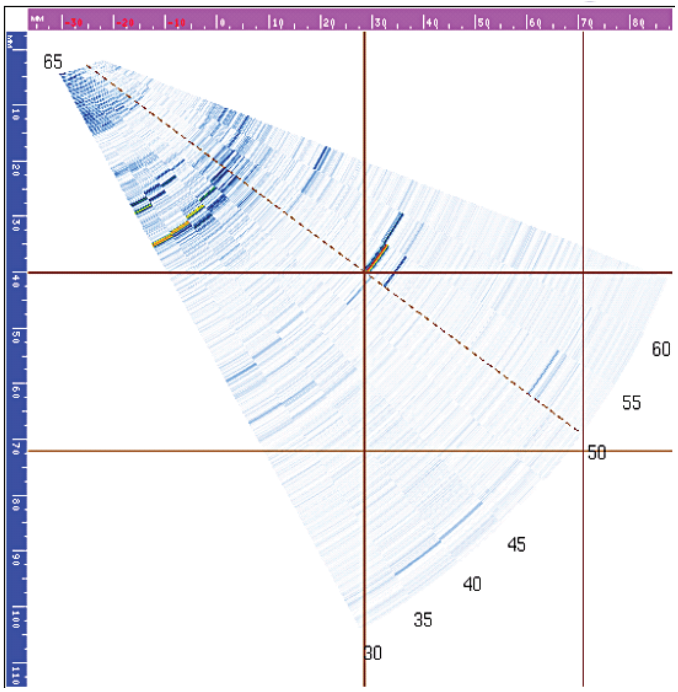


Рис. 8. Изучение влияния угловой разрешающей способности (5°)

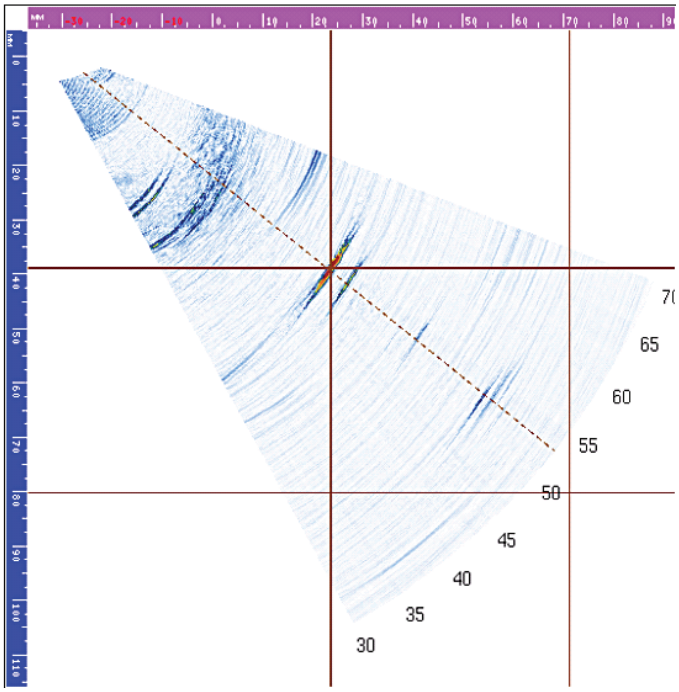


Рис. 7. Изучение влияния угловой разрешающей способности (0,5°)

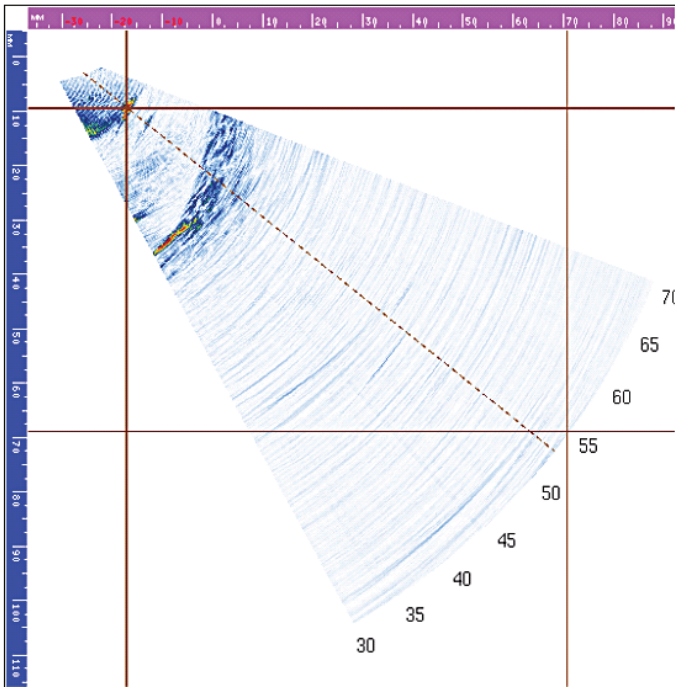


Рис. 9. Изучение влияния фокусного расстояния (выявление отражателя на глубине 10 мм при фокусировке на 10 мм)

Применение меньшего числа активных элементов апертуры сопровождается появлением побочных сигналов, не интересующих нас в данном исследовании, а также влияет на протяженность пятна, что видно при сравнении S-разверток на приведенных выше рисунках. Данный эффект объясняется зависимостью фокусного расстояния N_0 от активной апертуры A при неизменной величине длины волны λ:

$$N_0 = \frac{0,25 \cdot A}{\lambda}.$$

При изменении типа фокусировки – постоянный путь/глубина/смещение – получены протоколы, изображенные на рис. 4, 5 и 6, соответственно.

Тип фокусировки заметно влияет на характер изображения пятна от дефекта на S-скане. Несмотря на то, что в большинстве случаев данный параметр не редактируется (обычно при контроле устанавливается режим «постоянный путь»), неправильная настройка данного параметраможет негативно сказаться на результатах контроля.

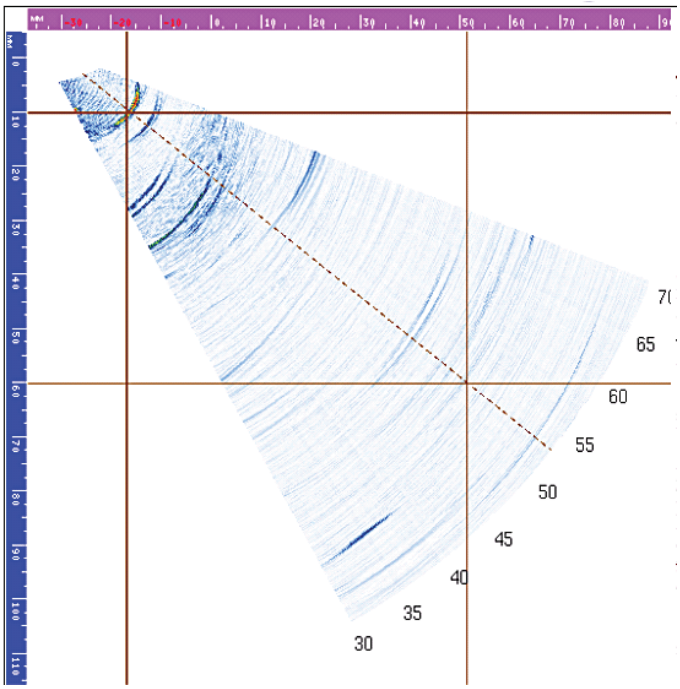


Рис. 10. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 10 мм при фокусировке на 60 мм)

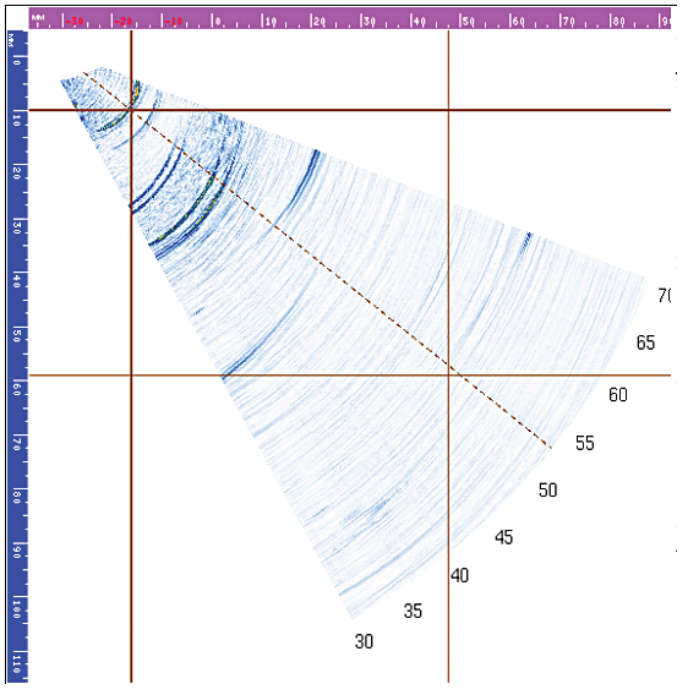


Рис. 11. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 10 мм при фокусировке на 1000 мм)

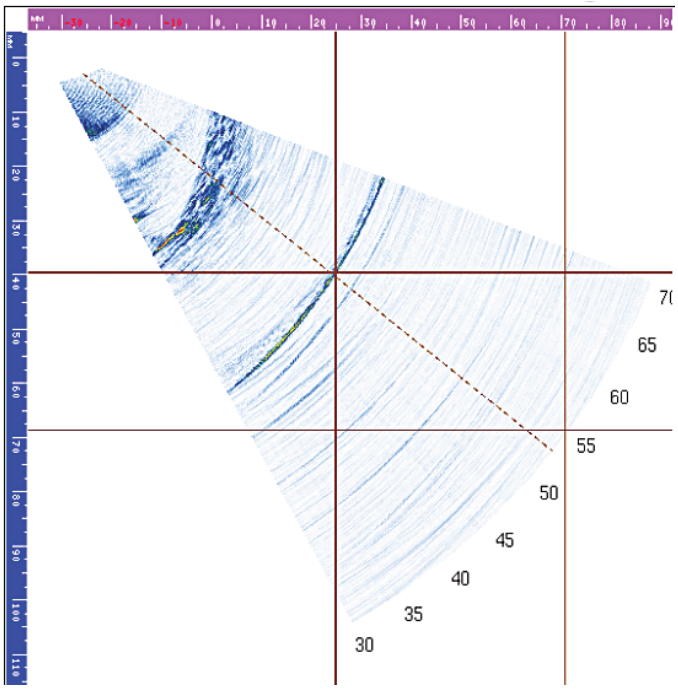


Рис. 12. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 40 мм при фокусировке на 10 мм)

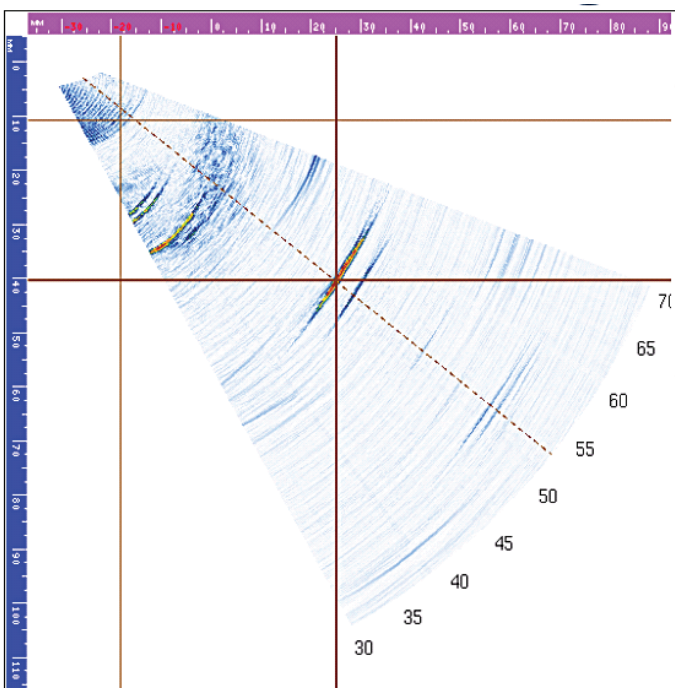


Рис. 13. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 40 мм при фокусировке на 30 мм)

Угловая разрешающая способность в процессе работы изменялась с 0,5° на 1,0° и 5,0°.

На рис. 7 и 8 для оценки представлены протоколы, полученные при значениях угловой разрешающей способности 0,5° и 5,0°.

Угловая разрешающая способность прямо влияет на полученные протоколы контроля. Ее увеличение приводит к ухудшению изображения на S-скане, к уменьшению разрешающей способности. При малых объемах контроля оптимальным вариантом для работы является значение угловой разрешающей способности 0,5–1°. При значительном объеме контроля для таких значений разрешающей способности будет создан большой массив данных, что может негативно повлиять на работу прибора [14]. Таким образом, данный параметр необходимо выбирать исходя из конкретной задачи и объекта контроля.

При изучении влияния фокусного расстояния (10, 30, 40, 60, 1000 мм), при получении эхо-сигналов от отражателей,

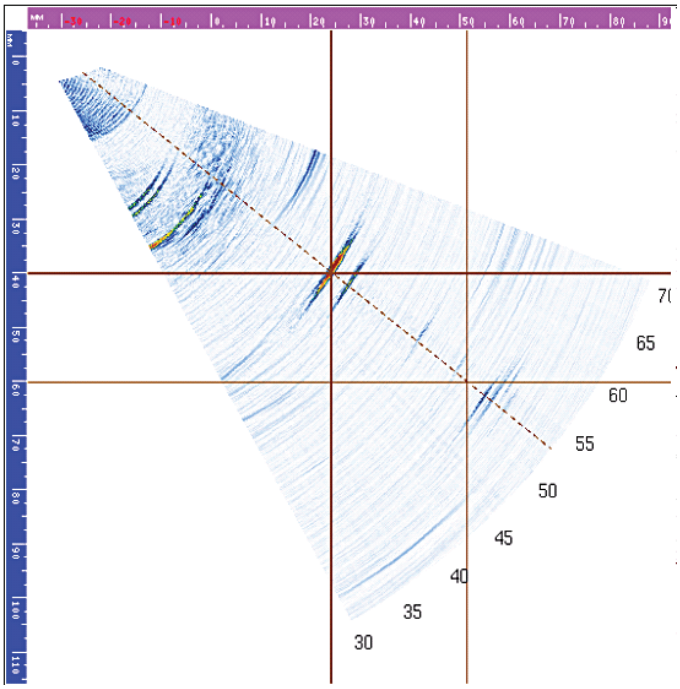


Рис. 14. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 40 мм при фокусировке на 40 мм)

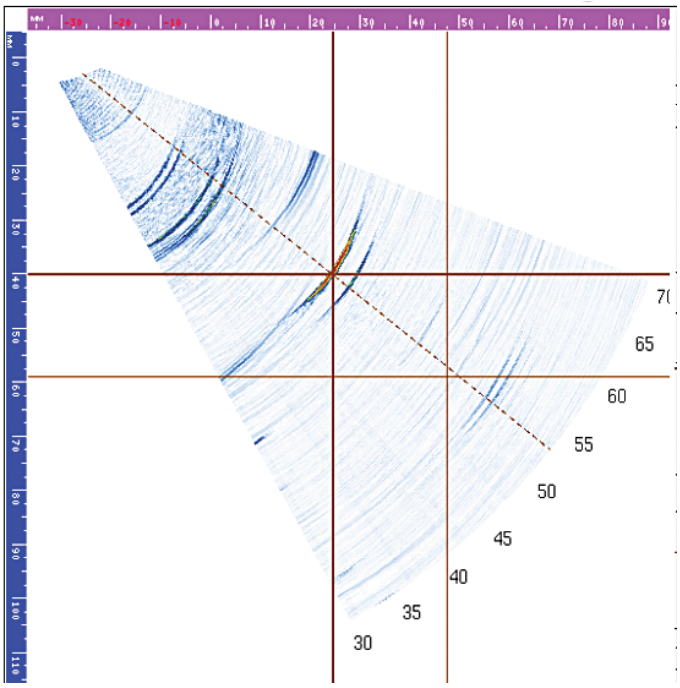


Рис. 15. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 40 мм при фокусировке на 1000 мм)

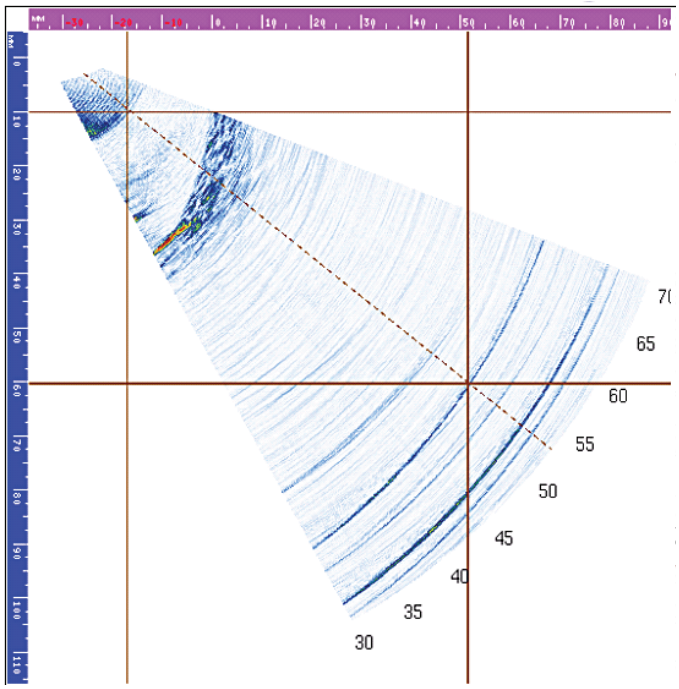


Рис. 16. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 60 мм при фокусировке на 10 мм)

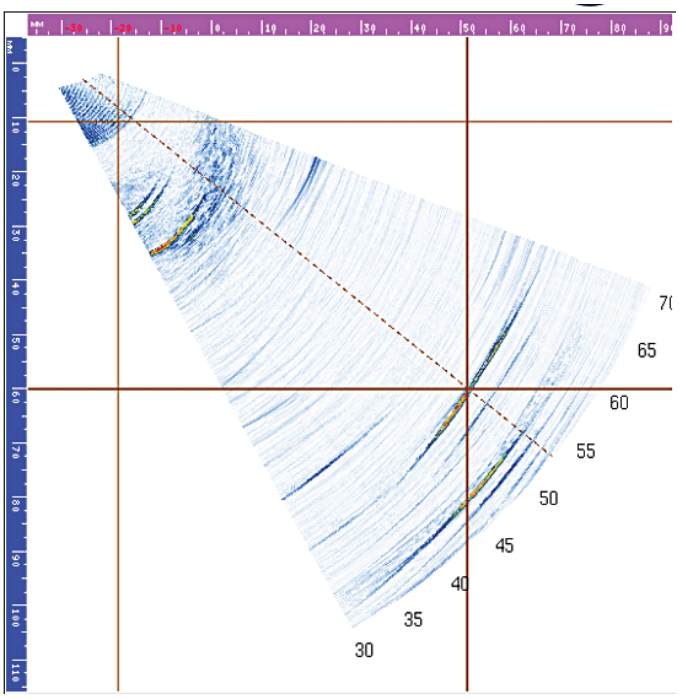


Рис. 17. Изучение влияния фокусного расстояния
(выявление отражателя на глубине 60 мм при фокусировке на 30 мм)

находящихся на разной глубине (10, 30, 40, 60 мм), получено большое количество протоколов, некоторые из которых изображены на рис. 9–19.

Сравнивая полученные протоколы, представленные на рис. 8–10, записанные при выявлении отражателя на глубине 10 мм при разных значениях фокусировки, обнаружилось, что, фокусируясь на глубину 10 мм, получили насыщенно окрашенное яркостное пятно на S-скане, однако при этой же настройке наблюдается большое количество помех на глубине, близкой к интересующей (сигналы, отображенные на S-скане ниже, являются сигналами от границы образца). При изменении фокусировки наблюдается уменьшение данных шумов, однако и у полезного сигнала яркостная (она же амплитудная характеристика на А-скане) характеристика на S-скане уменьшается, пятно от отражателя становится более протяженным.

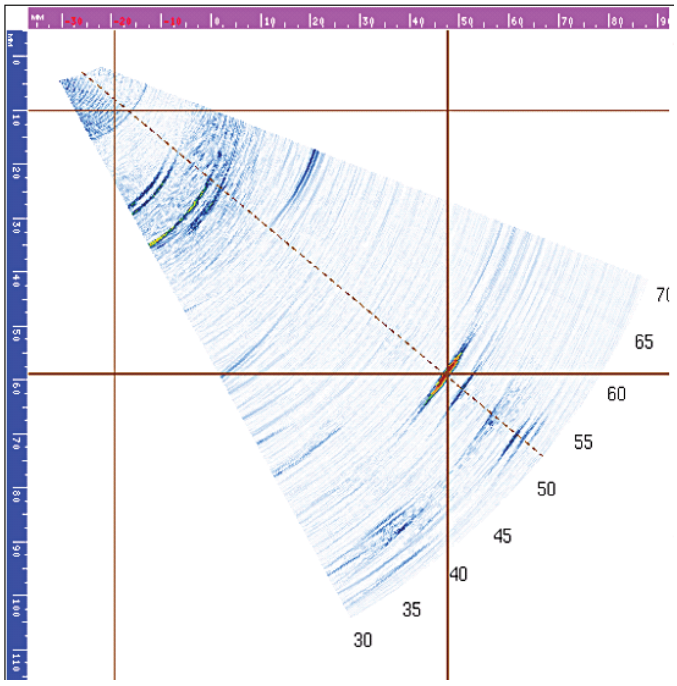


Рис. 18. Изучение влияния фокусного расстояния (выявление отражателя на глубине 60 мм при фокусировке на 60 мм)

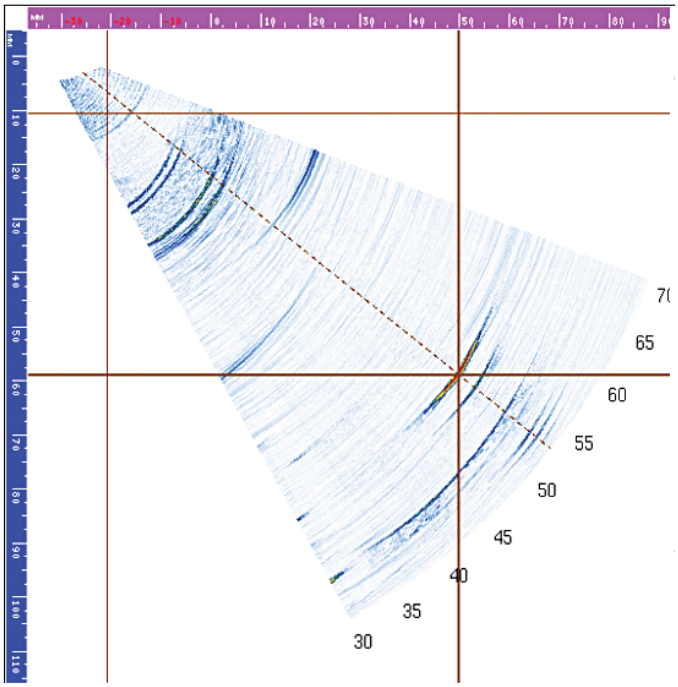


Рис. 19. Изучение влияния фокусного расстояния (выявление отражателя на глубине 60 мм при фокусировке на 1000 мм)

Как ожидалось, при выявлении отражателя на глубине 40 мм (при фокусном расстоянии 40 мм) было получено наиболее яркое, четкое изображение на S-скане. Сигнал от данного отражателя, полученный при фокусном расстоянии 40 мм, схож с полученным при фокусировке на 30 мм. Это объясняется небольшой разницей между фокусными расстояниями, в отличие от примера с отражателем на глубине 10 мм [15]. По той же причине не рассматривались протоколы, полученные от отражателя на глубине 30 мм: они схожи с результатами для отражателя на глубине 40 мм. Значительно различаются протоколы, полученные при значениях фокусного расстояния 10 мм и 1000 мм – пятно на S-скане более протяженное.

Сравнивая полученные протоколы, представленные на рис. 16–19, записанные при выявлении отражателя на глубине 60 мм при разных значениях фокусировки, обнаружилось, что, фокусируясь на глубину 10 мм, невозможно определить отражатель, не зная заранее его глубину. Под сигналом от интересующего отражателя на рис. 16, 17 и 19 находится сигнал, превышающий по глубине образец (переотраженный сигнал). Изображение этого сигнала присутствует и при фокусировке на глубину 60 мм, однако он выглядит значительно меньше. Таким образом, можно сделать вывод, что правильная настройка фокусировки позволяет исключить ложные срабатывания и фиксацию несплошностей.

Заключение

На основании исследований можно сделать ряд выводов. Использование большего числа активных элементов апертуры благотворно влияет на выявляемость отражателей. Угловую разрешающую способность лучше принимать равной 1°, так как ее уменьшение не приведет к значительным изменениям, а только создаст большой массив данных, который может затруднить работу дефектоскопа; увеличение угловой разрешающей способности ведет к ухудшению изображения на S-скане и к уменьшению разрешающей способности.

Тип фокусировки влияет на характер изображения на S-скане. Редактирование данного параметра может потребоваться для выявления дефектов, направление которых заранее известно или предполагаемо. Фокусное расстояние значительно влияет на результат контроля. Данный параметр важно не только правильно задать при подготовке к работе, но также корректировать при измерении характеристик дефектов для наибольшей точности. Верная настройка параметров контроля обеспечит правильное обнаружение дефектов и измерение их характеристик, а также позволит избежать фиксации ложных сигналов.

Литература

1. Дымкин Г. Я. Физические основы ультразвуковой дефектоскопии: учеб. пособие / Г. Я. Дымкин, С. Р. Цомук. – СПб.: ПГУПС, 1997. – 102 с.

2. Прохоренко А. А. Определение возможностей дефектоскопов с ФАР по фокусировке ультразвукового пучка / А. А. Прохоренко // В мире неразрушающего контроля. – 2014. – № 3 (65). – С. 56-60.

3. http://www.olympus-ims.com (дата обращения 29.05.2015).

4. http://www.defektoskopist.ru (дата обращения 16.11.2015).

5. ГОСТ 23066-79. Устройства управления лучом фазированных антенных решеток. Термины и определения. – М., 1979.

6. РД19.100.00-КТН-001-10. Неразрушающий контроль сварных соединений при строительстве и ремонте магистральных трубопроводов. – М., 2010.

7. ISO 13588:2012. Non-destructivetestingofwelds. Ultrasonic testing. Useofautomatedphasedarraytechnology. 2012

8. Коновалов Р. С. Акустические преобразователи для неразрушающего контроля: учеб. пособие. Ч. 1. Излучение

и регистрация акустических волн / Р.С. Коновалов, В.П. Лохов. – СПб.: ФГБОУ ВПО ПГУПС, 2015. – 65 с.

9. http://www.ndt.net (дата обращения 05.05.2015).

10. Dube N. Introduction to Phased Array Ultrasonic Technology Applications / N. Dube. – Canada: R/D Tech, 2004. – 376 p.

11. Кретов Е.Ф. Ультразвуковая дефектоскопия в энергомашиностроении / Е.Ф. Кретов. – 4-е изд., перераб. – СПб.: СВЕН, 2014. – 312 с.

12. http://www.harfangveo.ru (дата обращения 05.05.2015).

13. Гурвич А.К. Неразрушающий контроль. Общие вопросы. Контроль проникающими веществами / А.К. Гурвич, И.Н. Ермолов, С.Г. Сажин; под ред. проф. В.В. Сухорукова. – М.: Высш. шк., 1992. – 241 с.

14. Дефектоскоп ультразвуковой на фазированных решетках Х-32. Руководство по эксплуатации.

15. Hosseini S. Resolutions Studied on an Electronically Focused Ultrasonic Array / S. Hosseini, S.O. Harrold, J.M. Reeves // British J. Non-Destr. Test. – 1985. – Vol. 27, no. 4. – P. 234-238.

Influence of Parameters of a Linear Phased Array on the Ability to Identify the Reflectors

Kormiltseva M. F., Churova V. V.
Emperor Alexander I St. Petersburg State Transport University
Saint-Petersburg, Russia
Mariekor@outlook.com, Postkiser@mail.ru

Abstract. **The article describes the principle and characteristics of ultrasonic probes with a phased array. Studied parameters of flaw detector settings on the phased array and their influence on the tests results, namely the S-scans.**

Keywords: **non-destructive testing, ultrasonic flaw detection, ultrasonic testing method, phased array, probe.**

References

1. Dymkin G.Ya., Comuk S.R. Fizicheskie osnovy ultrazvukovoj defektoskopii. Uchebno eposobie [Basic physical principles of ultrasonic testing]. St. Petersburg, Petersburg State Transp. Univ., 1997, 102 p.

2. Prokhorenko A.A. Identify Opportunities Flaw Detector with Phased Array for Focusing the Ultrasonic Beam [Opredelenie Vozmozhnostei Defektoskopov s FAR po Fokusirovke Ul'trazvukovogo Puchka], *V Mire Nerazrushaiushchego Kontrolia [In the World of NDT]*, 2014, no. 3 (65), pp. 56-60.

3. http://www.olympus-ims.com (accessed 29.05.2015).

4. http://www.defektoskopist.ru (accessed 16.11.2015).

5. GOST 23066-79. Control Devices for Beam Phased Arrays. Terms and Definitions [Ustroistva Upravleniia Luchom Fazirovannykh Antennykh Reshetok. Terminy i Opredeleniia], 1979.

6. RD19.100.00-KTN-001-10. Non-destructive Testing of Welded Joints at Main Pipelines Construction and Repair [Nerazrushaiushchii Kontrol Svarnykh Soedinenii pri Stroitelstve i Remonte Magistralnykh Truboprovodov], 2010.

7. ISO 13588:2012. Non-destructive testing of welds. Ultrasonic testing. Use of automated phased array technology, 2012.

8. Konovalov R.S., Lokhov V.P. AkusticheskiePreobrazovatelidliaNerazrushaiushchegoKontrolia. UchebnoePosobie. Chast 1. Izluchenie i RegistratsiiaAkusticheskikhVoln [Acoustic Probes for Non-destructive Testing. Study Guide. Part 1: Radiation and Registration of Acoustic Waves], St. Petersburg, Emperor Alexander I St. Petersburg State Transp. Univ., 2015, 65 p.

9. http://www.ndt.net (accessed 05.05.2015).

10. Noel Dube. Introduction to Phased Array Ultrasonic Technology Applications, Canada, R/D Tech, 2004, 376 p.

11. Kretov E.F. UltrazvukovaiaDefektoskopiia v Energomashinostroenii [Ultrasonic Testing in Power-plant Engineering], St. Petersburg, SVEN, 2014, 312 p.

12. http://www.harfangveo.ru (accessed 05.05.2015).

13. Gurvich A.K., Ermolov I.N., Sazhin S.G. Nerazrushayushchijkontrol. Obshchievoprosy. Kontrol pronikayushchimi veshchestvami [Non-destructive Testing. General issues. Penetrant control], ed. V.V. Suhorukov. Moscow, Vysshaya Shkola, 1992, 241 p.

14. Defektoskop Ultrazvukovoi na Fazirovannykh Reshetkakh X-32. Rukovodstvo po Ekspluatatsii [Ultrasonic Flaw Detectorwith Phased Array X32. Service Manual].

15. Hosseini S., Harrold S.O., Reeves J.M. Resolutions Studied on an Electronically Focused Ultrasonic Array. *British J. Non-Destr. Test.*, 1985, vol. 27, no. 4, pp. 234-238.

Протокол стойкого шифрования по разделяемому ключу малого размера в группе точек эллиптической кривой

Рыжков А. В.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Санкт-Петербург, Россия
Ryzhkov.alex@gmail.com

Аннотация. **Для гарантированной защиты информации, передаваемой по открытым каналам, в условиях ограниченности ключевого материала недавно был предложен протокол на основе объединения процедур бесключевого (коммутативного) шифрования и шифрования по секретному ключу малого размера (до 56 бит). С целью повышения производительности процедур коммутативного шифрования представляет интерес реализация указанного протокола в группе точек эллиптической кривой (ЭК). В статье с учетом особенностей использования ЭК представлены два варианта протокола. В первом варианте механизм аутентификации из исходного протокола переносится без изменений, что накладывает ограничение на повторное использование секретного ключа малого размера. Во втором варианте предлагается новый механизм аутентификации, позволяющий снять указанное ограничение.**

Ключевые слова: **протокол стойкого шифрования, ключ малого размера, коммутативный шифр, задача дискретного логарифмирования, эллиптическая кривая.**

Введение

Если необходимо передать конфиденциальные сообщения по открытым каналам при наличии у отправителя и получателя общего секретного ключа малого размера (например, 32, 40 или 56 бит), то непосредственное шифрование сообщений по разделяемому ключу небезопасно, поскольку, перехватив криптограмму, нарушитель имеет практическую возможность подобрать ключ путем перебора по ключевому пространству. Однако ключ такого размера находит интересное применение в протоколах, включающих использование симметричной и ассиметричной криптографии.

Недавно был предложен протокол стойкого шифрования по ключу малого размера (ПМК) путем вовлечения в процесс шифрования на ключе малого размера процедур коммутативного криптографического преобразования, не требующего использования разделяемых секретных ключей [1–4]. Последние относятся к так называемым процедурам бесключевого шифрования [5], недостатком которых является то, что требуется обеспечить возможность аутентификации передаваемых сообщений. Таким образом, коммутативное шифрование обеспечивает заданный уровень стойкости путем выбора соответствующих параметров бесключевого шифрования, а малый ключ используется в механизме аутентификации передаваемых сообщений. Существующие ПМК основываются на вычислительной сложности задачи дискретного логарифмирования по простому модулю, имеющей субэкспоненциальную сложность [1, 2]. Для повышения производительности процедур коммутативного шифрования можно реализовать ПМК в группе точек эллиптической кривой (ЭК), заданной над конечным полем, так как при правильном выборе ЭК обеспечивается экспоненциальная стойкость [6, 7], что позволяет существенно уменьшить размер чисел, над которыми выполняются операции умножения по модулю, за счет чего повышается производительность алгоритмов шифрования.

Статья построена следующим образом. В первой части рассматривается протокол бесключевого шифрования как базовый элемент дальнейшего построения ПМК, а также особенности построения в группе точек ЭК и применения ключа малого размера при таком построении. Во второй части предлагается базовая реализация ПМК в группе точек ЭК (ПМК1) с использованием механизма аутентификации из исходного протокола, что в случае реализации на основе ЭК накладывает ограничение на повторное использование секретного ключа малого размера. Далее предлагается возможная модификация протокола (ПМК2) с целью снятия указанного ограничения.

Протокол бесключевого шифрования

Наиболее яркий пример решения задачи защищённой передачи информации без предварительной договорённости о ключе/обмена ключами – трехпроходной протокол Шамира [3, с. 516], который позволяет передать секретное сообщение по открытому каналу (защищая информацию от несанкционированного доступа со стороны пассивного нарушителя) без использования отправителем и получателем общих (разделяемых) секретных ключей или выработки общего ключа. С учетом последнего данный протокол может быть назван протоколом бесключевого шифрования. Протоколы данного типа основаны на использовании стойкого алгоритма коммутативного шифрования (АКШ) – алгоритма шифрования E_k сообщения M по ключу k, для которого выполняется условие коммутативности $E_{K_1}(E_{K_2}(M)) = E_{K_2}(E_{K_1}(M))$. D_k – процедура расшифровки на ключе k в алгоритме E_k, параметры A и B являются секретными ключами отправителя и получателя, соответственно. Схема протокола в общем описывается следующим образом:

1) отправитель сообщения M шифрует M по своему секретному ключу A, получает шифротекст $C_1 = E_A(M)$ и посылает C_1 по открытому каналу получателю;

2) получатель зашифровывает шифротекст C_1 по своему секретному ключу B, получает шифротекст $C_2 = E_B(C_1) = E_B(E_A(M))$ и посылает C_2 отправителю;

3) отправитель, используя процедуру расшифровки D по своему секретному ключу A, преобразует сообщение C_2, получает шифротекст $C_3 = D_A(C_2) = E_B(M)$ и посылает C_3 получателю сообщения M;

4) получатель из полученного шифротекста C_3 восстанавливает сообщение M по формуле $M = D_B(E_B(M))$.

Используемые в этом протоколе локальные (неразделяемые) ключи A и B выбираются каждой стороной независимо, причём передаваемое сообщение может разбиваться на множество блоков, каждый из которых может преобразовываться с использованием разных пар локальных ключей. Заметим, что на третьем шаге протокола отправитель передаёт шифротекст C_3 – сообщение M, зашифрованное на ключе получателя, – но в то же время отправитель не знает ключа получателя. Получение такого шифротекста обеспечивается свойством коммутативности: $D_A(C_2) = D_A(\mathbf{E_B}(\mathbf{E_A}(\mathbf{M}))) = D_A(\mathbf{E_A}(\mathbf{E_B}(\mathbf{M}))) = E_B(M)$.

В качестве коммутативной функции шифрования А. Шамир и – независимо – Дж. Омура предложили возведение в степень по простому модулю p [8]. Также известна аналогичная схема при реализации коммутативной функции как возведение в степень по модулю неприводимого многочлена в поле двоичных многочленов – схема шифрования Месси – Омуры [9]. В последнем случае возможно построение «идеального» коммутативного шифра в конечных полях двоичных многочленов, степени которых являются простыми числами Мерсенна [10, 11], т. е. шифра, свободного от «слабых» сообщений, шифрование которых дало бы возможность потенциальному нарушителю вычислить часть секретного ключа.

Приведённая схема бесключевого шифрования представляет практический интерес, как и схема открытого распределения ключей Диффи – Хеллмана, позволяя двум сторонам, не разделяющим общий секрет, конфиденциально обменяться информацией по незащищённому каналу. В то же время практическое значение протокола бесключевого шифрования ограничено тем, что он не обеспечивает стойкости к атакам активного нарушителя, который может выдавать себя за отправителя или получателя сообщения (уязвим к атаке «человек посередине»).

В ПМК упомянутый недостаток устраняется за счет использования механизма аутентификации передаваемых сообщений посредством шифрования передаваемых криптограмм симметричным алгоритмом на разделяемом ключе малого размера, благодаря чему потенциальный нарушитель не имеет возможности выдать себя за легального отправителя или получателя сообщения и найти значение секретного ключа методом угадывания или полного перебора. В качестве коммутативной функции в исходной работе [1, 2] использовано возведение по простому модулю p, т. е. задача дискретного логарифмирования в конечном простом поле, имеющая субэкспоненциальную сложность. При таком подходе каждое сообщение, кроме сообщения, представляющего нулевую битовую цепочку, интерпретируется ненулевым элементом поля. Однако для задания высокой стойкости АКШ требуется использовать поля́, порядок которых выражается простым числом или степенью простого числа размером не менее 1024 бит, что существенно ограничивает производительность АКШ. При этом увеличение быстродействия АКШ путем выбора в качестве модуля простого числа p специального вида связано также со следующим ограничением: в разложении числа $p - 1$ будут содержаться делители сравнительно малого размера, которые определяют наличие «слабых» значений сообщения. При использовании ЭК возможны существенное уменьшение размера чисел, над которыми выполняются операции умножения по модулю, а также выбор специальной структуры модуля p без того, чтобы это приводило к появлению «слабых» сообщений.

Особенности построения протокола в группе точек ЭК

Построение протоколов шифрования с использованием групп рациональных точек ЭК для выполнения процедур шифрования представляет интерес в связи с тем, что при правильном выборе ЭК обеспечивается экспоненциальная стойкость [6, 7], что позволяет существенно уменьшить размер чисел, над которыми выполняются операции умножения по модулю, за счет чего повышается производительность алгоритмов шифрования.

Обычно предполагается, что входное сообщение, предназначенное для шифрования, не должно иметь ограничений, кроме как ограничений на длину шифруемых блоков или на максимально допустимое значение при его интерпретации как двоичного числа. Это связано с тем, что в реальных ситуациях может понадобиться шифрование разных сообщений.

Данное требование трудно реализовать при разработке коммутативных шифров с использованием ЭК, заданных над конечными полями, поскольку координаты точек ЭК должны удовлетворять некоторому уравнению третьей степени, а значит, не все пары значений соответствуют точкам ЭК. Синтез АКШ с использованием вычислений на ЭК требует решения задачи кодирования сообщений точками ЭК.

Один из подходов к решению этой задачи предложил Н. Коблиц: «встраивать» сообщения в точку ЭК (вероятностное кодирование сообщения точкой ЭК), набросок алгоритма можно найти в [7, с. 202]. Для построения АКШ в группе точек ЭК на основе способа вероятностного кодирования сообщения точкой ЭК сообщение дополняется случайными битами (размещение и количество которых заранее оговаривается) так, что получаемые значения являются абсциссами точек ЭК. Задаваемые таким образом точки далее используются в коммутативных преобразованиях. Сообщение из точки ЭК декодируется простым отбрасыванием числа добавленных при кодировании бит. Важным элементом при построении алгоритма вероятностного кодирования сообщения точкой ЭК является выбор достаточной длины присоединяемой битовой последовательности для обеспечения пренебрежимо малой вероятности следующих событий:

- невозможно найти кодирующую точку для случайного сообщения;
- существует хотя бы одного сообщение заданной длины, которое невозможно закодировать точкой ЭК.

В [12, 13] показано, что для различных значений порядка простого и конечного двоичного поля, над которым задана ЭК, достаточным является увеличение сообщения не более чем на 5 %.

Другим вариантом решения задачи отображения сообщения в точку ЭК является способ «расщепления» сообщения

[13]: оно представляется по достаточно простой формуле парой из двух значений, одно из которых – абсцисса случайно выбранной точки ЭК, второе – значение случайного вида, необходимое для восстановления исходного сообщения из точки ЭК. При «расщеплении» сообщения размер шифротекста вдвое превышает размер исходного сообщения: сообщение m представляется парой значений (C, M_x), где C – значение произвольного вида, а M_x – значение абсциссы точки ЭК. При этом сам процесс кодирования сообщения точкой ЭК всегда выполняется за одну итерацию по простой формуле расщепления, например $C = M + K_x \bmod p$ в случае задания ЭК над полем $GF(p)$. Задаваемые таким образом точки далее используются в коммутативных преобразованиях. Сообщение из точки ЭК декодируется по формуле, соответствующей использованной для расщепления, в данном примере – $m = C - K_x \bmod p$.

Можно объединить два указанных способа – вероятностного кодирования и «расщепления» – в общий алгоритм, чтобы уменьшить среднее превышение размера шифротекста над исходным сообщением (до 3 %) и гарантированно представить любое сообщение точкой ЭК [13].

Указанные алгоритмы универсальны, т. е. не накладывают ограничений на шифруемые сообщения. В предлагаемых в настоящей работе протоколах можно применить любой алгоритм отображения сообщения в точку ЭК.

Особенности применения разделяемого ключа малого размера при построении в группе точек ЭК

Стандартные протоколы симметричного шифрования гарантируют стойкость при использовании ключей достаточно большого размера, например 128 или 256 бит, использование ключа малого размера (30–50 бит) небезопасно, так как при перехвате криптограммы практически можно найти ключ путём перебора по ключевому пространству. Может показаться парадоксальным, что ключи такого размера находят применение для построения протоколов стойкого шифрования. Идея такого построения заключена в комбинировании алгоритмов асимметричной и симметричной криптографии, малый ключ используется не напрямую для шифрования, а для процедур аутентификации сторон протокола, причём обеспечивается неразрывность процедур шифрования и аутентификации.

Применение разделяемого секретного ключа в процедурах аутентификации сообщений принципиально отличается от их применения в процедурах шифрования сообщений. Это отличие состоит в том, что в последнем случае у потенциального атакующего имеется возможность многократно опробовать разные значения ключа (атака по словарю), пока не будет найден секретный ключ, который использовался для шифрования, тогда как в первом случае имеется возможность только однократной попытки угадать секретный ключ и навязать легальному пользователю ложное сообщение. Вероятность такого обмана достаточно мала даже в случае использования коротких разделяемых ключей и составляет 2^{-k}, где k – длина ключа в битах.

Впервые такое применение малого ключа (пароля) было предложено С. Беловином и М. Мерритом: так была обозначена новая группа протоколов обмена зашифрованными ключами (EKE – encrypted key exchange), в которых общий секретный ключ используется для шифрования генерированного случайным образом открытого ключа [14]. В работе приводятся примеры использования указанного подхода с разными системами асимметричного шифрования.

Необходимым условием многократного использования одного и того же секретного ключа малого размера в исходном ПМК и в EKE [14] является псевдослучайность (вычислительная неотличимость от случайных значений) передаваемых шифротекстов, что предотвращает получение атакующим данных, использование которых позволяет многократно проверить предполагаемые значения разделяемого секретного ключа. Действительно, шифрование данных такого типа приводит к получению криптограмм, по которым определить короткий ключ шифрования методом перебора по пространству возможных ключей не представляется возможным, поскольку каждый испытываемый ключ приведет к восстановлению из криптограммы некоторого случайного (псевдослучайного) исходного текста. Для атакующего каждое допустимое значение ключа является равноправным, т. е. у него нет вычислительно эффективного критерия отбраковки неверных значений ключа.

Данное требование трудно реализовать при разработке ПМК с использованием ЭК, заданных над конечными полями, поскольку координаты точек ЭК, представляющие шифротексты, должны удовлетворять некоторому уравнению третьей степени (уравнению ЭК), т. е. обладать вычислительной неотличимостью от случайных значений. В результате критерий принадлежности точки используемой эллиптической кривой может быть использован злоумышленником для отбраковки неверных значений ключа при атаке полного перебора.

Один из возможных подходов к решению этой задачи – использование разделяемого малого ключа шифрования K таким образом, чтобы у злоумышленника не было критерия для отбраковки неверных значений ключа при атаке полного перебора по ключевому пространству ключа K, для чего необходимо, чтобы:

- либо сообщение до шифрования на малом ключе K было вычислительно неотличимо от случайной последовательности (а не ограничивалось множеством точек ЭК) – детальное рассмотрение этого вопроса представляет собой тему отдельной работы;
- либо само шифрование на малом ключе K оперировало только множеством точек ЭК, т. е. и при шифровании, и при дешифровании результат являлся точкой ЭК. Реализация данного подхода для стандартных алгоритмов симметричного шифрования неочевидна, однако он может быть выполнен на основе вычислений в группе точек ЭК, что показано в предлагаемом далее протоколе (ПМК2).

Базовая схема протокола стойкого шифрования на эллиптической кривой (ПМК1)

Пусть дана ЭК E над полем $GF(p)$, порядок которой $\#E = \Omega$ делится на большой простой делитель q (разрядностью не менее 160 бит) или равен большому простому числу. Ключи АКШ генерируется обеими сторонами в виде двух взаимно обратных по модулю Ω чисел e и $d = e^{-1} \bmod \Omega$. Ключ K есть разделяемый отправителем и получателем ключ малого размера для его использования в алгоритме симметричного шифрования (АСШ) G, например [15].

Передача сообщения m выполняется по следующему алгоритму.

1. Отправитель:

• кодирует передаваемое сообщение m точкой ЭК, например методом вероятностного кодирования $M = \Pr(m)$;

• зашифровывает полученную точку M на своём ключе e_1 АКШ по формуле $C_1 = Me_1$;

• зашифровывает полученное значение C_1 на общем ключе K АСШ G по формуле $C_1' = G_k(C_1) = G_k(Me_1)$;

• пересылает полученное значение получателю.

2. Получатель:

• расшифровывает переданное значение общим ключом K АСШ: $C_1 = G_k^{-1}(C_1')$;

• умножает полученное значение на свой ключ e_2 АКШ: $C_2 = C_1e_2$;

• зашифровывает полученное значение на общем ключе K АСШ: $C_2' = G_k(C_2) = G_k(C_1e_2) = G_k(Me_1e_2)$;

• пересылает полученное значение C_2' отправителю.

3. Отправитель:

• расшифровывает переданное значение общим ключом K АСШ: $C_2 = G_k^{-1}(C_2')$;

• умножает полученное сообщение на свой ключ расшифрования d_1 АКШ: $C_3 = C_2d_1 = Me_1e_2d_1 = Me_2$;

• зашифровывает полученное значение на общем ключе K АСШ: $C_3' = G_k(Me_2)$;

• пересылает полученное значение C_3' получателю.

4. Получатель:

• расшифровывает переданное значение общим ключом K АСШ: $C_3 = G_k^{-1}(C_3') = Me_2$;

• получает значение точки ЭК M умножением на свой ключ расшифрования d_2 АКШ: $M = C_3d_2 = Me_2d_2$;

• восстанавливает исходное сообщение m из полученной точки ЭК M декодированием по алгоритму вероятностного кодирования $m = Pr^{-1}(M)$.

Итоговая схема протокола приведена на рис. 1.

Стойкость ПМК определяется стойкостью используемого алгоритма коммутативного шифрования. Разделяемый секретный ключ K служит для того, чтобы предотвратить атаки активного нарушителя, в которых нарушитель выдаёт себя за легального отправителя или получателя. Это достигается путем шифрования на малом ключе K с использованием алгоритма симметричного шифрования точек ЭК, получаемых при процедурах коммутативного шифрования. В то же время такое использование симметричного шифрования предоставляет злоумышленнику критерий для отбраковки неверных значений ключа K при атаке полного перебора по ключевому пространству на основе перехваченных шифротекстов, а именно: передаваемое сообщение до шифрования секретным ключом K малого размера соответствовало абсциссе точки ЭК. При разработке способа вероятностного кодирования было показано [12], что случайное значение является абсциссой точки ЭК с вероятностью 0,5, что позволяет злоумышленнику методом перебора по пространству возможных ключей и проверкой полученного значения на соответствие точке ЭК уменьшать множество возможных значений ключа в два раза на каждом перехваченном шифротексте [16]. Таким образом, для нахождения значения ключа в среднем необходимо число перехваченных шифротекстов, равное битовой длине ключа.

Попытки модификации протокола – путем использования дополнительного разового ключа R для шифрования передаваемых на шагах протокола сообщений вместо малого ключа K, а также схемы на основе иммитовставок из исходной работы [1] – не устранили указанный недостаток. В первом случае это обусловлено тем, что утечка информации о разовом ключе R приводила к утечке информации о ключе K, во втором случае – необходимостью однократного шифрования точки ЭК на коротком ключе K.

Отправитель		**Получатель**
$M = Pr(m)$		
$C_1 = Me_1$		
$C_1' = G_k(C_1) = G_k(Me_1)$		
	$\xrightarrow{C_1' = G_k(Me_1)}$	
		$C_1 = G_k^{-1}(C_1')$
		$C_2 = C_1e_2 = Me_1e_2$
		$C_2' = G_k(C_2) = G_k(Me_1e_2)$
	$\xleftarrow{C_2' = G_k(Me_1e_2)}$	
$C_2 = G_k^{-1}(C_2')$		
$C_3 = C_2d_1 = Me_1e_2d_1 = Me_2$		
$C_3' = G_k(Me_2)$		
	$\xrightarrow{C_3' = G_k(Me_2)}$	
		$C_3 = G_k^{-1}(C_3') = Me_2$
		$M = C_3d_2 = Me_2d_2$
		$m = Pr^{-1}(M)$

Рис. 1. Базовый вариант протокола стойкого шифрования по разделяемому ключу малого размера в группе точек ЭК

С учетом указанного недостатка предложенный протокол (ПМК1) исключает повторное использование общего ключа малого размера, но при его разовом использовании позволяет гарантированно защищенно передать сообщение. Чтобы устранить указанный недостаток, предлагается новый механизм аутентификации передаваемых шифротекстов, в котором симметричное шифрование заменено на операции в группе точек ЭК и протокол на его основе (ПМК2).

Протокол защищенной передачи информации с разделяемым ключом малого размера, отличающийся новым механизмом аутентификации (ПМК2)

В основе данной вариации лежит идея использования разделяемого ключа шифрования K таким образом, чтобы у злоумышленника не было критерия для отбраковки неверных значений ключа при атаке полного перебора по ключевому пространству ключа K, для чего необходимо, чтобы само шифрование на малом ключе K оперировало только множеством точек ЭК, т. е. и при шифровании, и при расшифровании результат являлся точкой ЭК. Реализация данного подхода для алгоритмов симметричного шифрования неочевидна, предлагается использовать разделяемый ключ шифрования K для формирования секретной последовательности R («гаммы»), накладываемой на передаваемые шифротексты таким образом, чтобы все передаваемые на шагах протокола шифротексты также являлись точками ЭК. Результат сложения двух точек ЭК является также точкой ЭК, соответственно, необходимо, чтобы R также являлось точкой ЭК, получаемой, например, путем домножения специфицируемой точки G на значение малого разделяемого ключа K. При таком подходе следует учитывать, что при получении злоумышленником значения «гаммы» $R = GK$ для восстановления значения K он вместо решения вычислительно сложной задачи дискретного логарифмирования на ЭК может осуществить атаку полного перебора по ключевому пространству, соответственно, злоумышленник не должен получить значение R.

Пусть дана ЭК E над полем $GF(p)$, порядок которой $\#E = \Omega$ делится на большой простой делитель q (разрядностью не менее 160 бит) или равен большому простому числу. Ключи АКШ генерируется обеими сторонами в виде двух взаимно обратных по модулю Ω чисел e и $d = e^{-1} \bmod \Omega$. Точка G есть случайно выбранная специфицируемая точка большого порядка. Ключ K есть разделяемый отправителем и получателем ключ малого размера для создания добавляемой к передаваемым на шагах протокола шифротекстам последовательности (точки) R путем умножения на специфицированную точку G : $R = GK$. Передача сообщения m выполняется по следующему алгоритму.

1. Отправитель:

• кодирует передаваемое сообщение m точкой ЭК, например, методом вероятностного кодирования: $M = \mathrm{Pr}(m)$;

• зашифровывает полученную точку M на своём ключе e_1 АКШ по формуле $C_1 = Me_1$;

• умножает специфицированную точку G на значение общего малого ключа K по формуле $R = GK$;

• вычисляет шифротекст C_1', добавляя полученную точку R к точке C_1 по формуле $C_1' = C_1 + R = Me_1 + GK$;

• пересылает полученное значение C_1' получателю.

2. Получатель:

• умножает специфицированную точку G на значение общего малого ключа K по формуле $R = GK$ и вычитает полученную точку R из принятой точки C_1' по формуле $C_1 = C_1' - R = Me_1$;

• умножает полученное значение C_1 на свой ключ e_2 АКШ: $C_2 = C_1e_2 = Me_1e_2$;

• вычисляет пересылаемый шифротекст C_2', добавляя точку R к точке C_2, полученной на предыдущем шаге по формуле $C_2' = C_2 + R = Me_1e_2 + GK$;

• пересылает полученное значение C_2' отправителю.

3. Отправитель:

• вычитает точку R из принятой точки C_2' по формуле $C_2 = C_2' - R = Me_1e_2$;

• умножает полученное значение на свой ключ расшифрования d_1 АКШ: $C_3 = C_2d_1 = Me_1e_2d_1 = Me_2$;

• вычисляет пересылаемый шифротекст C_3', прибавляя полученную на первом шаге протокола точку R по формуле $C_3' = C_3 + R = Me_2 + GK$;

• пересылает полученное значение C_3' получателю.

4. Получатель:

• вычитает точку R из принятой точки C_3' по формуле $C_3 = C_3' - R = Me_2$;

• получает значение точки M умножением на свой ключ расшифрования d_2 АКШ: $M = C_3d_2 = Me_2d_2$;

• восстанавливает исходное сообщение m из полученной точки M декодированием по алгоритму вероятностного кодирования: $m = Pr^{-1}(M)$.

Полученная схема протокола приведена на рис. 2.

В протоколе промежуточные шифротексты процедур бесключевого шифрования, являющиеся точками ЭК, шифруются (суммируются с точкой, полученной на основе короткого ключа K) так, что они отображаются в другие точки ЭК, поэтому перебор ничего не даёт атакующему, так как все пробные варианты значения короткого ключа дают точки ЭК.

Обсуждение

Следует отметить, что в случае как схемы бесключевого шифрования, так и предложенных протоколов необходимо сохранять личные ключи участников протокола (ключей e_1, e_2) в тайне от злоумышленника/уничтожать ключи по завершении сеанса связи. В схеме бесключевого шифрования знание любого ключа напрямую приводит к восстановлению передаваемого сообщения M из перехваченных шифротекстов. В предложенных протоколах схема бесключевого шифрования дополнена механизмом аутентификации по ключу K малого размера, в результате знание одного из ключей e_1, e_2 позволит на основе перехваченных шифротекстов C_1`, $C_2$`, C_3` восстановить малый ключ K перебором по его ключевому пространству и далее – передаваемого сообщения M.

Для построения протокола представляет интерес использование ЭК, порядок которых является простым числом («идеальных» ЭК) или равен простому числу, умноженному на достаточно малое натуральное число [10]. В этом случае можно пренебречь вероятностью получения «слабых» сообщений – шифруемых точек малого порядка, что

Отправитель		**Получатель**
$M = Pr(m)$		
$C_1 = Me_1$		
$R = GK$		
$C_1' = C_1 + R = Me_1 + GK$		
	$\xrightarrow{C_1' = Me_1 + GK}$	
		$R = GK$
		$C_1 = C_1' - R$
		$C_2 = C_1 e_2 = Me_1 e_2$
		$C_2' = C_2 + R = Me_1 e_2 + GK$
	$\xleftarrow{C_2' = Me_1 e_2 + GK}$	
$C_2 = C_2' - R$		
$C_3 = C_2 d_1 = Me_1 e_2 d_1 = Me_2$		
$C_3' = Me_2 + GK$		
	$\xrightarrow{C_3' = Me_2 + GK}$	
		$C_3 = C_3' - GK = Me_2$
		$M = C_3 d_2 = Me_2 d_2$
		$m = Pr^{-1}(M)$

Рис. 2. Протокол стойкого шифрования по разделяемому ключу малого размера в группе точек ЭК, отличающийся новым механизмом аутентификации

потенциально могло бы позволить нарушителю вычислить часть секретного ключа. В случае использования для представления сообщения точкой ЭК способа вероятностного кодирования можно устранить возможность шифрования точек, которые имеют сравнительно малое значение порядка, однако это требует специальных процедур для определения порядка точек, кодирующих сообщение. Применение данных процедур приведет к существенному снижению производительности процедуры шифрования, поэтому предпочтительно использовать идеальные ЭК.

Для повышения производительности АКШ с использованием ЭК, заданных над полем $GF(p)$, можно использовать простые числа вида $p = 2^k \pm \mu_g 2^g \pm \mu_h 2^h \pm 1$, где $0 < h < g < k$; $\mu_g \in \{0,1\}$; $\mu_h \in \{0,1\}$. Использование простых чисел данного вида позволяет выполнить операцию умножения в поле $GF(p)$ без операции арифметического деления, наиболее трудоемкой при умножении по модулю p, что позволяет существенно повысить скорость шифрования по сравнению со случаем использования простых чисел произвольного вида. Причем выбор простого модуля указанного вида позволяет уменьшить сложность вычислений без того, чтобы это влияло на появление «слабых» сообщений.

Для повышения безопасности ПМК с учетом появления прорывного решения для вычислительно сложной задачи, лежащей в основе АКШ, представляет интерес рассмотрение подхода к синтезу ПМК на основе двух вычислительно сложных задач. Существующие ПМК основываются на вычислительной сложности одной задачи – дискретного логарифмирования по простому модулю [1, 2]. Однако если будет найден прорывной алгоритм решения указанной задачи, использующие ее алгоритмы не смогут обеспечивать требуемый уровень стойкости. Для решения данной проблемы во многих работах предлагались протоколы других типов, взлом которых требует одновременного решения двух независимых вычислительно сложных задач. Вопрос синтеза бесключевого шифрования (АКШ) на основе двух задач решен в работе [17], а построения ПМК – в работе [18].

Для сокращения размера передаваемых шифротекстов точку ЭК можно отправить в виде ее абсциссы с присоединенным значением бита, определяющего бóльшую или меньшую ординату, – для возможности однозначной идентификации точки ЭК. Это незначительно увеличивает время расшифрования криптограммы, поскольку для восстановления ординаты точки ЭК потребуется выполнить операцию извлечения квадратного корня в поле, над которым задана ЭК. В случае использования предложенной схемы ПМК1 использование сокращенного представления точки необходимо, так как в ином случае соответствие ординаты абсциссе точки может быть использовано злоумышленником как еще один критерий для отбраковки неверного значения малого ключа K при атаке полного перебора по ключевому пространству.

Практическое использование предложенных ПМК в общем случае относится к сценариям передачи секретного сообщения в условиях ограниченности ключевого материала, причем вмешательство активного атакующего, выдающего себя за легального участника протокола, нарушает процесс расшифрования, так как обеспечивается неразрывность процедуры шифрования и аутентификации сообщений за счет применения разделяемого ключа малого размера. Для получения последнего может быть использована существующая инфраструктура двухуровневой аутентификации на базе токенов, рассылаемых посредством SMS одноразовых кодов,

что упростит внедрение в существующие автоматизированные информационно-телекоммуникационные системы и программные комплексы. В качестве примера можно привести обладающую инфраструктурой SMS-оповещения систему автоматизированного мониторинга искусственных сооружений высокоскоростной железнодорожной магистрали, среди направлений развития которой указаны шифрование данных перед передачей между локальным и удаленным серверами и устройствами пользователя, а также проверка подлинности при получении [19].

С точки зрения обеспечения аутентификации сообщений с предложенными протоколами противодействия атаки «человек посередине» схож протокол [20]. Он предложен для применения в IP-телефонии (в Бразилии) и так же построен на основе протокола бесключевого шифрования, реализованного в группе точек ЭК. В нем решение проблемы атаки «человек посередине» основано на подходе так называемой Pairing-Based Cryptography [21]. В результате, с одной стороны, не требуется использовать разделяемый ключ малого размера, но с другой стороны, требуется обмен публичными ключами участников протокола и использование спаривания Вейля (Тейта) [22]. Последнее неявно подразумевает использование суперсингулярных ЭК, для которых, соответственно, можно применять алгоритмы решения ЗДЛ субэкспоненциальной сложности. Отметим, что в работе не освещаются вопросы аутентификации передаваемых в протоколе публичных ключей участников протокола и кодирования сообщения точкой ЭК.

Заключение

По сравнению с изначальной реализацией протокола стойкого шифрования по ключу малого размера в простом поле – при переходе к группе точек ЭК – обеспечивается повышение быстродействия при одновременном повышении стойкости, а также экспоненциальная стойкость. Построение протокола с использованием вычислений на ЭК обеспечивается механизмом вероятностного кодирования шифруемых сообщений точками ЭК или способом «расщепления» сообщения. При выборе для построения «идеальных» ЭК обеспечивается отсутствие «слабых» сообщений, поскольку все точки, которые кодируют исходные сообщения, имеют одно и то же значение простого порядка, равное числу точек на ЭК. В предложенных протоколах обеспечивается неразрывность процедуры бесключевого шифрования и аутентификации. Благодаря этому вмешательство активного атакующего, выдающего себя за легального участника протокола, нарушает процесс расшифрования. В качестве аутентификации предложен новый механизм, основанный на использовании операции умножения специфицированной точки ЭК большого порядка на значение разделяемого короткого ключа.

Литература

1. Березин А. Н. Протокол стойкого шифрования с использованием коротких ключей / А. Н. Березин, А. В. Муравьев, Д. Н. Молдовян // Приборостроение. – 2014. – № 11. – С. 68-72.

2. Молдовян Н. А. Протоколы шифрования с использованием разделяемых ключей малого размера и одноразовых открытых ключей / Н. А. Молдовян, А. В. Муравьев, А. А. Костина // Вопросы защиты информации. – 2015. – № 2. – С. 8-12.

3. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code (Second Edition) / B. Schneier. – NY: John Wiley & Sons, 1996. –758 p.

4. Hellman M. E. Exponentiation Cryptographic Apparatus and Method / M. E. Hellman, S. C. Pohling // U. S. Patent № 4,424,414. 1984. 3 Jan.

5. Молдовян Н. А. Введение в криптосистемы с открытым ключом / Н. А. Молдовян. – СПб.: БХВ – Петербург, 2007. – 286 с.

6. Болотов А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2011. – 274 с.

7. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: ТВП, 2001. – 270 с.

8. Massey J. L. An introduction to contemporary cryptology / J. L. Massey // Proc. IEEE. – 1988. – Vol. 76, no. 5. – P. 533-549.

9. Massey J. L. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission / J. L. Massey, J. K. Omura // US Patent № 4567600. 1986.

10. Демьянчук А. А. Выбор «идеальных» параметров в схеме двухшаговой аутентификации и коммутативном шифре / А. А. Демьянчук, Н. А. Молдовян, А. В. Рыжков // Изв. СПбГЭТУ «ЛЭТИ». – 2013. – № 8. – С. 15-18.

11. Березин А. Н., Молдовян Д. Н., Молдовян А. А., Рыжков А. В. Способ шифрования сообщения, представленного в виде битовой строки // Пат. РФ по заявке № 2013126860 / 08 от 11.06.2013. Бюл. № 35. 20.12.2014.

12. Молдовян Н. А. Способ коммутативного шифрования на основе вероятностного кодирования / Н. А. Молдовян, А. В. Рыжков // Вопр. защиты информации. – 2013. – № 3. – С. 3-10.

13. Рыжков А. В. Шифрование на основе кодирования сообщений точками эллиптической кривой, заданной над двоичным полем / А. В. Рыжков // 69-я науч.-техн. конф. профессорско-преподавательского состава СПбГЭТУ: сб. докладов (СПб., 26 янв. – 4 фев. 2016). – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2016. – С. 153–157.

14. Bellovin S. M. Encrypted key exchange: Password-based protocols secure against dictionary attacks / S. M. Bellovin, M. Merritt // Res. Secur. Privacy, IEEE Comput. Soc. Symp. – 1992. – P. 72-84.

15. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015.

16. Рыжков А. В. Шифрование на эллиптической кривой по разделяемому ключу малого размера / А. В. Рыжков // IX Санкт-Петербургская межрегионал. Конф. «Информационная безопасность регионов России – 2015»: материалы конф. – СПб.: СПОИСУ, 2015. – С. 121-122.

17. Молдовян Н. А. Коммутативные шифры на основе трудности одновременного решения задач факторизации и дискретного логарифмирования / Н. А. Молдовян, А. Н. Березин, А. В. Рыжков // Информационно-управляющие системы. – 2014. – № 4. – С. 106-110.

18. Березин А. Н. Протокол стойкого шифрования по ключу малого размера, взлом которого требует решения задач факторизации и дискретного логарифмирования / А. Н. Березин // Вопросы защиты информации. – 2016. – № 2. – С. 3-8.

19. Бубнов В. П. Программный комплекс автоматизированного геодезического мониторинга искусственных сооруженийдля высокоскоростной железнодорожной магистрали «Москва – Казань – Екатеринбург» / В. П. Бубнов, А. А. Никитчин, С. А. Сергеев // Интеллектуальные технологии на транспорте. – 2015. – № 4 – С. 27-33.

20. Deusajute A. The SIP security enhanced by using pairing-assisted massey-omura signcryption / A. Deusajute, P. Barreto // IACR Cryptology ePrint Archive. – 2008. – P. 72-84.

21. Oliveira L. B. Tiny PBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks / L. B. Oliveira, M. Scott, J. López, R. Dahab // Comput. Commun. – 2011. – Vol. 34, no. 3. – P. 485-493.

22. Boneh D. Identity-based encryption from the weil pairing / D. Boneh, M. Franklin // Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Comput. Sci. – Springer-Verlag, 2001. – P. 213-229.

Protocol for Secure Encryption with Using Small-size Key Based on Elliptic Curve

Ryzhkov A. V.
St.-Petersburg State Electrotechnical University «LETI»
St.-Petersburg, Russia
Ryzhkov.alex@gmail.com

Abstract. **For guaranteed protection of the data, which is transmitted over open channels, in condition of limited keying material recently the protocol was proposed based on combining the keyless procedures (commutative encryption) and the private small-size key (56 bits) encryption. In order to improve the commutative encryption performance is of interest to implement the protocol based on elliptic curve (EC). In the article, regarding to the use of EC, two variations for the base protocol was proposed. In the first one the authentication mechanism is transferred from the original protocol unchanged, which imposes a restriction on reuse small secret key. In the second case the new authentication mechanism was proposed to remove this restriction.**

Keywords: **secure encryption protocol, small-size key, commutative encryption, discrete logarithm problem, elliptic curve.**

References

1. Berezin A. N., Muravyov A. V., Moldovyan D. N. Protocol for secure encryption with using small-size key [Protokol stoikogo shifrovaniia s ispol'zovaniem korotkikh kliuchei], *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [*J. Instrument Eng.*], 2014, no. 11, pp. 68-72.

2. Moldovyan N. A. Muravyov A. V., Kostina A. A. Protocols for secure encryption with using small-size keys and one-time public keys [Protokoly shifrovaniia s ispol'zovaniem razdeliaemykh kliuchei malogo razmera i odnorazovykh otkrytykh kliuchei], *Voprosy zashchity informatsii* [*Information security questions*], 2015, no. 2, pp. 8-12.

3. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code (Second Edition), NY: John Wiley & Sons, 1996, 758 p.

4. Hellman M. E., Pohling S. C. Exponentiation Cryptographic Apparatus and Method, U. S. Patent no. 4,424,414, 3 Jan. 1984.

5. Moldovyan N. A. *Vvedenie v kriptosistemy s otkrytym kliuchom* [Introduction to public key cryptosystems], St. Petersburg, BKhV – Peterburg, 2007, 286 p.

6. Bolotov A. A., Gashkov S. B., Frolov A. B. *Elementarnoe vvedenie v ellipticheskuiu kriptografiiu. Protokoly kriptografii na ellipticheskikh krivykh* [An elementary introduction to elliptic curve cryptography. Cryptographic Protocols on elliptic curves], Moscow, KomKniga, 2011, 274 p.

7. Koblitz N. *Kurs teorii chisel i kriptografii* [The course in number theory and cryptography], Moscow, TVP, 2001. 270 p.

8. Massey J. L. An introduction to contemporary cryptology Proceedings of the IEEE, 1988, Vol. 76, no. 5, pp. 533-549.

9. Massey J. L., Omura J. K. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission, US Patent no. 4567600.1986.

10. Demyanchuk A. A., Moldovyan N. A., Ryzhkov A. V. Choosing ideal parameters for zero-knowledge authentication protocols and commutative ciphers [Vybor „ideal'nykh" parametrov v skheme dvukhshagovoi autentifikatsii i kommutativnom shifre], *Izvestiya SPbGETU "LETI"* [*J. St. Petersburg Electrotechnical Univ. "LETI"*], 2013, no. 8, pp. 15-18.

11. Berezin A. N., Moldovyan D. N., Moldovyan A. A., Ryzhkov A. V. Sposob shifrovaniia soobshcheniia, predstavlennogo v vide bitovoi stroki [A method of encrypting a message, represented as a bit string], Russian Federation Patent no. 2013126860/08, 11.06.2013.

12. Moldovyan N. A., Ryzhkov A. V. A method for commutative encryption based on probabilistic encryption [Sposob kommutativnogo shifrovaniia na osnove veroiatnostnogo kodirovaniia], *Voprosy zashchity informatsii* [*Information security questions*], 2013, no. 3, pp. 3-10.

13. Ryzhkov A. V. Encryptionbased on message encoding to points of an elliptic curve defined over the binary field [Shifrovanie na osnove kodirovaniia soobshchenii tochkami ellipticheskoi krivoi, zadannoi nad dvoichnym polem], *Trudy "69-ia Nauchno-tekhnicheskaia konferentsiia professorsko-prepodavatel'skogo sostava SPbGETU"*, St. Petersburg, 26 jan. – 4 feb. 2016, St. Petersburg, Pub. SPbGETU "LETI", 2016, pp. 153-157.

14. Bellovin S. M., Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks, Res. Secur. Privacy, IEEE Comput. Soc. Symp., 1992, pp. 72-84.

15. GOST R 34.12-2015 *Informatsionnaia tekhnologiia. Kriptograficheskaia zashchita informatsii. Blochnye shifry* [Information technology. Cryptographic protection of information. Block ciphers], Moscow, Standartinform, 2015.

16. Ryzhkov A. V. Encryption on an elliptic curve with using shared small-size key [Shifrovanie na ellipticheskoi krivoi po razdeliaemomu kliuchu malogo razmera], *Trudy "IX Sankt-Peterburgskaia mezhregional'naia konferentsiia 'Informatsionnaia bezopasnost' regionov Rossii – 2015'"*, St. Petersburg, SPOISU, 2015, pp. 121-122.

17. Moldovyan N. A., Berezin A. N., Ryzhkov A. V. Commutative ciphers based on difficulty of simultaneous solving factorization and discrete logarithm problems [Kommutativnye shifry na osnove trudnosti odnovremennogo resheniia zadach faktorizatsii i diskretnogo logarifmirovaniia], *Informatsionno-*

upravliaiushchie sistemy [*Information and Control Systems*], 2014, no. 4, pp. 106-110.

18. Berezin A. N. Protocol for secure encryption with using small-size key based on difficultyof simultaneous solving factorization and discrete logarithm problems [Protokol stoikogo shifrovaniia po kliuchu malogo razmera, vzlom kotorogo trebuet resheniia zadach faktorizatsii i diskretnogo logarifmirovaniia], *Voprosy zashchity informatsii* [*Information security questions*], 2016, no. 2, pp. 3-8.

19. Bubnov V. P., Nikitchin A. A., Sergeev S. A. Software for Automated Geodetic Monitoring of Artifi cial Structures for High-speed Railway "Moscow – Kazan – Yekaterinburg" [Programmnyi kompleks avtomatizirovannogo geodezicheskogo monitoringa iskusstvennykh sooruzhenii dlia vysokoskorostnoi zheleznodorozhnoi magistrali "Moskva – Kazan' – Ekaterinburg"], *Intellektual'nye tekhnologii na transporte* [*Intellectual Technol. Transp*], 2015, no. 4, pp. 27-33.

20. Deusajute A., Barreto P. The SIP security enhanced by using pairing-assisted massey-omura signcryption, *IACR Cryptology ePrint Archive*, 2008, pp. 72-84.

21. Oliveira L. B., Scott M., López J., Dahab R. Tiny PBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks, *Comput. Commun.*, 2011, Vol. 34, no. 3, pp. 485-493.

22. Boneh D., Franklin M. Identity-based encryption from the weilpairingin, *Advances in Cryptology – CRYPTO 2001, ser. Lecture Notesin Comput. Sci.*, Springer-Verlag, 2001, pp. 213-229.

Информационная безопасность в Европейских системах управления движением на железнодорожном транспорте

Мыльников П. Д., Попов П. А.
ОАО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»)
г. Санкт-Петербург, Россия
p.mylnikov@vniias.ru, p.popov@vniias.ru

Аннотация. **Описана история возникновения Европейской системы управления перевозочным процессом ERTMS, изучены механизмы обеспечения информационной безопасности в ERTMS, в том числе одна из основных задач криптографии – распределение ключей. Рассмотрены актуальные проблемы распределения ключей для тягового подвижного состава на примере железных дорог Германии. Определены направления для дальнейшего развития систем распределения ключей на железнодорожном транспорте.**

Ключевые слова: **транспорт, криптография, ключ, распределение ключей, протоколы аутентификации.**

Введение

В середине 1990-х годов консорциум ведущих европейских железнодорожных компаний пришел к мнению о необходимости создания единого набора стандартов (спецификаций) для универсализации работы систем управления и обеспечения безопасности движения поездов.

Последнее десятилетие продемонстрировало активный технологический рост в телекоммуникационной сфере железнодорожного транспорта. Для актуализации спецификаций компании – участницы консорциума проводят теоретические и практические исследования по реализации инноваций на железнодорожном транспорте, что позволяет им ежегодно обновлять спецификации.

Немаловажную роль в спецификациях занимает раздел информационной безопасности. С каждым годом растет количество исследований по кибербезопасности информационных и управляющих систем [1–3], что подталкивает к определению новых направлений исследований в области информационной безопасности для железнодорожных систем.

История создания ERTMS

Европейская система управления перевозочным процессом ERTMS (European Railway Traffic Management System) была создана для замены несовместимых между собой систем управления и обеспечения безопасности движения поездов, которые применялись на железных дорогах Западной Европы [4–7].

Проект ERTMS был инициирован в 1995 г. Европейской комиссией. Для разработки спецификаций и проведения испытаний в августе 1995 г. образована группа пользователей ERTMS, куда вошли железные дороги Германии (Deutsche Bahn AG), Италии (Ferroviedello Stato) и Франции (SNCF). Группа приступила к работе в декабре 1995 г. в Брюсселе. В ноябре 1997 г. к ней присоединились железные дороги Нидерландов (NS) и Испании (RENFE), а в 1998 г. – Великобритании (Railtrack).

Основными компонентами ERTMS являются Европейская система управления движением поездов ETCS (European Train Control System) и система цифровой связи GSM-R, обеспечивающая беспроводную передачу данных между поездами и центрами управления. Так как сеть связи GSM-R относится к открытым сетям связи, то в соответствии с требованиями стандарта EN 50129-2 [8] в приложениях, связанных с обеспечением безопасности движения с использованием открытых сетей связи, должны использоваться специальные средства для защиты системы от угроз внедрения, модификации и подмены сообщений.

Принципы защиты информации в ERTMS

Для реализации защиты от этих угроз в спецификациях ERTMS разработан стек протоколов межсетевого взаимодействия, включающий безопасный протокол взаимодействия Euroradio [9, 10] (рис. 1).

Протокол Euroradio используется для защиты передаваемых данных с использованием методов аутентификации и контроля целостности данных. В основе данного протокола лежат криптографические механизмы на основе симметричного блочного шифра TripleDES.

На первом этапе (после установления соединения на сетевом и транспортном уровне) по протоколу Euroradio выполняется аутентификация подключаемых абонентов. Для этого два взаимодействующих узла формируют случайные числа (R_A, R_B) и обмениваются ими в сообщениях AU1 и AU2 (рис. 2). На основе этих случайных чисел и сохраненного в памяти узлов симметричного ключа KMAC вырабатывается симметричный сессионный ключ

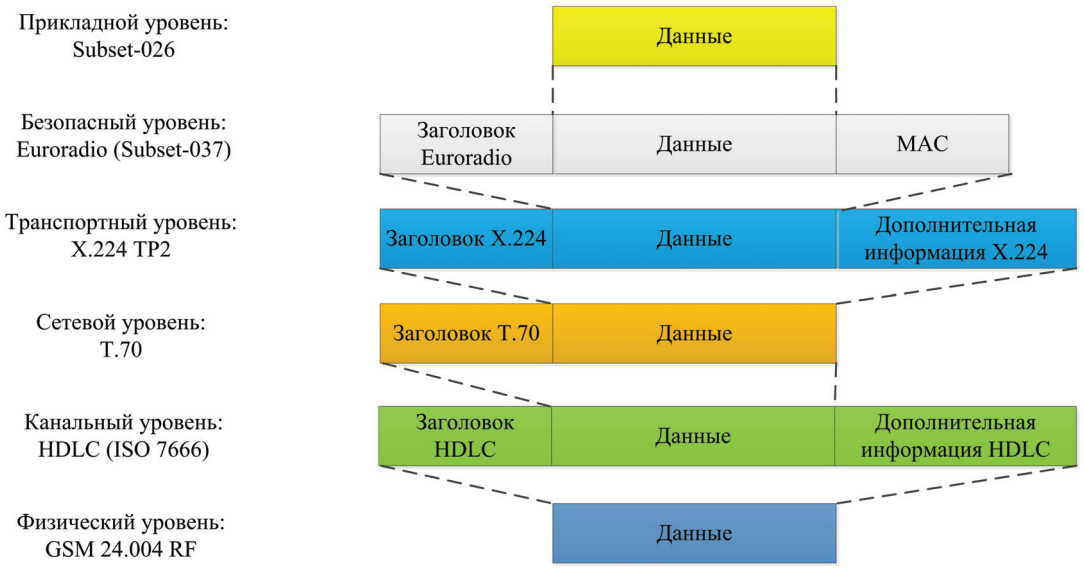


Рис. 1. Модель OSI при взаимодействии бортовых и стационарных устройств ERTMS в сети связи GSM-R

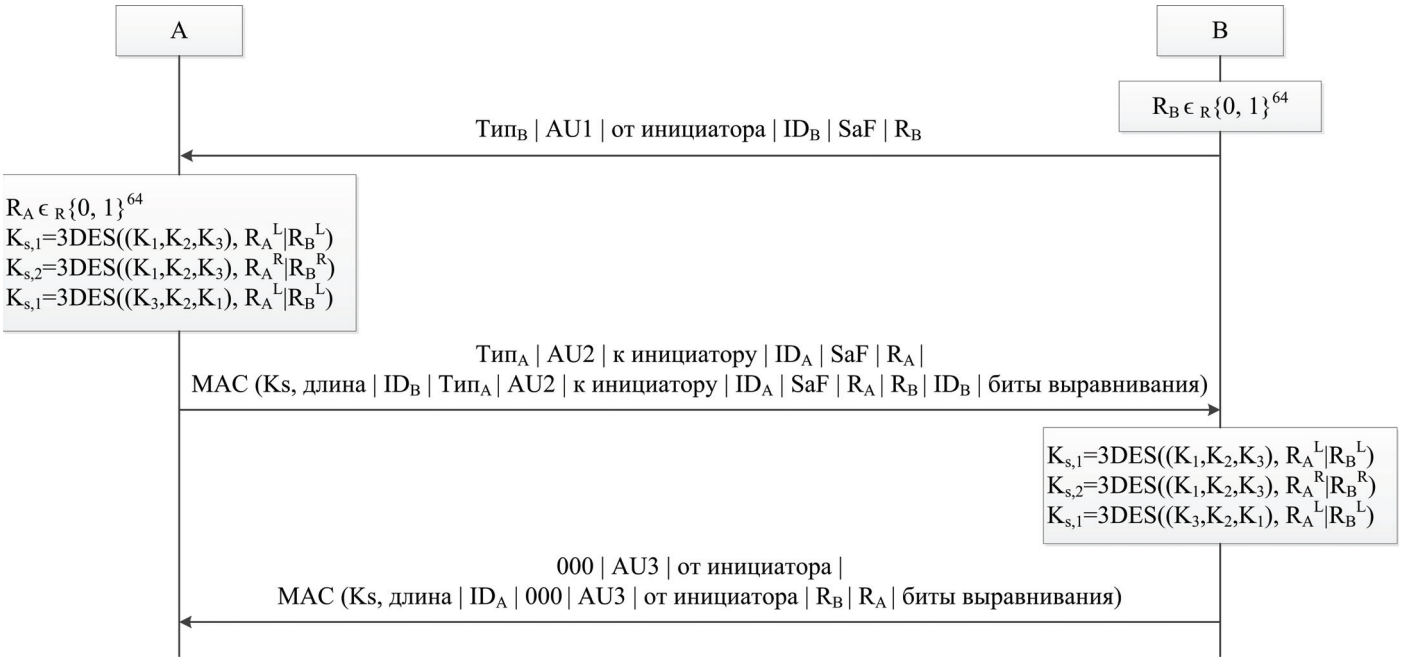


Рис. 2. Процедура аутентификации по протоколу Euroradio

KSMAC. KSMAC используется для вычисления аутентификационного кода сообщения (MAC) сообщения AU3. В результате проверки MAC сообщения AU3 второй узел может удостовериться в успешной генерации сессионного ключа и корректного завершения процедуры аутентификации.

На втором этапе работы протокола Euroradio выполняется вычисление аутентификационного кода всех передаваемых и принимаемых прикладных сообщений, что обеспечивает защиту от представленных ранее угроз. Стоит отметить, что сами данные, передаваемые между абонентами, не шифруются и передаются в открытом виде. Однако для работы протокола Euroradio необходимы предопределённые симметричные ключи шифрования, что, в свою очередь, ведет к рассмотрению другой фундаментальной задачи криптографии – распределению ключей.

Система распределения ключей ERTMS

Основным звеном в системе управления ключами ERTMS является Центр управления ключами (ЦУК) [11, 12] (рис. 3). ЦУК отвечает за создание ключей для объектов железнодорожного транспорта, включая центры радиоблокировки и тяговый подвижной состав, выполняющий подключения к ним. Сгенерированные ключи используются для создания безопасного соединения между поездом и центром радиоблокировки. ЦУК также отвечает за распределение, обновление и удаление уже установленных ключей, так как для каждого выданного ключа устанавливается определенный срок действия, по истечении которого производится одна из описанных процедур.

Система управления ключами ERTMS включает в себя иерархию ключей, представленную в таблице.

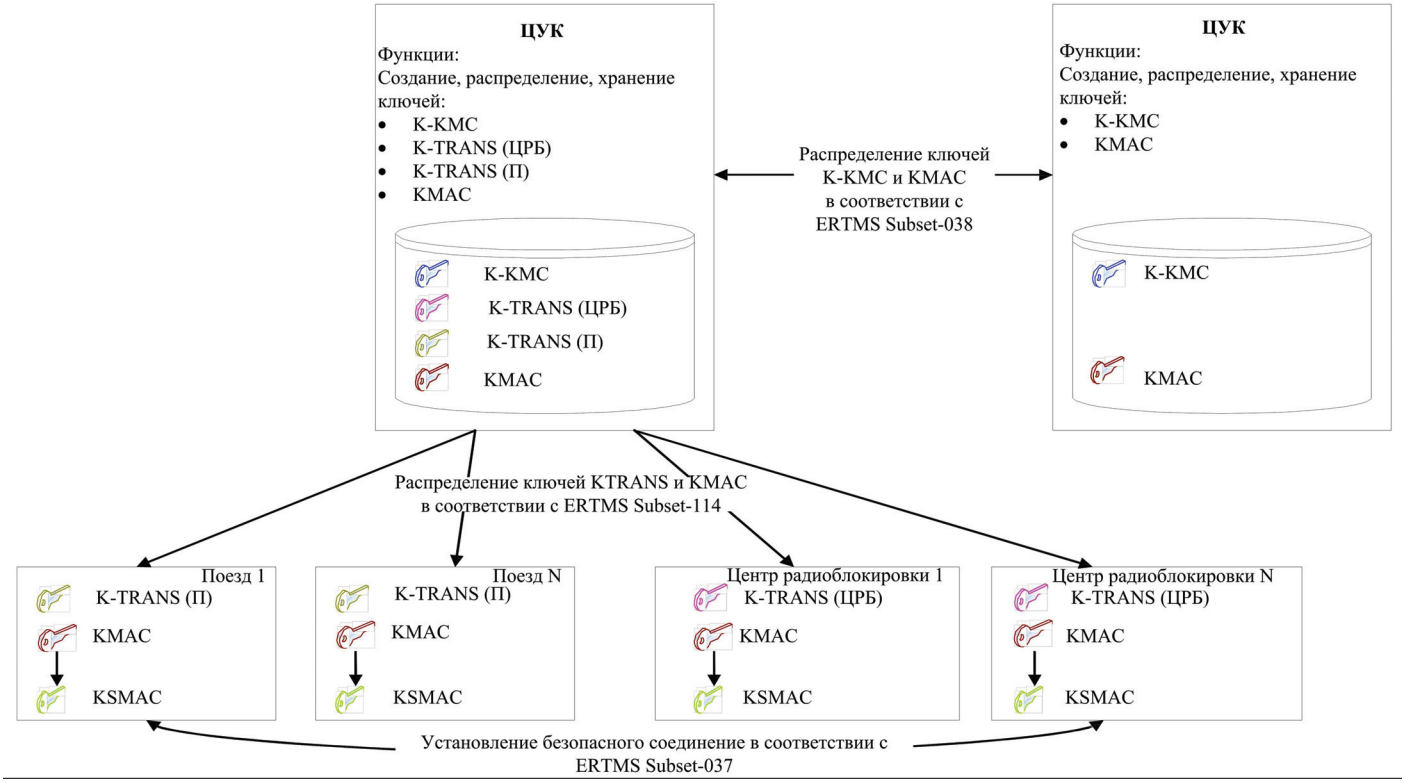


Рис. 3. Архитектура системы управления ключами ERTMS

Иерархия ключей ERTMS

Уровень иерархии	Наименование ключа	Назначение ключа
3	K-KMC	Транспортный ключ используется для обеспечения безопасного обмена между центрами управления ключами (ЦУК) ERTMS
	KTRANS	Транспортный ключ используется для обеспечения безопасного обмена между ЦУК и стационарным или бортовым оборудованием для создания, обновления или удаления аутентификационных ключей
2	KMAC	Аутентификационный ключ используется для создания сессионного ключа и установления безопасного соединения между двумя объектами ERTMS
1	KSMAC	Сессионный ключ используется для защищенного информационного обмена в течение одной сессии между двумя объектами ERTMS

Ключи третьего уровня иерархии должны быть заранее распределены для всех объектов информационного обмена. Ключи третьего уровня рассмотрим на примере ключа K-KMC [13]. Ключ K-KMC состоит из двух частей:

• K-KMC1 (192 бита) используется для аутентификации ЦУК и объектов ERTMS и для подтверждения целостности передаваемых ЦУК сообщений (например, команд управления ключами). Для защиты передаваемых сообщений применяется процедура расчета аутентификационного кода сообщений (MAC), результат выполнения операции используется для проверки целостности сообщений и подлинности источника сообщений;

• K-KMC2 (192 бита) используется для шифрования ключей второго уровня – ключей аутентификации (KMAC), которые распределяются между всеми сущностями ERTMS. K-KMC2 делится на три подключа K3, K2, K1, каждый длиной 64 бита. При выполнении процедуры шифрования/дешифрования ключа KMAC ключ делится на три блока, к каждому из которых применятся алгоритм шифрования Triple DES по схеме, представленной на рис. 4.

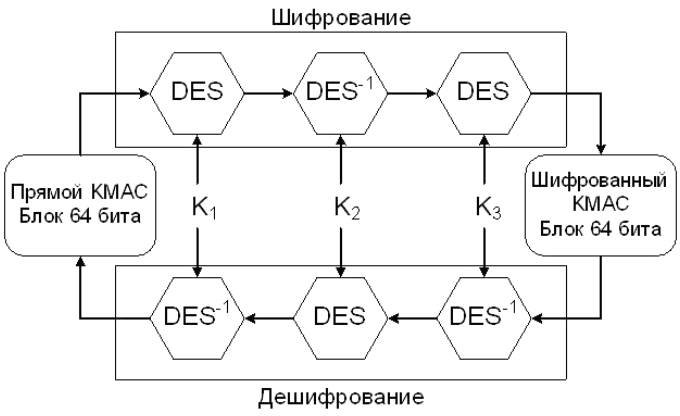


Рис. 4. Схема шифрования/дешифрования ключей аутентификации

В системе управления ключами ERTMS предусмотрено выполнение следующих функций:

1) настройка ЦУК. Администратор системы должен обеспечивать выполнение всех процедур, связанных с настройкой бортового и стационарного оборудования, т. е.:

- генерацию ключей;
- отправку ключей другим ЦУК;
- получение ключей от других ЦУК;
- удаление ключей;
- архивирование ключей;
- проверку ключей;
- создание логов;

2) распределение ключей K-KMC. Администратор должен распределять ключи K-KMC для каждого ЦУК, с которым необходима процедура обмена ключами. Основным способом распределения ключей K-KMC является использование доверенных каналов связи;

3) распределение ключей K-TRANS. Администратор должен распределять K-TRANS для каждого объекта ERTMS, входящего в зону ответственности данного ЦУК. Основным способом распределения ключей K-TRANS является использование доверенных каналов связи;

4) генерация ключей KMAC. Генерацию ключа выполняет ЦУК в соответствии с требованиями секретности. Генерируемые ключи подлежат проверке на «слабость». Каждому сгенерированному ключу KMAC дается уникальный порядковый номер;

5) обмен KMAC с другими ЦУК:

- передача ключа: передающий администратор должен обозначить бортовое оборудование, которому предназначается ключ, и список центров радиоблокировки, которые будут с ним взаимодействовать;
- получение ключа: администратор, получающий ключ, должен подтвердить факт приема ключа и предпринять необходимые действия для его использования.

При передаче ключ должен быть зашифрован с помощью ключа K-KMC;

6) обновление KMAC. Администратор ЦУК принимает решение о необходимости обновления ключа. Эта процедура может выполняться как по заранее подготовленному плану, так и при угрозе конфиденциальности распределенных ключей;

7) удаление KMAC. Администратор должен иметь возможность послать запрос другим администраторам для удаления ключей. В случае запроса об удалении ключа администратор ЦУК должен убедиться в удалении всех копий ключа;

8) архивация ключей и транзакций, связанных с управлением ключами. В задачи администратора входит хранение всей информации о сгенерированных ключах, в том числе:

- соответствие ключей бортовым и стационарным устройствам ERTMS;
- текущее состояние каждого ключа (используется в данный момент, удален и т. д.);

9) удаление K-KMC. Администратор ЦУК должен информировать администраторов других ЦУК об удалении ключей K-KMC. Также администратор должен убедиться в том, что все копии ключа удалены.

С использованием протоколов аутентификации, описанных в [10], ЦУК идентифицирует подключаемые объекты ERTMS и обеспечивает создание и своевременное обновление ключей второго уровня. Объекты ERTMS, используя протокол Euroradio, выполняют процедуру аутентификации, в результате которой генерируются ключи первого уровня, действительные только в течение одной сессии (около 1 часа).

Актуальные проблемы распределения ключей

Основным способом распределения ключей KTRANS для объектов железнодорожного транспорта в настоящий момент является физическое распределение ключей с помощью доверенных каналов или курьерской службы. Использование данного способа занимает много времени и несет определенные риски [14]. Так, время установки или обновления ключевой информации с помощью доверенной курьерской службы в одном бортовом устройстве может быть определено по формуле

$$T_k = T_{TO-2} + T_{\text{дост}} + T_{\text{уст}}[\text{ч}],$$

где T_{TO-2} – периодичность технического обслуживания ТПС; $T_{\text{дост}}$ – время доставки ключевой информации до депо обслуживания ТПС; $T_{\text{уст}}$ – время установки ключевой информации с помощью курьерской службы в бортовое устройство ТПС с помощью специального оборудования.

В нормативных документах железных дорог Германии регламентируется периодичность технического обслуживания ТПС каждые 9 дней [15]. Легко посчитать, что максимальное время установку или обновление ключевой информации по приведенной формуле составит ~219 часов, что критически много, когда вопрос касается информационной безопасности.

Заключение

Спецификации ERTMS входят в число передовых инструментов для проектирования безопасных и надежных систем управления и обеспечения безопасности движения поездов. Исследование механизмов обеспечения защиты данных и распределения ключей в ERTMS позволяет сформулировать важную задачу в области информационной безопасности транспортных систем, основанную на поиске новых технологических подходов и решений для повышения оперативности обеспечения ключами объектов радиосетей железнодорожного транспорта.

Литература

1. Корниенко А. А. Методика обнаружения и разрешения конфликтов программных средств защиты от кибератак на железнодорожном транспорте / А. А. Корниенко, М. А. Поляничко // Интеллектуальные технологии на транспорте. – 2015. – № 1. – С. 18-21.

2. Гапанович В. А. Некоторые положения отказобезопасности и киберзащищенности систем управления / В. А. Гапанович, Е. Н. Розенберг, И. Б. Шубинский // Надежность. – 2014. – № 2 (49). – С. 88-94.

3. Шубинский И. Б. О киберзащищенности информационных систем управления движением поездов / И. Б. Шубинский, Б. А. Макаров // Автоматика, связь, информатика. – 2014. – № 11. – С. 9-12.

4. Соловьев В. П. Интеллектуальные транспортные системы железнодорожного транспорта (основы инновационных технологий) / В. П. Соловьев, В. В. Скалозуб, И. В. Жуковицкий, К. В. Гончаров. – Днепропетровск: Изд-во Днепропетров. нац. ун-та железнодорожного транспорта им. акад. В. Лазаряна, 2013. – 211 с.

5. Корнашевски М. ETCS как способ унификации систем управления железнодорожным движением в Польше и в Европе / М. Корнашевски, М. Хшан, В. Новаковски // Вестн. Урал. гос. ун-та путей сообщения. – 2010. – № 4. – С. 46-54.

6. Тиверовский В. И. Телематика и информатизация на транспорте / В. И. Тиверовский // Транспорт: наука, техника, управление. – 2013. – № 5. – С. 61-63.

7. Abed S. European rail traffic management system – an o verview / S. Abed // Iraqi J. Electr. Electron. Eng. – 2010. – Vol. 6, no. 2. – P. 172-179.

8. BS EN 50129:2003. Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signaling.

9. ERTMS / ETCS. Subset-098. RBC-RBC Safe Communication Interface. Vol. 3.0.0.

10. ERTMS / ETCS. Subset-037. Euroradio FIS. Vol. 3.0.0.

11. Мыльников П. Д. Обеспечение информационной безопасности в спецификациях ERTMS. Управление ключами и защита данных / П. Д. Мыльников // Интеллектуальные системы на транспорте: материалы IV междунар. науч.-практич. конф. «ИнтеллектТранс-2014». – СПб.: ПГУПС, 2014. – С. 498–500.

12. ERTMS/ETCS. Subset-114. KMC-ETCS Entity Off-line KM FIS. Vol. 1.0.0.

13. ERTMS/ETCS. Subset-038. Off-line Key Management FIS. Vol. 3.0.0.

14. Коржик В. И. Основы криптографии / В. И. Коржик, В. П. Просихин, В. А. Яковлев. – СПб.: СПбГУТ, 2014. – 276 с.

15. Осяев А. Т. О системе обслуживания локомотивов за рубежом / А. Т. Осяев, В. А. Никифоров // Вестн. ВНИИЖТ. – 2012. – № 5. – С. 56-62.

Information Security in European Railway Traffic Management System

Mylnikov P., Popov P.
Center of traffic control and safety ensuring systems
Research and design institute for information technology,
signaling and telecommunications on railway transport (JSC NIIAS)
St. Petersburg, Russia
p.mylnikov@vniias.ru, p.popov@vniias.ru

Abstract. **The article describes the history of the European Railway Traffic Management System (ERTMS), studied the principles of information security in the ERTMS, including one of the main tasks of cryptography – key distribution. The actual problem of key distribution for the locomotives is announced.The directions for the further development of key distribution systems for rail transport are determined.**

Keywords: **transport, cryptography, key, key distribution, authentication protocols.**

References

1. Kornienko A.A., Poljanichko M.A. Metodika obnaruzhenija i razreshenija konfliktov programmnyh sredstv zashhity ot kiberatak na zheleznodorozhnom transporte, *Intellektual'nye tehnologii na transporte*, 2015, no. 1, pp. 18-21.

2. Gapanovich V.A., Rozenberg E.N., Shubinskij I.B. Nekotorye polozhenija otkazobezopasnosti i kiberzashhishhennosti system upravlenija, *Nadezhnost*, 2014, no. 2 (49), pp. 88-94.

3. Shubinskij I.B., Makarov B.A. O kiberzashhishhennosti informacionnyh system upravlenija dvizheniem poezdov, *Avtomatika, svjaz', informatika*, 2014, no. 11, pp. 9-12.

4. Soloviev V.P., Skalozub V.V., Zhukovickij I.V., Goncharov K.V. Intellektual'nye transportnye sistemy zhe-leznodorozhnogo transporta (osnovy innovacionnyh teh-nologij). Dnepropetrovsk, Izdatel'stvo Dnepropetrovskogo nacional'nogo universiteta zheleznodorozhnogo transporta im. Akademika V. Lazarjana, 2013, 211 p.

5. Kornashevski M., Hshan M., Novakovski V. ETCS kak spos ob unifikacii system upravlenija zheleznodorozhnym dvizheniem v Pol'she i v Evrope, *Vestnik Ural'skogo gosudarstvennogo universiteta putejsoobshhenija*, 2010, no. 4, pp. 46-54.

6. Tiverovskij V.I. Telematika i informatizacija na transporte, *Transport: nauka, tehnika, upravlenie*, 2013, no. 5, pp. 61–63.

7. Abed S. European rail traffic management system – an overview, *Iraqi J. Electr. Electron. Eng.*, 2010, vol. 6, no. 2, pp. 172-179.

8. BSEN 50129:2003. Railwayapplications. Communication, signaling and processing systems. Safety related electronic systems for signaling.

9. ERTMS/ETCS. Subset-098. RBC-RBC Safe Communication Interface. Vol. 3.0.0.

10. ERTMS/ETCS. Subset-037. Euroradio FIS. Vol. 3.0.0.

11. Mylnikov P.D. Obespechenie informacionnoj bez-opasnosti v specifikacijah ERTMS. Upravlenie kljuchami i zashhita dannyh. Intellektual'nye sistemy na transporte: materialy IV mezhdunarodnoj nauchno-prakticheskoj konferencii «IntellektTrans-2014». SPb, PGUPS, 2014, pp. 498-500.

12. ERTMS/ETCS. Subset-114. KMC-ETCS Entity Off-line KM FIS. Vol. 1.0.0.

13. ERTMS/ETCS. Subset-038. Off-line Key Management FIS. Vol. 3.0.0.

14. Korzhik V.I., Prosihin V.P., Jakovlev V.A. Osnovy Kriptografii. SPb., SPbGUT, 2014, 276 p.

15. Osjaev A.T., Nikiforov V.A. O sisteme obsluzhivanija lokomotivov zarubezhom, *Vestnik VNIIZhT*, 2012, no. 5, pp. 56-62.

Список авторов статей, опубликованных в № 3 журнала «Интеллектуальные технологии на транспорте» за 2016 год

Блажко Людмила Сергеевна
д.т.н., профессор
Должность: проректор по учебной работе ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», заведующая кафедрой «Железнодорожный путь».
Область научных интересов: строительство железных дорог, конструкции железнодорожного пути для сверхтяжелых нагрузок и высокоскоростного движения.
E-mail: dou@pgups.edu

Киселев Игорь Павлович
инженер путей сообщения, д.ист.н.
Должность: проректор по международному сотрудничеству и связям с общественностью ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I», профессор кафедры «История», профессор кафедры «Строительство дорог транспортного комплекса».
Область научных интересов: история транспорта, системы высокоскоростного сухопутного транспорта.
E-mail: kis1347@mail.ru

Плеханов Павел Андреевич
к.т.н., доцент
Должность: доцент кафедры «Электрическая связь» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: безопасность на транспорте, техническое регулирование и стандартизация, системы беспроводной связи.
E-mail: pavelplekhanov@gmail.com

Утепбергенов Ирбулат Туремуратович
профессор
Должность: ведущий научный сотрудник Института информационных и вычислительных технологий МОН РК. Профессор Алматинского университета энергетики и связи.
Область научных интересов: информационные системы и технологии.
E-mail: i.utepbergenov@gmail.com

Касымова Динара Тугелбековна
Должность: старший преподаватель Алматинского университета энергетики и связи.
Область научных интересов: информационные системы и технологии.
E-mail: dika.cat@mail.ru

Ахмедиярова Айнур Танатаровна
Должность: научный сотрудник Института информационных и вычислительных технологий МОН РК; старший преподаватель Казахской академии транспорта и коммуникации им. М. Тынышпаева.
Область научных интересов: информационные системы и технологии.
E-mail: aat.78@mail.ru

Ходаковский Валентин Аветикович
д.т.н., профессор
Должность: заведующий кафедрой «Математика и моделирование» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: математическое моделирование, теория вероятностей и математическая статистика, системный анализ сложных систем, случайные процессы, радиотехнические системы и сигналы, сжатие изображений, информации и данных, оптимальное кодирование и оценивание параметров сигналов, аналитическая обработка данных, исследование операций, методы оптимизации, экспертные системы, нейронные сети.
E-mail: hva1104@mail.ru

Дегтярев Валентин Григорьевич
д.т.н., профессор
Должность: профессор кафедры «Математика и моделирование».
ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: прикладная и небесная механика, теория вероятности и математическая статистика.
E-mail: vdegt@list.ru

Кормильцева Мария Федоровна
студент (магистратура) кафедры «Методы и приборы неразрушающего контроля» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: неразрушающий контроль, ультразвуковой контроль, фазированные антенные решетки.
E-mail: mariekor@outlook.com

Чурова Валентина Владимировна
Должность: младший научный сотрудник научно-исследовательской лаборатории программных средств неразрушающего контроля кафедры «Методы и приборы неразрушающего

контроля» ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I».
Область научных интересов: обнаружение и фильтрация сигналов в неразрушающем контроле.
E-mail: churova_mk@mail.ru

Рыжков Алексей Викторович
аспирант Санкт-Петербургского государственного электротехнического университета «ЛЭТИ»
Область научных интересов: информационная безопасность, криптография, коммутативное шифрование, программирование.
E-mail: Ryzhkov.alex@gmail.com

Мыльников Павел Дмитриевич
Должность: начальник сектора Центра систем управления и обеспечения безопасности движения Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте (ОАО «НИИАС»).
Область научных интересов: информационная безопасность, транспортные системы, цифровые системы связи.
E-mail: p.mylnikov@vniias.ru, paul.mylnikov@gmail.com

Попов Павел Александрович
к.т.н.
Должность: руководитель Центра систем управления и обеспечения безопасности движения Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте (ОАО «НИИАС»).
Область научных интересов: системы интервального регулирования, спутниковая навигация.
E-mail: p.popov@vniias.ru, pavel.niias@gmail.com

The list of authors of articles published in the journal number 3 «Intellectual Technologies on Transport» for 2016

Blazhko Luidmila Sergeevna
Dr. Sci. (Eng.), professor
Appointment: vice rector for academic affairs Petersburg State Transport University, head of the department "Railway Track".
Academic interests: railway construction, railway track structures for extra heavy loads and high-speed railway operation.
E-mail: dou@pgups.edu

Kiselev Igor Pavlovich
Transport engineer, Dr. Sci. (History)
Appointment: vice rector for international cooperation and public relations o Petersburg State Transport University, professor of the department "History", professor of the department "Construction of Routes of Transport Complex".
Academic interests: history of transport, high-speed land transport systems.
E-mail: kis1347@mail.ru

Plekhanov Pavel Andreevich
Cand. Sci. (Eng.)
Appointment: assistant professor of Telecommunication Department of Emperor Alexander I St. Petersburg State Transport University.
Academic interests: safety and security on transport, technical regulation and standardization, wireless communication systems.
E-mail: pavelplekhanov@gmail.com

Utepbergenov Irbulat Turemuratovich
Dr. Sci (Eng.), professor
Appointment: Professor of Almaty University of Power Engineering and Telecommunication. Leading Researcher, Institute of Information and Computer Technology MES RK.
Academic interests: information systems and technology.
E-mail: i.utepbergenov@gmail.com

Kassymova Dinara Tugelbekovna
Appointment: researcher, Institute of Information and Computer Technology MES RK; senior lecturer, Kazakh Academy of Transport and Communications named M. Tynyshpaeva.
Academic interests: information systems and technology.
E-mail: dika.cat@mail.ru

Ahmediyarova Ainur Tanatarovna
Appointment: researcher, Institute of Information and Computer Technology MES RK; senior lecturer, Kazakh Academy of Transport and Communications named M. Tynyshpaeva.
Academic interests: information systems and technology.
E-mail: aat.78@mail.ru

Khodakovsky Valentin Avetikovich
Dr. Sci. (Eng.), professor
Appointment: head of the department "Mathematics and Modeling" Petersburg State Transport University.
Academic interests: mathematical modeling, probability theory and mathematical statistics, system analysis of complex systems, stochastic processes, radio systems and signals, image compression, and data, the optimal coding and estimation of signal parameters, analytical data processing, operations research, optimization techniques, expert systems, neural networks.
E-mail: hva1104@mail.ru

Degtyarev Valentin Grigor'evich
Dr. Sci. (Eng.), professor
Appointment: professor of "Mathematics and Modeling", Petersburg State Transport University.
Academic interests: applied and celestial mechanics, probability theory and mathematical statistics.
E-mail: vdegt@list.ru

Kormil'tseva Maria Fedorovna
student (Master) Department of "Methods and tools for non-destructive testing"
Petersburg State Transport University.
Academic interests: non-destructive testing, ultrasonic testing, phased array antennas.
E-mail: mariekor@outlook.com

Churova Valentina Vladimirovna
Appointment: junior researcher research Laboratory of non-destructive testing software of the department "non-destructive testing methods and devices» Petersburg State Transport University.
Academic interests: the detection and filtering of signals in non-destructive testing.
E-mail: churova_mk@mail.ru

Ryzhkov Alexey Viktorovich
postgraduate student St.-Petersburg State Electrotechnical University «LETI»
Academic interests: computer security, applied cryptography, commutative ciphers, software engineering.
E-mail: Ryzhkov.alex@gmail.com

Myl'nikov Pavel Dmitrievich
Appointment: head of sector Center control systems and traffic safety of the Scientific Research and Design Institute of Informatization, Automation and Communication on Railway Transport (JSC "NIIAS").
Academic interests: information security, transportation systems, digital communication systems.
E-mail: p.mylnikov@vniias.ru, paul.mylnikov@gmail.com

Popov Pavel Alexandrovich
Cand. Sci. (Eng.)
Appointment: head of the Center of control systems and traffic safety of the Scientific Research and Design Institute of Informatization, Automation and Communication on Railway Transport (JSC "NIIAS").
Academic interests: the interval control system, satellite navigation.
E-mail: p.popov@vniias.ru, pavel.niias@gmail.com