



Том 7. № 4
2021

ISSN: 1813-324X (print)
ISSN: 2712-8830 (online)

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Темы номера:

- ✓ Влияние деградации соединений на искажение оптических сигналов
- ✓ Модель функционирования сети связи на основе радиорелейных станций
- ✓ Генетическая декомпиляция машинного кода телекоммуникационных устройств

Vol. 7. Iss. 4
2021

PROCEEDINGS
OF TELECOMMUNICATION UNIVERSITIES

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Научный журнал

**ТРУДЫ
УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ**

Том 7. № 4

Proceedings of Telecommunication Universities

Vol. 7. Iss. 4

Санкт-Петербург

2021

Описание журнала

Научный журнал. Включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (распоряжение Минобрнауки России № 21-р от 12.02.2019), по специальностям (приказ № 118 от 24.02.2021):

1.2.2. Математическое моделирование, численные методы и комплексы программ

2.2.6. Оптические и оптико-электронные приборы и комплексы

2.2.13. Радиотехника, в том числе системы и устройства телевидения

2.2.14. Антенны, СВЧ-устройства и их технологии

2.2.15. Системы, сети и устройства телекоммуникаций

2.2.16. Радиолокация и радионавигация

2.3.1. Системный анализ, управление и обработка информации

2.3.6. Методы и системы защиты информации, информационная безопасность

Выпускается с 1960 года. Выходит 4 раза в год (ежеквартально). Издается на русском и английском языках.

Редакционный совет

Дукельский К.В. <i>Главный редактор</i>	к.т.н., доцент, АО «Государственный оптический институт имени С.И. Вавилова» (ГОИ), г. Санкт-Петербург, Россия
Буйневич М.В. <i>Зам. Главного редактора</i>	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Розанов Н.Н.	д.ф.-м.н., проф., чл.-корр. РАН, АО «Государственный оптический институт имени С.И. Вавилова» (ГОИ), г. Санкт-Петербург, Россия
Кучерявый Е.	PhD, Технологический университет Тампере, г. Тампере, Финляндия
Гошек И.	PhD, Технологический университет Брно, г. Брно, Чешская республика
Тиамийу О.А.	PhD, Университет Илорина, г. Илорин, Нигерия
Козин И.Д.	д.ф.-м.н., проф., Алматинский университет энергетики и связи, г. Алма-Аты, Казахстан
Самуйлов К.Е.	д.т.н., проф., Российский университет дружбы народов (РУДН), г. Москва, Россия
Степанов С.Н.	д.т.н., проф., Московский технический университет связи и информатики (МТУСИ), г. Москва, Россия
Росляков А.В.	д.т.н., проф., Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), г. Самара, Россия
Кучерявый А.Е.	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Канаев А.К.	д.т.н., проф., Петербургский университет путей сообщения имени Александра I (ПГУПС), г. Санкт-Петербург, Россия
Новиков С.Н.	д.т.н., проф., Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), г. Новосибирск, Россия
Дворников С.В.	д.т.н., проф., Военная академия связи им. Маршала Советского Союза С.М. Буденного (ВАС), г. Санкт-Петербург, Россия
Коржик В.И.	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Ковалгин Ю.А.	д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия
Владыко А.Г.	к.т.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Регистрационная информация

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций: ПИ № 77-77501 от 17.01.2020 г. (пред. рег. № 77-17986 от 07.04.2004 г.)

Подписной индекс в объединенном каталоге «ПРЕССА РОССИИ»: 59983

Размещение в РИНЦ (elibrary.ru) по договору: № 59-02/2013R от 20.02.2013

Контактная информация

Учредитель и издатель:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)	Адрес:	193232, Санкт-Петербург, пр. Большевиков, 22/1, к. 334/2
		редакции:	
		Тел.:	+7 (812) 326-31-63, м. т. 2022, +79643759970
		E-mail:	tuzs@spbgut.ru
		Web:	http://tuzs.sut.ru
		ВК:	http://vk.com/spbtuzs
Адрес учредителя:	191186, Санкт-Петербург, набережная реки Мойки, д. 61, литера А		

Description

Scientific journal. The journal is included in the List of reviewed scientific publications, in which the main scientific results of dissertations for the degree of candidate of science and for the degree of doctor of science should be published (order of the Ministry of Education and Science of Russia No 21-r of 12 February 2019) in the field of (order of the Ministry of Education and Science of Russia No 118 of 24 February 2021):

1.2.2. Mathematical modeling, numerical methods and complexes of programs

2.2.6. Optical and optoelectronic devices and complexes

2.2.13. Radio engineering, including television systems and devices

2.2.14. Antennas, microwave devices and its technologies

2.2.15. Systems, networks and telecommunication devices

2.2.16. Radiolocation and radio navigation

2.3.1. System analysis, management and information processing

2.3.6. Methods and systems of information security, cybersecurity

Since 1960. Published 4 times per year. Published in Russian and English.

Editorial Board

K.V. Dukel'skii <i>Editor-in-chief</i>	PhD, associate prof., executive Director of Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI), Saint-Petersburg, Russia
M.V. Buinevich <i>Deputy editor-in-chief</i>	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunications (SPbSUT), Saint-Petersburg, Russia
N.N. Rozanov	DSc, prof., member-corr. RAS, Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI), Saint-Petersburg, Russia
Y. Koucheryav	PhD, Tampere University of Technology, Tampere, Finland
I. Hošek	PhD, Brno University of Technology, Brno, Czech Republic
O.A. Tiamiyu	PhD, University of Ilorin, Ilorin, Nigeria
I.D. Kozin	DSc, prof., Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
K.E. Samuilov	DSc, prof., Peoples' Friendship University (RUDN), Moscow, Russia
S.N. Stepanov	DSc, prof., Moscow Technical University of Communication and Informatics (MTUCI), Moscow, Russia
A.V. Roslyakov	DSc, prof., Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia
A.E. Koucheryav	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
A.K. Kanaev	DSc, prof., Emperor Alexander I-st Petersburg State Transport University (PSTU), Saint-Petersburg, Russia
S.N. Novikov	DSc, prof., Siberian State University of Telecommunications and Information Sciences (SibSUTIS), Novosibirsk, Russia
S.V. Dvornikov	DSc, prof., Military Academy of Telecommunications named after Marshal Union S.M. Budyonny, Saint-Petersburg, Russia
V.I. Korzhik	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
Yu.A. Kovalgin	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
A.G. Vladyko	PhD, The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia

Registration Information

Registered by Federal Service for Supervision of Communications, Information Technology and Mass Media on 17.01.2020: PI No. 77-77501 (prev. reg. on 04.07.2004: No. 77-17986)

Subscription index for joint catalog «PRESSA ROSSII»: 59983

Accommodation in RINC (elibrary.ru) by agreement on 20.02.2013: No. 59-02/2013R

Contact Information

Publisher:	Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruевич Saint-Petersburg State University of Telecommunications» (SPbSUT)	Post address:	193232, Saint Petersburg, Prospekt Bolshevikov, 22/1
		Phone:	+7 (812) 326-31-63, local 2022, +79643759970
		E-mail:	tuzs@spbgut.ru
		Web:	http://tuzs.sut.ru
Publisher address:	191186, Saint Petersburg, Moika river embankment, 61-A		

Год науки и технологий: в ТУЗС – каждый год

Завершается непростой 2021 год. Журнал «Труды учебных заведений связи», несмотря на то, что постоянно вносятся штатные коррективы в нашу повседневную жизнь, продолжает удерживать высокую планку высококвалифицированного научного издания, соответствующему Году науки и технологий, который установлен Президентом Российской Федерации.

20.21 – ритм Редакции

В Указе Президента РФ от 25.12.2020 № 812 «О проведении в Российской Федерации Года науки и технологий» редакция журнала «Труды учебных заведений связи» ощутила официальную востребованность в результатах многолетней работы профессорско-преподавательского состава и научных работников нашего университета. Ориентирами Года науки и технологий в СПбГУТ стали изменения научных специальностей Высшей аттестационной комиссией (ВАК), мероприятия дорожной карты журнала, направленные на подготовку издания к подаче заявки на вступление в базу данных Scopus, расширение базиса публикационной активности сотрудников СПбГУТ, а также научный stream молодежи.

На основании рекомендации ВАК приказом Минобрнауки России от 24.02.2021 № 118 в соответствии с поручением Президента РФ от 28.03.2021 № Пр-589 была утверждена новая номенклатура научных специальностей, по которым присуждаются ученые степени. Наш журнал достаточно быстро отреагировал на изменения номенклатуры, и, начиная с № 2 тома 7 (2021), разместил новый рубрикатор научных специальностей. С опережением была усовершенствована неформальная база предварительной экспертизы результатов квалификационных работ Диссертационных советов, председатели – С.В. Бачевский и А.А. Гоголь [1], в которых прошли и успешно защищены в 2021 г. 3 докторские (А.И. Бобровский, Г.Г. Рогозинский, Г.А. Фокин) и 14 кандидатских диссертаций (А.А. оглы Ганбаев, Ву Дык Куен и Нгуен Ван Винь (Вьетнам), И.А. Кайсина, А.Н. Докучаева, В.В. Фицов, Н.А. Чистова, А.А. Миняев, Р.В. Жук, А.Н. Волков, М.В. Лобастова, Е.В. Тонких, П.Т.Д. Поннимбадуге (Шри-Ланка) и другие).

В Год науки и технологий Редакция действовала в рамках дорожной карты Scopus: утверждена новая редакция Устава журнала, введены Положение о стимулировании публикационной активности работников СПбГУТ в высокорейтинговых журналах и Положение о бюджетировании перевода метаданных и статей университета на английский язык. Также в рамках дорожной карты конструктивно проводится экспертиза подаваемых для опубликования рукописей с целью достижения ТУЗС с высокой научной значимостью публикаций [2]. В 2021 г. по результатам независимого рецензирования 12 рукописей не были приняты к печати, а наличие вхождения журнала в Перечень ВАК способствует тому, что на ближайшие номера 2021/2022 г.г. уже создан большой задел статей для опубликования.

Показатели публикационной активности СПбГУТ, характеризующие научную деятельность университета, неуклонно возрастают: количество публикаций авторов из СПбГУТ, индексируемых в базах данных Web of Science и Scopus, в 2016 г. составило 72, в 2020 г. – 168.

Наукометрические показатели журнала «Труды учебных заведений связи» демонстрируют положительную динамику. Согласно рейтингу SCIENCE INDEX по тематике «Связь» (по данным БД РИНЦ) издание поднялось с 23-го на 6-е место [3]. Суммарное количество цитирований журнала достигло 965 против 500 в 2019 г. Увеличилось количество новых авторов: в 2017 г. их было 27, в 2021 г. – 57. Расширилась география зарубежных авторов – в выпусках 2021 г. были опубликованы материалы исследований Научно-технологического института Малави (Индия), Университета Квазулу-Натар (ЮАР), Научно-технического университета Китая, Университета Луизиана (Ангола) и т. д.

[1] Ссылка на сайт СПбГУТ «Защиты диссертации в 2021 году»



[2] Ссылка на сайт журнала «Труды учебных заведений связи»



[3] Анализ публикационной активности журнала «Труды учебных заведений связи»



Все выпуски журнала размещаются на порталах Научно-электронной библиотеки «КиберЛенинка», Российской государственной библиотеки (РГБ), Государственной публичной научно-технической библиотеки. Расширяя свое присутствие на просторах научных электронных библиотек, увеличивается публикационная активность журнала. По данным e-library, если в 2019 г. количество просмотров статей журнала за год не превышало 2172, то сейчас оно достигло 4246, т. е. увеличилось в 2 раза.

Запасная скамейка ВАК – научные журналы университета

СПбГУТ издает несколько научных журналов. Один из них – рецензируемое сетевое издание «Информационные технологии и телекоммуникации» (электронный научный, научно-практический журнал), главным редактором которого является А.Е. Кучерявый [4]. В состав международной Редакционной коллегии входят представители Египта, Великобритании, Вьетнама, Чехии, Финляндии и Бразилии. Журнал выходит в свет 4 раза в год.

В разделе Системы, сети и устройства телекоммуникации должное освещение в 2021 г. получили проблемы машинного обучения (Д.Д. Алексеева, А.В. Марочкина, А.И. Парамонов), оптимизации мобильного трафика технологий Wi-Fi в условиях пандемии и дистанционного обучения (А.Д. Антоненко, Р.А. Дунайцев), сетевого кодирования (С.С. Владимиров, А.И. Фомин). В разделе Радиотехника, в том числе и устройства телевидения опубликованы исследования, связанные с моделированием радиоканала по модели Джейкса, обработкой цифровых сигналов и повышением помехоустойчивости их приема (Г.А. Фокин). В разделе Системный анализ, управление и обработка информации представлены научные результаты в сфере защиты веб-сервера от атаки злоумышленника (И.В. Давыдович, В.С. Зурахов, И.А. Ушаков), анализ векторов атак и сопутствующих им аномалии (М.М. Ковцур, А.Ю. Киструга, Г.Е. Ворошнин, А.Э. Федоров), методика определения необходимого и достаточного числа разовых испытаний в ходе ретроспективных исследований на базе геохронотрекинга (Я.А. Ивакин, С.Н. Потапычев, В.С. Елагин).

«Вестник гуманитарного факультета СПбГУТ» издается с 2004 г. [5], а в Год науки и технологий трансформируется не только по содержанию, но и по форме. В 2021 г. факультету исполнилось 25 лет, а с 01.04.2021 официальное название факультета – Социальных цифровых технологий. Социальные технологии – это методы воздействия на общество при помощи PR-коммуникаций, медиа, event'ов, рекламы и т. д. Социальные коммуникации не обходятся без онлайн-технологий, поэтому качественное социогуманитарное образование уже немыслимо без освоения цифровых навыков. Руководство факультета (Д.В. Шутман, А.Б. Гехт) планомерно работает по подготовке журнала к включению в Перечень ВАК.

Книжная полка науки – базис Редакции

Труд любого ученого складывается не только из научных публикаций в том или ином научном журнале, но и из любых других работ, в том числе и монографий. Ведь монография, как правило, посвящена глубокому изучению одной темы, содержащая новые гипотезы, концепции или теории. Она имеет узкую направленность, максимально подробно и всесторонне рассматривает проблему, демонстрируя глубокие знания и умение ученого проводить научные изыскания. Такой научный труд является итоговым.

По информации Редакционно-издательского отдела СПбГУТ [6], в 2021 г. вышли в свет 5 монографий. Например, Е.И. Туманова подготовила монографию «Требования к устройствам визуализации нового поколения». Авторы А.В. Куликович и А.Ю. Туманов представили труд «Методы оценки поражающих факторов источников чрезвычайных ситуаций при изолированном и комбинированном воздействии». Готовится к печати монография Ю.А. Ковалгина «Частотное планирование сетей цифрового радиовещания». С высоким дидактическим уровнем представлено учебное пособие «Геоинформационные системы в мониторинге и управлении техногенными объектами. Схемы и QR-ссылки», которое реализует методологию мобильного электронного образования, что несомненно актуально при дистанционных формах обучения.

[4] Ссылка на сайт журнала
«Информационные технологии
и телекоммуникации»



[5] Информация о журнале «Вестник
гуманитарного факультета СПбГУТ»
на сайте НЭБ eLIBRARY.RU



[6] Ссылка на сайт Управления
информационно-образовательных
ресурсов СПбГУТ



ТУЗС для ученых университета является площадкой для апробации новых научных результатов, и обобщенной отчетности в результатах монографий и комплекса публикаций. Книжную полку университета в 2021 г. как потенциал будущих публикаций в ТУЗС пополнили научные монографии и печатные учебные материалы А.Б. Волчкова, О.В. Воробьева, А.Б. Гехта, Ю.А. Дуболазовой, А.С. Дюбова, А.Г. Казанцевой, Ю.В. Кондрашова, В.Е. Коротина, М.В. Лобастовой, А.Н. Логиновской, В.В. Макарова, А.Ю. Матюхина, М.А. Мельтенисова, С.Р. Новиковой, Я.А. Плетнева, А.Г. Подгайского, М.Г. Слуцкого, М.П. Стародубцева, И.А. Ушакова, Е.Л. Федоровой, К.А. Фроловой, А.Г. Чернышова, А.В. Шестакова и других.

Молодежь – научный stream Редакции

Результаты научной работы молодых ученых оформлены в публикациях, размещенных в соответствующем разделе журнала ТУЗС – «Труды молодых ученых» [7]. Предложена модернизация метода Хука – Дживса для монотонно убывающей функции (В.В. Фицов), подходы к структурно-параметрическому моделированию блокчейн-систем (А.В. Спиркина), метод оценки качества группового управления роев автономных робототехнических комплексов (Т.В. Зикратова), проанализированы гомоморфные криптосистемы Бенало и Пэйе (В.Д. Салман), влияние режимов передачи, заложенных в стандарт DRM на размер зоны обслуживания (С.В. Мышьянов).

Ресурс идей и проектов для ТУЗС в 2021 г. – победители конкурса грантов Комитета по науке и высшей школе Санкт-Петербурга для студентов и аспирантов вузов отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, конкурса лучших инновационных проектов в сфере науки и высшего образования Санкт-Петербурга – аспиранты (А.П. Валов, А.А. Задорожная, А.В. Помогалова, А.А. Савельева, А.В. Спиркина) и студенты (факультета инфокоммуникационных сетей и систем, факультета информационных систем и технологий, института магистратуры, института непрерывного образования).

В номинации «Лучшая научно-инновационная идея» конкурса лучших инновационных проектов в сфере науки и высшего образования Санкт-Петербурга представлен проект СПбГУТ «Разработка методов, моделей и средств производительности и отказоустойчивости программно-определяемых систем хранения данных с помощью автоматизированного контроля и анализа диагностической информации с использованием нейронной сети», авторский коллектив: А.А. Зарубин, Н.Н. Алексеева, Н.А. Грудицын, Н.М. Редругина, А.А. Савельева, А.А. Швидкий [8].

Всероссийский конкурс на лучшую научную работу студентов образовательных организаций высшего образования, реализующих образовательные программы в области информационной безопасности, отметил работу СПбГУТ «Исследование влияния атак ARP inject и association flood на сети с оборудованием Mikrotik» (Г. Воронин).

В 2021 г. университет впервые номинирован в гранте по приоритетному направлению деятельности Российского научного фонда «Проведение фундаментальных научных исследований и поисковых научных исследований малыми отдельными научными группами» с тематикой «Диаграммообразование на основе позиционирования в сверхплотных сетях радиодоступа миллиметрового диапазона» (Г.А. Фокин).

Апробация результатов исследований молодых ученых на научно-практических конференциях проходила на конференциях, организованных университетом: АПИНО, ПКМ, ВАФО, СТУДЕНЧЕСКАЯ ВЕСНА. В 2021 г. СПбГУТ принимал несколько тематических форумов. В феврале проходила юбилейная, X-я Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» [9]. Действовало 7 научных направлений, в которых сделано более 600 докладов в 27 подсекциях, представителями ВУЗов России, телекоммуникационных и IT-компаний, учеными, аспирантами и студентами.

[7] Ссылка на раздел «Труды молодых ученых» в журнале «Труды учебных заведений связи»



[8] Победители конкурса инновационных проектов в СПбГУТ



[9] Ссылка на сайт конференции АПИНО



В мае состоялась 75-я Юбилейная региональная научно-техническая конференция студентов, аспирантов и молодых ученых «СТУДЕНЧЕСКАЯ ВЕСНА–2021» [10]. Участники представили свои научные результаты в семи научных направлениях: радиотехнологии связи, инфокоммуникационные сети и системы, информационные системы и технологии, теоретические основы радиоэлектроники, цифровая экономика, управление и бизнес-информатика, социальные цифровые технологии. На заседаниях 27 секций было представлено более 600 докладов. В ноябре в стенах СПбГУТ работала региональная научно-методическая конференция магистрантов и их руководителей «Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ)» [11]. Девиз конференции – апробация результатов научно-исследовательской деятельности магистрантов, их наставников, а также руководителей образовательных программ магистратуры. В декабре в университете состоялся Международный Балтийский коммуникационный форум – BAFO [12]. Масштабное научно-практическое мероприятие, ставшее визитной карточкой факультета ЦТ. Программа Форума включает в себя: мастер-классы от специалистов в области социальных, маркетинговых и международных коммуникаций; студенческая и преподавательская научные конференции, круглый стол «Цифровая трансформация в государственном управлении». По итогам Форума издан студенческий сборник тезисов и «Вестник факультета ЦТ».

Освещение новых технологий

Публикации в журнале «Труды учебных заведений связи» дают четкую информацию о выполнении НИР и грантов.

Например, в рамках Национальной программы «Цифровая экономика РФ» при поддержке Министерства цифрового развития, связи и массовых коммуникаций РФ, А.Г. Владыко и Г.А. Фокиным был исполнен НИР, который лег в основу проекта международной рекомендации МСЭ (ИК-16), что нашло свое отражение в статье «Позиционирование транспортных средств с комплексированием дальномерных, угломерных и инерциальных измерений в расширенном фильтре Калмана» (№ 2, 2021 г.).

В журнале были опубликованы и другие работы при поддержке РФФИ: результаты исследования характеристик изготовленных опытных образцов кирального маломодового оптического волокна (А.В. Бурдин, А.Ю. Барашкин, В.А. Бурдин, М.В. Дашков, В.В. Демидов и др.), способ построения схем цифровой подписи, основанных на скрытой задаче дискретного логарифмирования, на основе которого разработана практическая схема цифровой подписи (Молдовян Д.Н., Фахрутдинов Р.А., Мирин А.Ю., Костина А.А.).

Год науки и технологий: в ТУЗС – каждый год

По данным Генерального директора АНО «Национальные приоритеты» оператора Года науки и технологий Софии Малявиной, в стране было проведено более 4100 мероприятий, из них 3935 – в регионах.

8–10 декабря 2021 г. образовательный центр «Сириус» в Сочи стал площадкой для подведения итогов Года науки и технологий и определения приоритетов российской науки на будущие годы. На Конгрессе представили основные результаты Года науки и технологий в России. Отдельное внимание уделено результатам Года науки – тематическим месяцам: март посвящен новой медицине; апрель – освоение космоса; май – новые вызовы и угрозы безопасности; июнь – новые производственные материалы и технологии; июль – связанность территорий и освоение пространства; август – климат и экология; сентябрь – генетика и качество жизни; октябрь – энергетика будущего; ноябрь – искусственный интеллект; декабрь – человек, природа, общество и технологии. Для ТУЗС в 2022 г. Год науки и технологий продолжается.

Поздравляю коллектив Редакции, авторов публикаций и всех тех, кто запланировал объединить свои научные усилия под эгидой ТУЗС, с плодотворным 2021 годом и успешными очередными выпусками журнала университета в интересах науки...

Проректор по научной работе СПбГУТ,

доктор технических наук, старший научный сотрудник Александр Викторович Шестаков

[10] Ссылка на сайт конференции
СТУДЕНЧЕСКАЯ ВЕСНА



[11] Ссылка на сайт конференции ПКМ



[12] Ссылка на сайт конференции BAFO



СОДЕРЖАНИЕ

CONTENTS

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

Буранова М.А., Карташевский И.В. Применение ЕМ-алгоритма для аппроксимации гиперэкспонентами плотностей вероятностей коррелированного трафика	10	Buranova M., Kartashevskiy I. Application of EM-algorithm for approximation of correlated traffic probabilities density by hyperexponents
Бурдин А.В., Пашин С.С. Исследование влияния деградации разъемных соединений линейного тракта внутриобъектовых ВОЛП с криптоволокнами на искажение оптических сигналов мультигигабитных сетей передачи данных	18	Bourdine A., Pashin S. Research of fiber optic connector ferrule end-face degradation influence on optical pulse distortion during propagation over indoor multi-gigabit optical network links with crypto-fibers
Канаев А.К., Опарин Е.В., Опарина Е.В. Имитационная модель противостояния организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации	31	Kanaev A., Oparin E., Oparina E. A simulation model of the confrontation between an organized attacker and an information security system in the implementation of an attack on a network management system of clock network synchronization
Ковалгин Ю.А., Соколов С.А. Расчет зоны покрытия DRM-передатчиков, работающих в режиме устойчивости Е	43	Kovalgin Y., Sokolov S. Calculation DRM station coverage for robustness mode E
Ковальский А.А., Митряев Г.А., Питрин А.В. Управление орбитальным каналным ресурсом на основе немарковских приоритетных СМО. Часть 2. Методика диспетчеризации	54	Kovalsky A., Mitryaev G., Pitrin A. The orbital channel resource control on non-Markov priority systems of mass service basis. Part 2. Dispatch method
Одоевский С.М., Ключников В.О., Степанец И.В. Модель функционирования сети связи, построенной на основе радиорелейных станций с адаптивной модуляцией и коммутацией пакетов	63	Odoevsky S., Kluychnikov V., Stepanets I. Functional model of communication network of microwave link stations with adaptive modulation and package switching

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

Власенко А.В., Евсюков М.В., Путятто М.М., Макарян А.С. Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 2. Оценка прототипа	78	Vlasenko A., Evsyukov M., Putyato M., Makaryan A. Decision support system for finding an optimal postquantum key encapsulation mechanism. Part 2. Prototype evaluation
Иванов С.А. Метод оценки устойчивости информационного направления, функционирующего на ресурсах сети связи с отказами	85	Ivanov S. Method for assessing the sustainability of the information direction functioning on the resources of the communication network with failures
Израилов К.Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств	95	Izrailov K. The genetic decompilation concept of the telecommunication devices machine code
Кулик А.А. Метод парирования угрозы авиационного происшествия на основе искусственного интеллекта	110	Kulik A. Artificial intelligence-based aircraft accident threat parrying method

ТРУДЫ МОЛОДЫХ УЧЕНЫХ

Герасимович А.С. Безопасная передача информации при помощи двух методов бесключевой криптографии	119	Gerasimovich A. Secure information transfer using two keyless cryptography methods
Муренин И.Н. Обнаружение аномалий в трафике устройств Интернета вещей	128	Murenin I. Detection of IoT device traffic anomalies
Мышьянов С.В. Экспериментальное исследование влияния схем модуляции-кодирования на размер зоны обслуживания цифрового радиовещания DRM в диапазоне ОВЧ. Часть 2	138	Mishyanov S. Experimental research of modulation-coding schemes influence on size of the DRM digital radio broadcasting service area in the VHF band. Part 2

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

**2.2.6 – Оптические
и оптико–электронные приборы
и комплексы**

**2.2.13 – Радиотехника, в том числе системы
и устройства телевидения**

**2.2.14 – Антенны, СВЧ–устройства
и их технологии**

**2.2.15 – Системы, сети и устройства
телекоммуникаций**

2.2.16 – Радиолокация и радионавигация

Применение ЕМ-алгоритма для аппроксимации гиперэкспонентами плотностей вероятностей коррелированного трафика

М.А. Буранова¹^{*}, И.В. Карташевский¹

¹Поволжский государственный университет телекоммуникаций и информатики,
Самара, 443010, Российская Федерация

^{*}Адрес для переписки: buranova-ma@psuti.ru

Информация о статье

Поступила в редакцию 18.09.2021

Поступила после рецензирования 11.10.2021

Принята к публикации 18.10.2021

Ссылка для цитирования: Буранова М.А., Карташевский И.В. Применение ЕМ-алгоритма для аппроксимации гиперэкспонентами плотностей вероятностей коррелированного трафика // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 10–17. DOI:10.31854/1813-324X-2021-7-4-10-17

Аннотация: Точная оценка параметров качества обслуживания в современных инфокоммуникационных сетях является весьма важной задачей. В работе предложено использование гиперэкспоненциальных распределений для решения задачи аппроксимации произвольной плотности вероятностей в системе G/G/1 для случая, когда предполагается аппроксимация системой типа H₂/H₂/1. Для определения параметров плотности вероятностей гиперэкспоненциального распределения предлагается использовать ЕМ-алгоритм, который дает достаточно простые варианты использования для некоррелированных потоков. В данной работе предложен вариант реализации алгоритма ЕМ для определения параметров гиперэкспоненциального распределения при наличии корреляционных свойств анализируемого потока.

Ключевые слова: ЕМ-алгоритм, распределения случайных величин, корреляция, аппроксимация, QoS.

Введение

Традиционно для оценки параметров качества обслуживания используют методы теории массового обслуживания [1], при этом в простейшем случае такие системы представляются математической моделью системы обработки потоков на основе M/M/1, где интервалы времени между пакетами и интервалы длительности пакетов представляют собой последовательности независимых случайных величин с показательными плотностями вероятностей. Учитывая, что трафик современных приложений, обрабатываемый в IP-сети, отличается от простейшего потока и обладает фрактальными свойствами [2, 3], системы обработки таких потоков следует описывать моделью G/G/1. Следует учесть, что для потоков, генерируемых современными приложениями, часто характерно наличие корреляций внутри структур трафика [2, 3].

Использование известных математических подходов для оценки параметров качества обработки трафика современных приложений может привести к ошибочным результатам, потому что большинство подходов по оценке QoS основано на предположении отсутствия корреляций внутри струк-

тур потоков [1, 4–6]. При этом есть многочисленные доказательства того, что для современного трафика характерно наличие корреляционных свойств [7–10]. Это связано с характером формирования потоков, поведением пользователей, агрегированием потоков, сетевым управлением и т. д.

В то же время, работ по оценке параметров функционирования сетей с учетом обработки коррелированных потоков весьма мало, что осложняет возможность получения точных прогнозов функционирования инфокоммуникационных сетей в современных условиях. Существуют некоторые подходы к оценке параметров функционирования с учетом автокорреляции потоков, например, в работах [7–9, 11]. Но представленные подходы не всегда дают требуемую точность и связаны с необходимостью выполнения сложных вычислений.

Одним из возможных вариантов использования методов классической теории массового обслуживания при обработке коррелированного трафика является вариант аппроксимации системы G/G/1 системой H₂/H₂/1 [12], имеющей гиперэкспоненциально распределенное время поступления и об-

служивания. В [13, 14] было установлено, что применение смеси экспоненциальных распределений являются теоретически обоснованным подходом к моделированию IP-трафика. Получение аппроксимации такого типа возможно при использовании подходов кластерного анализа, например, алгоритма ЕМ (*аббр. от англ.* Expectation-Maximization), который позволяет определить параметры распределений и число экспонент аппроксимации реальной системы.

Кроме алгоритма ЕМ, существуют и другие подходы по определению параметров экспоненциальных распределений, такие как определение параметров по двум моментам (среднее, дисперсия) исходного распределения для независимых случайных величин [15]. При использовании данного подхода возможно получение аналитических выражений начальных моментов гиперэкспоненциальных распределений до второго порядка.

ЕМ-алгоритм часто применяют в разнообразных задачах оптимизации, он является удобным инструментом реализации итерационной процедуры поиска экстремума целевой функции с использованием численных методов. Такие подходы востребованы при поиске оценок максимального правдоподобия параметров вероятностных моделей в случае, если есть предположение о присутствии в модели скрытых переменных.

ЕМ-алгоритм является весьма эффективным для нахождения аппроксимации наблюдаемых реализаций как одномерных, так и многомерных распределений, но применение ЕМ-алгоритма, как правило, используется для разделения смеси нормальных распределений. Однако в теории очередей чаще всего используется показательное распределение, так как параметры, описывающие поведение трафика в современной IP-сети, являются непрерывными случайными величинами, принимающими неотрицательные значения.

Ранее в работах [6, 15] были представлены подходы по определению параметров гиперэкспоненциальных распределений с использованием ЕМ-алгоритма для систем с некоррелированными реализациями мгновенных значений случайных величин. Применение алгоритма ЕМ в случае наличия корреляционных свойств потока случайных величин вызывает безусловный интерес.

Реализация ЕМ-алгоритма для некоррелированных величин

Основными составляющими при оценке параметров QoS с использованием теории очередей являются следующие случайные величины: интервалы времени между пакетами и длины пакетов обрабатываемого в системе потока. Реализации потоков данных случайных интервалов времени обычно описываются различными распределениями для положительных случайных величин.

Смеси распределений являются весьма эффективным механизмом для описания плотностей распределения вероятностей любой реализации случайной величины в случае, если описание конкретным законом распределения с достаточной точностью вызывает затруднения.

Плотность вероятностей показательного распределения имеет вид:

$$f(x) = \lambda e^{-\lambda x},$$

где λ – параметр распределения, имеющий смысл интенсивности потока.

Если произвольную плотность вероятностей в системе $G/G/1$ на любой позиции G (в данном рассмотрении) обозначить как $w(x)$, то задача аппроксимации $w(x)$ с использованием гиперэкспоненциальных распределений может быть представлена в виде:

$$w(x) \approx H_K(x) = \sum_{i=1}^K p_i f_i(x), \quad (1)$$

где $f_i(x)$ – функция правдоподобия i -ой компоненты смеси, $f_i(x) = \lambda_i e^{-\lambda_i x}$, $p_i \geq 0$ – априорная вероятность:

$$\sum_{i=1}^K p_i = 1.$$

Для определения параметров гиперэкспоненциальных распределений можно воспользоваться подходом, основанным на использовании ЕМ-алгоритма [15–17], который может реализовывать получение достоверных оценок максимального правдоподобия для многих приложений, включая оценку параметров плотности смеси.

Будем предполагать, что в выражении (1) вид функций $f_i(x)$ известен, а параметры p_i и λ_i неизвестны, совокупность которых обозначим вектором $\theta = (p_1, \dots, p_K; \lambda_1, \dots, \lambda_K)$.

Теперь при разложении смеси (1) будем решать задачу статистического оценивания параметров θ по известной реализации случайной величины $X = (x_1, \dots, x_N)$. Предполагая независимость значений x_i , в рамках модели (1) логарифм функции правдоподобия $L(\theta; x)$ параметра θ имеет вид [18]:

$$\begin{aligned} \log L(\theta; x) &= \log \prod_{j=1}^N \phi_{\theta}^x(x_j) = \\ &= \sum_{j=1}^N \log \left(\sum_{i=1}^K p_i f_i(x_j; \theta_i) \right). \end{aligned} \quad (2)$$

Далее, следуя [18], введем в рассмотрение ненаблюдаемую случайную величину Y , которая играет роль индикатора выбора компоненты плотности $f_{\theta, y}^x(x_j)$, где y принимает значения $y_j \in (1, 2, \dots, K)$ ненаблюдаемой случайной величины Y . Другими

словами, предположим, что в процессе поступления x_j , $j = 1, \dots, N$, реализуется также ненаблюдаемое значение $y_j \in (1, 2, \dots, K)$.

Рассмотрим теперь совместную плотность случайных величин X и Y , обозначаемую как $\phi_\theta(x, y)$. С учетом того, что маргинальная плотность величины Y равна $\phi_\theta^Y(i) = p_i$, $i = 1, \dots, K$, для условной плотности случайной величины X при фиксированном $Y = i$ можно записать $\phi_\theta(x|i) = f_i(x; \theta_i)$.

Для полной функции правдоподобия, учитывающей присутствие в эксперименте случайной величины Y , следует:

$$\begin{aligned} \log L(\theta; x, y) &= \log \prod_{j=1}^N \phi_\theta(x_j, y_j) = \\ &= \sum_{j=1}^N \log \phi_\theta(x_j, y_j) = \sum_{j=1}^N \log [\phi_\theta(x_j|y_j) \phi_\theta^Y(y_j)] = \\ &= \sum_{j=1}^N \log [p_{y_j} f_{y_j}(x_{y_j}; \theta_{y_j})] = \\ &= \sum_{j=1}^N \log p_{y_j} + \sum_{j=1}^N \log f_{y_j}(x_{y_j}; \theta_{y_j}). \end{aligned} \quad (3)$$

С учетом вышеприведенных выражений для $\phi_\theta^Y(i)$ и $\phi_\theta(x|i) = f_i(x; \theta_i)$ совместная плотность $\phi_\theta(x, y)$ записывается как:

$$\phi_\theta(x, y) = p_y f_y(x; \theta_y) = \phi_\theta(y|x) \phi_\theta^X(x),$$

и на основе формулы Байеса для апостериорной вероятности того, что наблюдение x получено в соответствии с распределением, задаваемым компонентой f_i , можно получить:

$$\phi_\theta(y|x) = \frac{\phi_\theta(x, y)}{\phi_\theta^X(x)} = \frac{p_y f_y(x; \theta_y)}{\sum_{i=1}^K p_i f_i(x; \theta_i)}.$$

Далее, учитывая независимость реализаций X и Y , последняя формула записывается в виде:

$$\phi_\theta(y|x) = \prod_{j=1}^N \phi_\theta(y_j|x_j) = \prod_{j=1}^N \frac{p_{y_j} f_{y_j}(x_j; \theta_{y_j})}{\sum_{i=1}^K p_i f_i(x_j; \theta_i)}. \quad (4)$$

Как показано в [18], если определить условное среднее (по возможным итерациям) логарифма полной функции правдоподобия при известном значении наблюдаемой компоненты X , то максимизация этого условного среднего методом неопределенных множителей Лагранжа дает следующие формулы для формирования оценок максимального правдоподобия на каждой (m) -ой итерации алгоритма:

$$p_l^{(m+1)} = \frac{1}{N} \sum_{j=1}^N \frac{p_l^{(m)} f_l(x_j; \theta_l^{(m)})}{\sum_{i=1}^K p_i^{(m)} f_i(x_j; \theta_i^{(m)})}, \quad (5)$$

$$\lambda_l^{(m+1)} = \frac{\sum_{j=1}^N \frac{f_l^{(m)}(x_j) \cdot x_j}{\sum_{l=1}^K f_l^{(m)}(x_j)}}{\sum_{j=1}^N \frac{f_l^{(m)}(x_j)}{\sum_{l=1}^K f_l^{(m)}(x_j)}}, \quad l = 1, \dots, K. \quad (6)$$

В формуле (6) учитывается, что при гиперэкспоненциальной аппроксимации $f_l(x) = \lambda_l e^{-\lambda_l x}$ и для модели $H_2(x)$ оцениванию подлежат только три параметра: p , λ_1 , λ_2 , т. к. модель $H_2(x)$ может быть представлена в виде:

$$g(x; p, \lambda_1, \lambda_2) = p \lambda_1 e^{-\lambda_1 x} + (1-p) \lambda_2 e^{-\lambda_2 x}.$$

С введением обозначения $g(x; p, \lambda_1, \lambda_2)$ формулы (5) и (6) могут быть записаны проще:

$$p^{(m+1)} = \frac{1}{N} \sum_{j=1}^N \frac{p^{(m)} f_1(x_j; \lambda_1^{(m)})}{g^{(m)}(x_j)}, \quad (7)$$

$$\lambda_l^{(m+1)} = \frac{\sum_{j=1}^N \frac{f_l^{(m)}(x_j) \cdot x_j}{g^{(m)}(x_j)}}{\sum_{j=1}^N \frac{f_l^{(m)}(x_j)}{g^{(m)}(x_j)}}, \quad l = 1, 2. \quad (8)$$

Рассмотренный подход применим для последовательностей с независимыми (в крайнем случае некоррелированными) случайными величинами. В случае наличия корреляции внутри последовательностей необходимо применять другие подходы.

Реализация ЕМ-алгоритма для коррелированных величин

Известно, что при вычислении оценок максимального правдоподобия для ненаблюдаемых параметров априорная информация играет очень важную роль. Для последовательности $(x_1, x_2, \dots, x_N)$, которая обладает корреляционными связями соседних элементов, коэффициент корреляции $R = R(x_{k-1}, x_k)$ является необходимой информацией для построения оценок плотностей вероятностей смеси.

Поэтому на этапе определения априорных сведений о последовательности $(x_1, x_2, \dots, x_N)$ целесообразно получить оценку одномерной плотности вероятностей $\hat{w}(x)$ и ее первых двух моментов m_x, σ_x^2 , а также коэффициента корреляции соседних элементов R . Кроме того, для инициализации вычислений при нулевой итерации ($m = 0$) следует в последовательности $(x_1, x_2, \dots, x_N)$ задать элемент x_0 (возможно $x_0 = 0$), т. е. для $g(x; p, \lambda_1, \lambda_2)$ задать значения λ_1 , λ_2 и p . Значение отсчета x_0 , в принципе, может выбираться произвольно, главное, чтобы это значение было сопоставимо с m_x .

Если $(x_1, x_2, \dots, x_N)$ – заданная последовательность временных интервалов, то, очевидно, что $\lambda_x = m_x^{-1}$ имеет смысл интенсивности наступления некоторых событий. Тогда при нулевой итерации ($m = 0$) при обработке отсчета x_0 можно ограничиться заданием одного параметра интенсивности

(например, λ_1), т. к. λ_1 и λ_2 связаны очевидным соотношением:

$$\lambda_x = \frac{\lambda_1 \lambda_2}{p \lambda_2 + (1-p) \lambda_1}, \quad (9)$$

из которого при заданном λ_1 и априорно известном λ_x можно легко определить λ_2 .

Выбор значения для λ_1 достаточно произволен, но всегда надо следить за тем, чтобы полученное из (9) значение λ_1 было положительным. В противном случае необходимо изменить выбор для λ_1 . Выбор значения p из интервала $(0, 1)$ также достаточно произволен, но обычно выбирается $p = 0,5$.

Корреляционные свойства последовательности $(x_1, x_2, \dots, x_N)$ благодаря рекуррентности формул (7) и (8) могут быть явно учтены в этих формулах, если установить аналитическую связь соседних элементов последовательности.

Это можно сделать при использовании уравнения регрессии, записанного в виде [11]:

$$x_k = R x_{k-1} + m_x(1-R) + (\sigma_x \sqrt{1-R^2}) S, \quad (10)$$

где S – случайная нормально распределенная величина с нулевым средним и единичной дисперсией, не коррелированная с x_k .

Учтем теперь выражение (10) в рекуррентном соотношении (8). Выпишем несколько первых слагаемых из числителя выражения при $l = 1$, включив в него слагаемое для x_0 , служащее для инициализации процесса вычислений:

$$\frac{f_1(x_0) \cdot x_0}{g(x_0)} + \frac{f_1(x_1) \cdot x_1}{g(x_1)} + \frac{f_1(x_2) \cdot x_2}{g(x_2)} + \dots \quad (11)$$

Рассмотрим формирование значения $f_1(x_i)x_i$ в формуле (8) с учетом соотношения (10). Например, при обработке x_1 :

$$f_1(x_1) \cdot x_1 = f_1(x_1) \left[\frac{1}{R} (x_2 - m_x(1-R) - S^{(2)}) \right] = \frac{1}{R} f_1(x_1) [x_2 - G^{(2)}]. \quad (12)$$

где $G^{(2)} = m_x(1-R) + (\sigma_x \sqrt{1-R^2}) S^{(2)}$ – случайная величина, которая должна генерироваться в данном случае на втором шаге вычислений, когда проводятся вычисления, связанные с элементом последовательности x_2 .

Очевидно, для произвольного x_i :

$$f_1(x_i)x_i = \frac{1}{R} f_1(x_i) [x_{i+1} - G^{(i+1)}]. \quad (13)$$

Стоящее в правой части выражения (13) значение $f_1(x_i)$ вычисляется по информации о λ_1 , полученной на предыдущей итерации вычислений:

$$f_1^{(m)}(x_i) = \lambda_1^{(m-1)} e^{-\lambda_1^{(m-1)} x_i}. \quad (14)$$

Соответственно:

$$g^{(m)}(x_i) = p^{(m-1)} \lambda_1^{(m-1)} e^{-\lambda_1^{(m-1)} x_i} + (1 - p^{(m-1)}) \lambda_2^{(m-1)} e^{-\lambda_2^{(m-1)} x_i}.$$

Теперь можно определить порядок действий при реализации соотношений (7) и (8).

1) Методами статистического анализа, реализованного соответствующими программными продуктами, определяется плотность вероятностей $\hat{w}(x)$, аппроксимирующая истинную плотность анализируемой выборки. Определяются также моменты m_x , σ_x^2 и коэффициент корреляции соседних элементов R . При этом предполагается, что следующим шагом аппроксимации $\hat{w}(x)$, является выбор функции:

$$g(x) = p f_1(x) + (1-p) f_2(x).$$

2) Осуществляется выбор исходных данных p , $\lambda_1(0)$, $\lambda_2(0)$ для x_0 .

3) Текущие вычисления производятся по формулам (7) и (8) с использованием (10) и (12). Особенностью вычислений является то, что на каждом шаге необходимо генерировать нормальную случайную величину со средним значением $m_x(1-R)$ и дисперсией $\sigma_x^2(1-R^2)$.

4) Выбор момента останова вычислений можно выбирать следующим образом.

Если ошибку аппроксимации на каждом (v) -шаге представить в виде:

$$\varepsilon_{(v)} = \frac{\sum_{i=1}^{(v)} \log[g^{(v)}(x_i)] - \sum_{i=1}^{(v)} \log[g^{(v-1)}(x_i)]}{\sum_{i=1}^{(v)} \log[g^{(v-1)}(x_i)]},$$

где при фиксированном N должно выполняться $(v)_{\max} < N$, то при выполнении условия $\varepsilon_{(v)} \leq \varepsilon_{\text{пороговое}}$, можно считать алгоритм сходящимся и фиксировать полученные значения $p^{(v)}$, $\lambda_1^{(v)}$, $\lambda_2^{(v)}$. В противном случае следует искать другую «траекторию» вычислений, задав другое начальное значение x_0 [18]. При данном вычислении и значение $\varepsilon_{\text{пороговое}}$, изменив которое, можно получить сходящийся алгоритм, оказывает влияние на сходимость алгоритма.

Анализ ошибки аппроксимации при выполнении условия $\varepsilon_{(v)} \leq \varepsilon_{\text{пороговое}}$ можно осуществить, используя для оценивания ошибки аппроксимации меру Кульбака – Лейблера [19]:

$$\Delta = \sum_{i=1}^N w(x_i) \ln \frac{w(x_i)}{g(x_i)}.$$

Анализ точности аппроксимации через параметр Δ целесообразно проводить для выбора среди сходящихся «траекторий» наилучшей, т. е. обладающей наименьшим значением Δ .

Моделирование работы ЕМ-алгоритма при коррелированной реализации случайных величин

Проверка работоспособности рассмотренного алгоритма расчета параметров аппроксимирующей плотности (1) при коррелированной выборке была проведена на основе эксперимента, реализованного методом статистического моделирования. Для простоты моделирования была выбрана последовательность случайных событий с интервалами времени между событиями, имеющими логнормальное распределение с заданным коэффициентом корреляции соседних интервалов.

Плотность вероятностей логнормального распределения имеет вид:

$$w(x) = \frac{1}{\sigma_0 x \sqrt{2\pi}} \exp\left(-\frac{\ln^2 x}{2\sigma_0^2}\right),$$

$$m_x = \sigma_0 \sqrt{e}, \quad \sigma_x^2 = e(e-1)\sigma_0^2.$$

Моделирование стационарного логарифмически-нормального случайного процесса с заданным коэффициентом корреляции R можно осуществить следующим образом [20]:

– моделируется нормальный стационарный случайный процесс $\{y_i\}$, $i = 1, 2, \dots$ с коэффициентом корреляции:

$$\rho = \ln(1 + (e-1)R),$$

– каждый элемент последовательности y_i подвергается преобразованию $x = e^y$ для получения последовательности $\{x_i\}$, $i = 1, 2, \dots$

При этом нормальный процесс с заданным коэффициентом корреляции моделируется разностным уравнением первого порядка:

$$y(n) = a_0 \xi(n) + b_1 y(n-1),$$

где $a_0 = \sigma_0 \sqrt{1 - \rho^2}$; $b_1 = \rho$; $\xi(n)$ – последовательность нормальных случайных чисел с нулевым средним и единичной дисперсией – $N(0,1)$.

Итак, если положить, что $R = 0,7$, то при $\sigma_0 = 1$ получается $a_0 = 0,613$, $b_1 = 0,79$.

Сгенерированная трасса из 5000 логнормальных интервалов с коэффициентом корреляции соседних интервалов $R = 0,7$, с начальными условиями, согласованными с (9), в виде:

$$\lambda_x = 0,606, \quad p = 0,5, \quad \lambda_1 = 0,5, \quad \lambda_2 = 0,77$$

при обработке алгоритмом ЕМ по формулам (7) и (8) с $\varepsilon_{\text{пороговое}} = 0,01$ дала при $(v) = 499$ следующие результаты:

$$\hat{p} = 0,45, \quad \hat{\lambda}_1 = 2,72, \quad \hat{\lambda}_2 = 2,78.$$

Это означает, что для трассы с коэффициентом корреляции соседних элементов $R = 0,7$ вместо модели плотности в виде гиперэкспоненциального распределения $g(x; p, \lambda_1, \lambda_2)$ можно использовать (в рамках допустимой погрешности) просто экспоненциальное распределение с показателем $\lambda \approx 2,75$.

Такой вывод основан на более подробном анализе корреляционных свойств сгенерированной трассы, представленном на рисунке 1 и на сравнении данных результатов с результатами, полученными в работах [9, 21].

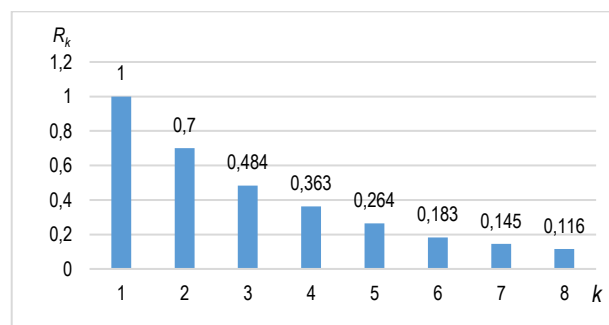


Рис. 1. Коэффициенты корреляции последовательности

Fig. 1. Sequence Correlation Coefficients

В этих работах рассмотрены методы синтеза параметров гиперэкспоненциального распределения $H_2(x)$ при полном учете корреляционных свойств последовательности (таких, как на рисунке 1), который основан на использовании индекса дисперсии интервалов (или отсчетов) последовательности. Практически все результаты в данных работах указывают на то, что одна из экспонент в распределении $H_2(x)$ в данной ситуации присутствует с весом p из интервала $(0,95 \dots 0,98)$. Поэтому для достаточно простой модели плотности вероятностей мгновенных значений коррелированной последовательности случайных интервалов времени может использоваться экспоненциальная плотность с показателем, учитывающим корреляционные свойства последовательности. Справедливость данного утверждения демонстрируют результаты, показанные на рисунке 2, где приведены плотности распределений вероятностей при полученных значениях параметров гиперэкспоненциальных распределений для коррелированного трафика ($f_k(t)$), для некоррелированного трафика ($f_n(t)$), а также в случае использования экспоненциальной плотности распределений коррелированного трафика ($f_{1\text{exp}}(t)$) и некоррелированного трафика ($f_{2\text{exp}}(t)$).

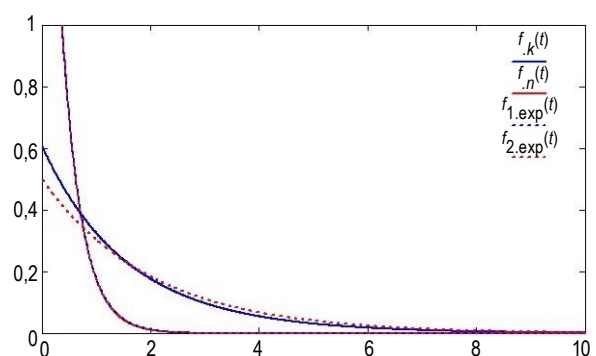


Рис. 2. Плотности распределений вероятностей

Fig. 2. Densities of Probability Distributions

Анализ полученных результатов (см. рисунок 2) показывает, что график плотности экспоненциального распределения практически совпал с графиком плотности гиперэкспоненциального распределения для некоррелированной последовательности, и весьма близок для коррелированной последовательности.

Использование ЕМ-алгоритма подтвердило вывод о том, что при рекуррентном формировании оценок максимального правдоподобия для параметров гиперэкспоненциального распределения при априорной неопределенности относительно значений этих параметров, оценивания параметров гиперэкспоненциального распределения при наличии корреляционных свойств у рассматриваемых последовательностей.

Заключение

В работе представлена методика аппроксимации распределения смеси гиперэкспонентами для систем обработки коррелированного потока с использованием ЕМ-алгоритма. В результате были

получены выражения для программной реализации ЕМ-алгоритма для случаев некоррелированных и коррелированных потоков.

Проверка на основе использования методов статистического моделирования работоспособности представленного ЕМ-алгоритма для коррелированных последовательностей была проведена для случайных величин, имеющих логнормальное распределение с коэффициентом корреляции соседних интервалов $R = 0,7$. Результаты проверки показали точность в пределах порогового значения $\varepsilon_{\text{пороговое}} = 0,01$. Были получены следующие параметры гиперэкспоненциального распределения: $\hat{p} = 0,45$, $\hat{\lambda}_1 = 2,72$, $\hat{\lambda}_2 = 2,78$. Данные результаты согласуются с решениями, полученными на основе других подходов оценивания параметров гиперэкспоненциальных распределений.

Установлено, что для достаточно простой модели плотности вероятностей мгновенных значений коррелированной последовательности случайных величин может использоваться экспоненциальная плотность с параметром, учитывающим корреляционные свойства последовательности.

Список используемых источников

1. Kleinrock L. Queueing Systems. Vol. I. Theory. John Wiley & Sons, 1975. 432 p.
2. Шелухин О.И., Тенякшев А.М., Осин А.В. Фрактальные процессы в телекоммуникациях. М.: Радиотехника, 2003. 480 с.
3. Буранова М.А. Исследование статистических характеристик самоподобного телекоммуникационного трафика // Инфокоммуникационные технологии. 2012. Т. 10. № 4. С. 35–41.
4. Kartashevskiy V., Kireeva N., Buranova M., Chupakhina L. Study of queueing system G/G/1 with an arbitrary distribution of time parameter system // Proceedings of the 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T, Kharkiv, Ukraine, 13–15 October 2015). IEEE, 2015. DOI:10.1109/INFOCOMMST.2015.7357297
5. Kartashevskiy V., Buranova M. Analysis of Packet Jitter in Multiservice Network // Proceedings of the 5th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T, Kharkiv, Ukraine, 9–12 October 2018). IEEE, 2015. PP. 797–802. DOI:10.1109/INFOCOMMST.2018.8632085.
6. Буранова М.А., Карташевский В.Г., Латыпов Р.Т. Оценка джиттера в системе G/M/1 на основе использования гиперэкспоненциальных распределений // Инфокоммуникационные технологии. 2020. Т. 18. № 1. С. 13–20. DOI:10.18469/ikt.2020.18.1.02
7. Kartashevskiy I., Buranova M. Calculation of Packet Jitter for Correlated Traffic // Proceedings of the 19th International Conference on Next Generation Wired/Wireless Networking (NEW2AN 2019) and Proceedings of the 12th Conference on Internet of Things and Smart Spaces (ruSMART, 2019, St. Petersburg, Russia, 26–28 August 2019). Lecture Notes in Computer Science. Computer Communication Networks and Telecommunications. Vol. 11660. PP. 610–620. Cham: Springer, 2019. DOI:10.1007/978-3-030-30859-9_53.
8. Vishnevskii V.M., Dudin A.N. Queueing Systems with Correlated Arrival Flows and Their Applications to Modeling Telecommunication Networks // Automation and Remote Control. 2017. Vol. 78(8). PP. 1361–1403. DOI:10.1134/S000511791708001X
9. Balcioglu B., Jagerman D.L., Altioek T. Approximate mean waiting time in a GI/D/1 queue with autocorrelated times to failures // IIE Transactions. 2007. Vol. 39. Iss. 10. PP. 985–996. DOI:10.1080/07408170701275343
10. Бузов А.Л., Букашкин С.А. Специальная радиосвязь. Развитие и модернизация оборудования и объектов. М.: Радиотехника, 2017. 448 с.
11. Balcioglu B., Jagerman D.L., Altioek T. Merging and splitting autocorrelated arrival processes and impact on queueing performance // Performance Evaluation. 2008. Vol. 65. Iss. 9. PP. 653–669. DOI:10.1016/j.peva.2008.02.003
12. Keilson J., Machihara F. Hyperexponential waiting time structure in hyperexponential $H_N/H_K/1$ system // Journal of the Operation Society of Japan. 1985. Vol. 28(3). PP. 242–250.
13. Feldmann A., Whitt W. Fitting Mixtures of Exponentials to Long-Tail Distributions to Analyze Network Performance Models // Performance Evaluation. 1998. Vol. 31. Iss. 3-4. PP. 245–279. DOI:10.1016/S0166-5316(97)00003-5
14. Buranova M., Ergasheva D., Kartashevskiy V. Using the EM-algorithm to approximate the Distribution of a Mixture by Hyperexponents // Proceedings of the International Conference on Engineering and Telecommunication (EnT, Dolgoprudny, Russia, 20–21 November 2019). IEEE, 2019. DOI:10.1109/EnT47717.2019.9030551
15. Baird S.R. Estimating mixtures of exponential distributions using maximum likelihood and the EM algorithm to improve

simulation of telecommunication networks. University of British Columbia, 2002. URL: <https://open.library.ubc.ca/collections/ubctheses/831/items/1.0090805> (дата обращения 18.10.2021)

16. Королев В.Ю. ЕМ-алгоритм, его модификации и их применение к задаче разделения смесей вероятностных распределений. Теоретический обзор. М.: ИПИ РАН, 2007. 94 с.

17. Воронцов К.В. Математические методы обучения по прецедентам (теория обучения машин) URL: <http://www.machinelearning.ru/wiki/images/6/6d/Voron-ML-1.pdf> (дата обращения 18.10.2021)

18. Ip E.H. A Stochastic EM Estimator in the Presence of Missing Data: Theory and Practice. PhD Dissertation. Stanford University, 1994. 127 p.

19. Kullback S., Leibler R.A. On information and sufficiency // The Annals of Mathematical Statistics. 1951. Vol. 22. PP. 79–86.

20. Быков В.В. Цифровое моделирование в статистической радиотехнике. М.: Советское радио, 1971. 328 с.

21. Карташевский И.В., Сапрыкин А.В. Анализ времени ожидания заявки в очереди для системы массового обслуживания общего вида // Т-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 2. С. 4–10. DOI:10.24411/2072-8735-2018-10024

* * *

Application of EM-Algorithm for Approximation of Correlated Traffic Probabilities Density by Hyperexponents

M. Buranova¹, I. Kartashevskiy¹

¹Povolzhskiy State University of Telecommunications and Informatics, Samara, 443010, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-10-17

Received 18th September 2021

Revised 11th October 2021

Accepted 18th October 2021

For citation: Buranova M., Kartashevskiy I. Application of EM-Algorithm for Approximation of Correlated Traffic Probabilities Density by Hyperexponents. *Proc. of Telecom. Universities*. 2021;7(4):10–17. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-10-17

Abstract: An accurate assessment of the quality of service parameters in modern information communication networks is a very important task. This paper proposes the use of hyperexponential distributions to solve the problem of approximating an arbitrary probability density in the G/G/1 system for the case when the approximation by a system of the type $H_2/H_2/1$ is assumed. To determine the parameters of the probability density of the hyperexponential distribution, it is proposed to use EM- algorithm that provides fairly simple use cases for uncorrelated flows. In this paper, we propose a variant of the EM algorithm implementation for determining the parameters of the hyperexponential distribution in the presence of correlation properties of the analyzed flow.

Keywords: EM-algorithm, distributions of random variables, correlation, approximation, QoS.

References

1. Kleinrock L. *Queueing Systems. Vol. I. Theory*. John Wiley & Sons; 1975. 432 p.
2. Sheluhin O.I., Tenyakshev A.M., Osin A.V. *Fractal Processes in Telecommunications*. Moscow: Radiotekhnika Publ.; 2003. 480 p. (in Russ.)
3. Buranova M.A. Research of statistical characteristics of the self-similar telecommunication traffic. *Infokommunikacionnie tehnologii*. 2012;10(4):35–40. (in Russ.)
4. Kartashevskiy V., Kireeva N., Buranova M., Chupakhina L. Study of queueing system G/G/1 with an arbitrary distribution of time parameter system. *Proceedings of the 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T, 13–15 October 2015, Kharkiv, Ukraine*. IEEE; 2015. DOI:10.1109/INFOCOMMST.2015.7357297
5. Kartashevskiy V., Buranova M. Analysis of Packet Jitter in Multiservice Network // *Proceedings of the 5th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T, 9–12 October 2018, Kharkiv, Ukraine*. IEEE; 2018. p.797–802. DOI:10.1109/INFOCOMMST.2018.8632085

6. Buranova M.A., Kartashevskiy V.G., Latypov R.T. Estimation of jitter in the G/M/1 system based on the use of hyperexponential distributions. *Infokommunikacionnie tehnologii*. 2020;18(1):13–20. (in Russ.) DOI:10.18469/ikt.2020.18.1.02
7. Kartashevskiy I., Buranova M. Calculation of Packet Jitter for Correlated Traffic. *Proceedings of the 19th International Conference on Next Generation Wired/Wireless Networking, NEW2AN 2019, and Proceedings of the 12th Conference on Internet of Things and Smart Spaces, ruSMART 2019, 26–28 August 2019, St. Petersburg, Russia. Lecture Notes in Computer Science. Computer Communication Networks and Telecommunications*. vol.11660. p.610–620. Cham: Springer; 2019. DOI:10.1007/978-3-030-30859-9_53
8. Vishnevskii V.M., Dudin A.N. Queueing Systems with Correlated Arrival Flows and Their Applications to Modeling Telecommunication Networks. *Automation and Remote Control*. 2017;78(8):1361–1403. DOI:10.1134/S000511791708001X
9. Balcioglu B., Jagerman D.L., Altioek T. Approximate mean waiting time in a GI/D/1 queue with autocorrelated times to failures. *IIE Transactions*. 2007;39(10):985–996. DOI:10.1080/07408170701275343
10. Buzov A.L., Bukashkin S.A. *Special Radio Communication. Development and Modernization of Equipment and Facilities*. Moscow: Radiotekhnika Publ.; 2017. 448 p. (in Russ.)
11. Balcioglu B., Jagerman D.L., Altioek T. Merging and splitting autocorrelated arrival processes and impact on queueing performance. *Performance Evaluation*. 2008;65(9):653–669. DOI:10.1016/j.peva.2008.02.003
12. Keilson J., Machihara F. Hyperexponential waiting time structure in hyperexponential $H_N/H_K/1$ system. *Journal of the Operation Society of Japan*. 1985;28(3):242–250.
13. Feldmann A., Whitt W. Fitting Mixtures of Exponentials to Long-Tail Distributions to Analyze Network Performance Models. *Performance Evaluation*. 1998;31(3-4):245–279. DOI:10.1016/S0166-5316(97)00003-5
14. Buranova M., Ergasheva D., Kartashevskiy V. Using the EM-algorithm to approximate the Distribution of a Mixture by Hyperexponents. *Proceedings of the International Conference on Engineering and Telecommunication, EnT, 20–21 November 2019, Dolgoprudny, Russia*. IEEE; 2019. DOI:10.1109/EnT47717.2019.9030551
15. Baird S.R. *Estimating mixtures of exponential distributions using maximum likelihood and the EM algorithm to improve simulation of telecommunication networks*. University of British Columbia; 2002. Available from: <https://open.library.ubc.ca/collections/ubctheses/831/items/1.0090805> [Accessed 18th October 2021]
16. Korolyov V.Yu. The EM-Algorithm, its Modifications, and Their Application to the Problem of Separating Mixtures of Probability Distributions. Theoretical Review. Moscow: Institute of Informatics Problems of the Russian Academy of Sciences Publ.; 2007. 94 p. (in Russ.)
17. Voroncov K.V. Mathematical Teaching Methods on Precedents. (in Russ.) Available from: <http://www.machinelearning.ru/wiki/images/6/6d/Voron-ML-1.pdf> [Accessed 18th October 2021]
18. Ip E.H. *A Stochastic EM Estimator in the Presence of Missing Data: Theory and Practice*. PhD Dissertation. Stanford University; 1994. 127 p.
19. Kullback S., Leibler R.A. On information and sufficiency. *The Annals of Mathematical Statistics*. 1951;22:79–86.
20. Bykov V.V. *Digital Modeling in Statistical Radio Engineering*. Moscow: Soviet radio Publ.; 1971. 328 p. (in Russ.)
21. Kartashevskiy I.V., Saprykin A.V. Waiting time analysis for the request in general queueing system. *T-Comm*. 2018;12(2): 4–10. (in Russ.) DOI:10.24411/2072-8735-2018-10024

Сведения об авторах:

БУРАНОВА
Марина Анатольевна

кандидат технических наук, доцент, доцент кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, buranova-ma@psuti.ru
 <https://orcid.org/0000-0003-2986-8252>

КАРТАШЕВСКИЙ
Игорь Вячеславович

доктор технических наук, профессор кафедры программного обеспечения и управления в технических системах Поволжского государственного университета телекоммуникаций и информатики, ivk@psuti.ru
 <https://orcid.org/0000-0002-1388-4867>

Исследование влияния деградации разъемных соединений линейного тракта внутриобъектовых ВОЛП с криптоволоконными на искажение оптических сигналов мультигигабитных сетей передачи данных

А.В. Бурдин^{1, 2}, С.С. Пашин²

¹Научно-производственное объединение Государственный оптический институт им. С.И. Вавилова, Санкт-Петербург, 192171, Российская Федерация

²Поволжский государственный университет телекоммуникаций и информатики, Самара, 443010, Российская Федерация

*Адрес для переписки: pashinstanislav@outlook.com, bourdine@yandex.ru

Информация о статье

Поступила в редакцию 23.08.2021

Поступила после рецензирования 08.10.2021

Принята к публикации 13.10.2021

Ссылка для цитирования: Бурдин А.В., Пашин С.С. Исследование влияния деградации разъемных соединений линейного тракта внутриобъектовых ВОЛП с криптоволоконными на искажение оптических сигналов компактных мультигигабитных сетей передачи данных // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 18–30. DOI:10.31854/1813-324X-2021-7-4-18-30

Аннотация: Представлены результаты апробации модели кусочно-регулярной волоконно-оптической линии передачи, функционирующей в маломодовом режиме с последовательно соединенной парой специализированных многомодовых оптических криптоволокон, выполняющих функции «шифратор – дешифратор». Модель дополнена возможностью учета влияния на условия ввода сигнала с выхода когерентного источника в оптоволоконной линии характера и степени загрязнения торцевой поверхности феррул волоконно-оптических коннекторов. Приведены результаты сопоставления расчетных огибающих искаженных оптических импульсов, распространяющихся в описанных линиях передачи с криптоволоконными сетями спецификации 10GBase-LX, в зависимости от состояния торца феррула коннектора оптоволоконной линии, подключаемого к источнику излучения трансивера.

Ключевые слова: феррул, волоконно-оптический коннектор, загрязнение феррула, торец феррула, волоконно-оптическое разъемное соединение, коэффициент связи мод, структурированные кабельные системы, дифференциальная модовая задержка.

Введение

В ранее опубликованных работах [1, 2] было предложено техническое решение организации защищенного на физическом уровне канала передачи конфиденциальной информации кластера/сегмента внутрикорпоративной сети связи «первая/последняя миля». Данный кластер «первой/последней мили» внутрикорпоративных сетей, в целом, отличается малой протяженностью соединительных кабельных линий: от десятков метров – в случае структурированных кабельных систем (СКС) центров обработки данных, до 1–2 км, соответствующих «кампусным» СКС, объединенной группы зданий (производственные цеха, технологические площадки и административные помещения предприятия). Для этого сегмента се-

тей также характерно увеличенное, по сравнению с сетями передачи данных общего пользования, количество информационных портов. В настоящее время, как минимум, вертикальные подсистемы современных СКС реализуются на базе волоконно-оптических кабелей (ОК) с применением технологии FTTE (*аббр. от англ.* Fiber to the Enclosure – волокно до конструктива). Однако нередко в условиях повышенных требований к пропускной способности соответствующего подкластера сети, объединяющего выделенную группу пользователей, используется технология FTTD (*аббр. от англ.* Fiber to the Desk – волокно до рабочего места), и в этом случае горизонтальная подсистема СКС также представляет собой совокупность ОК [3].

Предлагаемое решение базируется на применении в соединительных кабельных линиях специализированных кварцевых волоконных световодов, функционирующих в маломодовом режиме передачи оптического сигнала, который достигается за счет совместного использования когерентных источников оптического излучения (лазеров), являющихся основой приемо-передающих модулей (трансиверов) активного оборудования мультигигабитных сетей передачи данных, и предлагаемых специализированных оптических волокон (ОВ) с увеличенным диаметром сердцевин, поддерживающих в маломодовом режиме распространение ограниченного набора модовых составляющих [4] – так называемых многомодовых оптических криповолокон (МОКВ).

Геометрия МОКВ остается традиционной и представляет собой классическую коаксиальную конструкцию в виде легированной соответствующими редкоземельными примесями кварцевой сердцевин, окруженную одной внешней сплошной оболочкой из чистого кварца. Однако при этом специализированная форма профиля показателя преломления таких ОВ обеспечивает усиленное проявление заданного характера эффекта дифференциальной модовой задержки (ДМЗ) [4], уникальное для того или иного световода. В результате такое МОКВ на всем протяжении линии является шифратором, а форма его специализированного профиля показателя преломления выполняет роль ключа [1, 2]. Таким образом, транслируемый сильно искаженный за счет ДМЗ трафик становится невозможно разобрать без соответствующего дешифратора. Роль последнего, в общем случае, может также выполнять второе криповолокно, профиль показателя преломления которого должен обеспечить «зеркальное» или «реверсивное» воспроизведение диаграммы ДМЗ МОКВ-шифратора [1, 2].

В данной работе предложена модель ВОЛП, функционирующей в маломодовом режиме с последовательно соединенной парой описанных специализированных МОКВ. Модель базируется на кусочно-регулярном представлении, при этом, в отличие от ранее разработанной и экспериментально верифицированной версии, позволяющей совместно учитывать исходный модовый состав оптического излучения на выходе когерентного источника, вводимого в ОВ-линии, условия ввода сигнала, проявление ДМЗ, хроматической дисперсии, в том числе на модах высших порядков, вариации геометрических параметров ОВ вдоль длины ВОЛП, а также наличие изгибов и механических воздействий на ОВ, неизбежно возникающих в процессе инсталляции и последующей эксплуатации ОК, дополнена возможностью учета влияния на условия ввода сигнала с выхода когерентного источника в ОВ-линии характера и степени загрязнения торцевой поверхности феррул волоконно-оптических коннекторов. Приведены ре-

зультаты апробации описанной модели на примере линейного тракта ВОЛП с последовательно соединенной парой МОКВ, функции выполняющих роли «шифратор – дешифратор». Представлены некоторые результаты сопоставления расчетных огибающих искаженных оптических импульсов, распространяющихся в описанных ВОЛП с криповолокнами сетей спецификации 10GBase-LX, в зависимости от состояния торца феррула волоконно-оптического коннектора ОВ-линии, подключаемого непосредственно к источнику излучения трансивера.

Модель кусочно-регулярной ВОЛП с многомодовыми ОВ, дополненная возможностью учета состояния торцевой поверхности феррул волоконно-оптических коннекторов разъемных соединений

Маломодовый режим передачи оптического сигнала формируется за счет возбуждения ОВ с увеличенным диаметром сердцевин когерентным источником оптического излучения – лазером (например, типовыми лазерным диодом или VCSEL (спецификации LX или SX, соответственно, серии стандартов IEEE 802.3), которые, в частности, также традиционно используются в оптических приемо-передающих модулях (трансиверах) активного оборудования мультигигабитных сетей [3–6]). Сочетание когерентного источника излучения и ОВ с увеличенным диаметром сердцевин приводит к тому, что сигнал переносится в таком световоде ограниченным числом модовых составляющих, количество которых в первую очередь определяется исходным модовым составом излучения, генерируемого лазером, условиями ввода самого сигнала в торец сердцевин ОВ и геометрией/параметрами последнего. Отличительной особенностью передачи оптического сигнала по ОВ в маломодовом режиме является непосредственно эффект ДМЗ, который проявляется в виде разделения оптического импульса на отдельные компоненты неодинаковой амплитуды и разбросом по времени поступления на приемную сторону [4]. При этом огибающая оптического импульса, традиционно имеющая квазигауссовскую форму, не сохраняется и приобретает форму «перчатки». Степень и характер проявления эффекта ДМЗ для разных сочетаний «лазер – ОВ» может проявляться по-разному. Кроме того, эффект может проявляться и для одной и той же пары «лазер – ОВ» при неконтролируемых, в общих случаях, условиях ввода.

Последнее как раз характерно непосредственно для волоконно-оптических разъемных соединений (пара коннекторов, стыкуемые в проходной розетке/адапторе), для которых характерны наличие и углового/радиального рассогласований, и воздушный зазор, обусловленных неидеальностью внутренней поверхности юстировочной втулки розетки, так и торцевой поверхности феррул кон-

некторов, в том числе и загрязнением последних. Таким образом, данный фактор также должен в обязательном порядке учитываться при моделировании указанного класса ВОЛП, поскольку во многом определяет условия ввода и не может не влиять на перераспределение мощности между возбуждаемыми в ОВ линейного тракта модами при подключении к когерентному источнику излучения. Очевидно, что в ряде случаев, определенный характер загрязнения торца феррула коннектора за счет блокирования полей возбуждаемых мод низшего порядка может привести к дополнительным искажениям оптического сигнала при передаче в маломодовом режиме.

Предлагаемое в рамках данной работы решение базируется на ранее разработанной и экспериментально верифицированной модели кусочно-регулярной ВОЛП, функционирующей в маломодовом режиме [7]. В отличие от известных подходов, данная модель, в общем случае, ориентированная на одиночные кварцевые слабораспространяющие ОВ с увеличенным, относительно стандартных одномодовых ОВ, диаметром сердцевин (нормированная частота $V \gg 1$), совместно учитывает исходный модовый состав оптического излучения на выходе когерентного источника, вводимого в ОВ-линии, условия ввода сигнала, ДМЗ, дифференциальные модовые потери, хроматическую дисперсию основной и высших направляемых мод, а также процессы взаимодействия и смещения модовых компонентов оптического сигнала, обусловленные нерегулярной структурой реальных промышленных ОВ, а также наличием микро- и макроизгибов волокон в ОК, неизбежно возникающих при инсталляции ВОЛП.

Как было отмечено выше, модель базируется на кусочно-регулярном представлении (рисунок 1) и использует общий подход метода расщепления по физическим процессам [8].

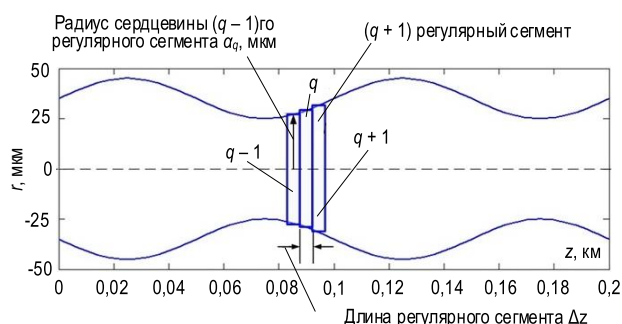


Рис. 1. Кусочно-регулярное представление участка ОВ длиной 200 м

Fig. 1. Piecewise Regular Representation of 200 m Fiber Optic Link Span

Так, в пределах регулярного сегмента заданной длины Δz геометрия световода (например, радиус сердцевин, параметры профиля показателя преломления и пр.) остаются постоянными, связь мод отсутствует, а модовые компоненты сигнала рас-

пространяются независимо друг от друга. Предполагается, что каждая направляемая мода, постоянная распространения которой, изменяясь от сегмента к сегменту, удовлетворяет условию отсечки для всех регулярных световодов, составляющих исследуемое ОВ, переносит одиночный импульс заданной формы, идентичной вводимому сигналу (например, гауссовой). Кроме того, в пределах регулярного сегмента амплитуда импульса уменьшается за счет собственных потерь моды.

Границы регулярных сегментов рассматриваются в виде соосного соединения двух подобных ОВ с разбросом технологических параметров (например, диаметром сердцевин) с некоторым заданным малым угловым рассогласованием, что позволяет непосредственно учесть наличие изгибов ОВ и остаточных механических воздействий, неизбежно возникающих на практике при инсталляции строительных длин ОК. Перераспределение мощности сигнала между амплитудами отдельных составляющих как результат взаимодействия и смещения модового состава определяется путем оценки коэффициентов связи на вышеописанных стыках по известной методике, базирующейся на хорошо известном ([9–11] и др.) методе интеграла перекрытия полей взаимодействующих мод m и n , который в скалярной постановке задачи для цилиндрической системы координат имеет следующий вид:

$$\eta_{pq} = \frac{\left| \int_0^\infty \int_0^{2\pi} F_m^{(lp)} F_m^{(lq)} r dr d\varphi \right|^2}{\int_0^\infty \int_0^{2\pi} \left| F_m^{(lp)} \right|^2 r dr d\varphi \int_0^\infty \int_0^{2\pi} \left| F_m^{(lq)} \right|^2 r dr d\varphi}, \quad (1)$$

где $F_m^{(lp)}$ и $F_m^{(lq)}$ – радиальные распределения полей взаимодействующих мод – поступающей с выхода «возбуждающего» ОВ «возбуждающей» моды $LP_{lm(p)}$ и «возбуждаемой» в «возбуждаемом» ОВ моды $LP_{lm(q)}$; l и m – азимутальный и радиальные порядки моды LP_{lm} , соответственно; r – радиальная координата, φ – полярный угол в полярной системе координат.

На приемную сторону указанные «одиночные» импульсы, переносимые соответствующими «индивидуальными» направляемыми модами LP_{lm} , приходят с определенной задержкой относительно друг друга, обусловленной разбросом значений их групповых скоростей или, иными словами, разбросом модовой задержки. В случае появления новой модовой компоненты форма переносимого данной модой сигнала представляет собой результат сложения гауссовых импульсов всех направляемых мод, которые непосредственно передали часть своей мощности указанной составляющей пропорционально соответствующему значению коэффициента связи. На приемной стороне результирующая огибающая импульса рассматривается как суперпозиция всех существующих модо-

вых компонентов сигнала, которая для частотного отклика оптического сигнала, переносимого M модовыми компонентами LP_{lm} в регулярном многомодовом ОВ длиной z , в общем случае, имеет следующий вид выражения (2), где F – прямое преобразование Фурье; $h_{\text{вх}}(t)$ – импульс на входе ОВ; $A_p^{(0)}$ и α_p – начальная амплитуда и коэффициент затухания p -й направляемой моды LP_{lm} ($p = 1, \dots, M$); $\beta_1^{(p)}$ и $\beta_2^{(p)}$ – дисперсионные параметры p -й направляемой моды LP_{lm} , которые являются элементами разложения частотной зависимости постоянной распространения $\beta(\omega)$ в ряд Тейлора – хорошо известный алгоритм записи основного уравнения распространения, подробно описанный в [8], где первый элемент этого ряда является непосредственно задержкой p -й направляемой моды LP_{lm} $\beta_1^{(p)} = \tau_3^{(p)}$, в то время как второй параметр $\beta_2^{(p)}$

позволяет учесть вклад хроматической дисперсии [4].

Таким образом, в рамках предложенного кусочно-регулярного представления многомодовой ВОЛП, частотный отклик оптического сигнала, переносимого M модовыми компонентами LP_{lm} в нерегулярном многомодовом ОВ общей протяженностью z при выбранной длине регулярного сегмента Δz , с учетом (2), может быть описан выражением (3), где $N_z = E(z/\Delta z)$; $E(x)$ – целая часть действительного числа x ; $h_{\text{вх}}(t)$ – импульс на входе многомодового ОВ; $A_q^{(p)}$, $\alpha_q^{(p)}$, $\tau_3^{(p;q)}$ и $\beta_2^{(p;q)}$ – соответственно, амплитуда, коэффициент затухания, задержка и параметр хроматической дисперсии p -й направляемой моды LP_{lm} ($p = 1, \dots, M$) на q -ом регулярном сегменте [7].

$$H_{\text{вых}}(\omega, z) = F[h_{\text{вх}}(t)] \sum_p^M A_p^{(0)} \exp(-\alpha_p z) \exp[-j(\omega - \omega_0) \beta_1^{(p)} z] \exp\left[-j \frac{1}{2} (\omega - \omega_0)^2 \beta_2^{(p)} z\right], \quad (2)$$

$$\begin{aligned} H_{\text{вых}}(\omega, z) = F[h_{\text{вх}}(t)] \sum_p^M A_{(N_z+1)}^{(p)} \exp\left[-\alpha_{(N_z+1)}^{(p)} (z - N_z \Delta z)\right] \times \\ \times \exp\left[-j(\omega - \omega_0) \tau_3^{(p;N_z+1)} (z - N_z \Delta z)\right] \exp\left[-j \frac{1}{2} (\omega - \omega_0)^2 \beta_2^{(p;N_z+1)} (z - N_z \Delta z)\right] \times \\ \times \prod_{q=1}^{N_z} A_q^{(p)} \exp(-\alpha_q^{(p)} \Delta z) \exp\left[-j(\omega - \omega_0) \tau_3^{(p;q)} \Delta z\right] \exp\left[-j \frac{1}{2} (\omega - \omega_0)^2 \beta_2^{(p;q)} \Delta z\right]. \end{aligned} \quad (3)$$

Результирующий импульсный отклик сигнала на выходе исследуемого нерегулярного многомодового ОВ $h_{\text{вх}}(t)$ определяется по общеизвестной формуле [8]:

$$h_{\text{вых}}(t) = F^{-1}(H_{\text{вых}}(\omega)) \cdot [F^{-1}(H_{\text{вх}}(\omega))]^*, \quad (4)$$

где F^{-1} – обратное преобразование Фурье; $[x]^*$ – комплексно сопряженное число.

Очевидно, что реализация представленной модели линейного тракта кусочно-регулярной ВОЛП, функционирующей в маломодовом режиме, требует многократного проведения расчета параметров передачи модовых компонентов сигнала на отдельных регулярных сегментах. Для этой цели предлагается воспользоваться разработанной ранее модификацией приближения Гаусса (ОМПГ) [7, 12], обобщенной на случай расчета параметров передачи направляемых мод произвольного порядка, распространяющихся в слабонаправляющих ОВ с произвольным осесимметричным профилем показателя преломления в области сердцевины, ограниченной одной внешней сплошной оболочкой. Данный метод базируется на совместном применении «классического» приближения Гаусса [9], заключающегося в аппроксимации радиального распределения поля моды произвольного порядка исследуемого ОВ полем моды этого

же порядка световода с идеальным неограниченным параболическим профилем показателя преломления, которое описывается известным аналитическим выражением на основе функции Лагерра – Гаусса, и метода стратификации [13], применяемого для представления профиля показателя преломления исследуемого ОВ. Предложенный подход позволяет перейти от известной интегральной [9] к аналитической форме записи вариационного выражения для квадрата волноводного параметра моды в сердцевине U^2 и характеристического уравнения для эквивалентного нормированного радиуса пятна моды $\partial U^2 / \partial R_0 = 0$, в виде конечных вложенных сумм.

Далее предлагается получить аналитические формулы для производных постоянной распространения и, как результат, записать достаточно громоздкие, но конечные аналитические выражения для модовой задержки τ_3 и коэффициента хроматической дисперсии D направляемой моды заданного порядка, которые приведены в работах [7, 12]. ОМПГ характеризуется малой погрешностью [12] и при этом позволяет выполнять анализ ОВ с профилями достаточно сложной конструкции, в том числе и восстановленных непосредственно по протоколам измерений промышленных образцов ОВ, при одновременно низких тре-

бованиях к вычислительным ресурсам даже в случае перехода к направляемым модам высших порядков.

В свою очередь, для расчета дифференциальных модовых потерь предлагается воспользоваться представленной в работе [14] известной простой эмпирической формулой, записанной для кварцевых ОВ, легированных Германием GeO_2 .

Математическое описание перераспределения мощности модовых составляющих на границах регулярных сегментов реализуется путем совместного применения ОМПГ и указанного выше метода интеграла перекрытия полей. Данный подход сводится к расчету коэффициентов связи мод, аналитические выражения для которых были выведены ранее в [15], а также приведены в [7] как для стыков с угловым рассогласованием, имитирующих в контексте данной модели микро- или макроизгибы ОВ и различные локальные и распределенные механические напряжения на ОК, так

и для строго соосных соединений и стыков с внесенным прецизионным осевым/радиальным рассогласованием.

При этом в данной работе математическое описание ввода маломодового оптического сигнала в ОВ с учетом характера и степени загрязнения торца феррула подключаемого к источнику излучения коннектора предлагается воспользоваться ранее разработанным и экспериментально верифицированным методом расчета коэффициентов связи мод [16–18], базирующимся на оригинальном представлении интеграла перекрытия полей в виде конечных вложенных сумм по компонентам радиального распределения полей этих мод (5), где $F_m^{(lm)}$ и $F_n^{(ln)}$ – радиальные распределения полей взаимодействующих мод – поступающей/вводимой «Тх»-моды LP_{lm} и возбуждаемой «Rx»-моды LP_{ln} ; l , m и n – азимутальный и радиальные порядки мод LP_{lm} и LP_{ln} , соответственно; x и y – координаты Декартовой системы координат:

$$\eta_{mn} = \frac{\left[\sum_p \sum_q F_m^{(lm)}(x_p, y_q) F_n^{(ln)}(x_p, y_q) \right]^2}{\left\{ \sum_p \sum_q \left[F_m^{(lm)}(x_p, y_q) \right]^2 \right\} \cdot \left\{ \sum_p \sum_q \left[F_n^{(ln)}(x_p, y_q) \right]^2 \right\}}, \quad (5)$$

Формально радиальные распределения полей взаимодействующих мод могут быть непосредственно корректно рассчитаны через представление, например, в базе функций Лагерра – Гаусса [9] либо с помощью строгих численных методов, где в качестве исходных данных могут использоваться протоколы измерений профиля показателя преломления промышленных образцов ОВ, выполненных с помощью штатных лабораторных комплектов анализаторов волоконных световодов. Подобное «сеточное» представление соединения ОВ позволяет вводить нулевые компоненты радиального распределения поля вводимой и/или возбуждаемой моды в загрязненных локациях сердцевин стыкуемых ОВ и, как результат, учитывать данный фактор в итоговом значении коэффициента связи. Иными словами, предлагаемый подход позволяет использовать в качестве исходных данных непосредственно фотографии торцов феррул коннекторов анализируемого разъёмного соединения, получаемые штатными полевыми комплектами видеодиагностики (например, [19] и др.). В свою очередь, согласно [16–18], используется представление анализируемого разъёмного соединения в виде эквивалентного стыка ОВ с введенным заданным прецизионным радиальным рассогласованием и дискретизацией полей взаимодействующих мод, с учетом искажения последних за счет загрязнения торца ОВ путем наложения соответствующим образом предварительно обработанного в соответствии с ранее разработанной методикой [20] изображения феррула.

Расчет динамики огибающей оптического импульса при распространении в ВОЛП с последовательно включенной парой МОКВ-шифратор/дешифратор

Для апробации предложенного подхода было проведено моделирование ВОЛП с последовательно соединенной парой МОКВ-шифратор/дешифратор для передачи сигналов волоконно-оптической системы 10GBase-LX стандарта IEEE 802.3ae. Коммерческие трансиверы таких систем данной спецификации LX традиционно реализуются на базе одномодовых лазеров с резонатором Фабри – Перо, генерирующих оптический сигнал на длине волны $\lambda = 1310$ нм. В качестве исходных данных использовались полученные в результате оптимизации градиентные профили показателя преломления указанной пары МОКВ идентичной длины, подробно описанные в [2]: здесь параметры дефекта в центре сердцевины МОКВ-дешифратора подбирались, как было отмечено выше, для обеспечения реверсивного воспроизведения диаграммы ДМЗ МОКВ-шифратора при выборе одинаковой протяженности каждого из данных ОВ. Полученные профили, представленные на рисунках 2а и 2б [2], обеспечивают ДМЗ до 2120 пс/км по основной моде LP_{01} для базовых 12 модовых составляющих (до 3-го азимутального ($l = 3$) и 3-го радиального ($m = 3$) порядков включительно), осуществляющих перенос оптического сигнала в маломодовом режиме.

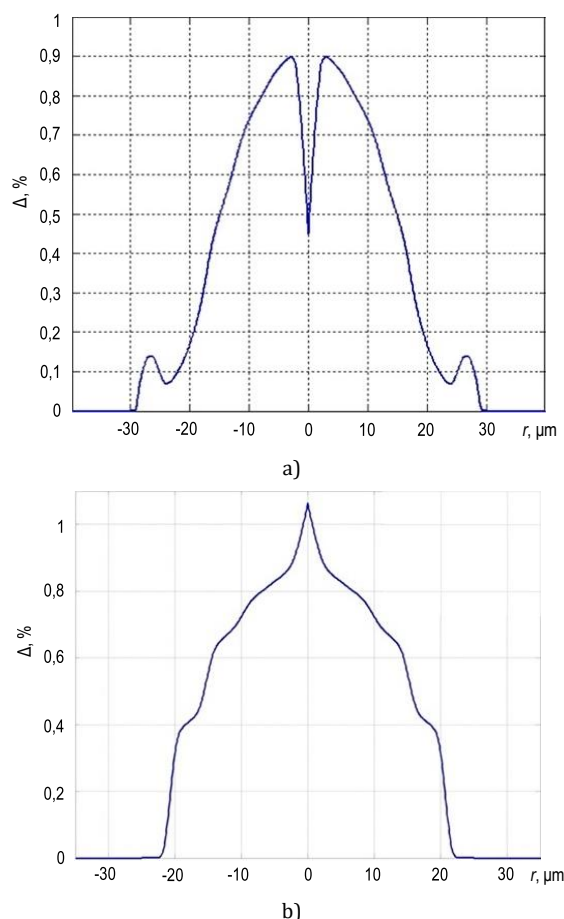


Рис. 2. Полученные в результате оптимизации образцы градиентных профилей показателя преломления МОКВ-: а) шифратора; б) дешифратора

Fig. 2. Optimized Graded Refractive Index Profiles of Optical Crypto-Fibers: a) Encryptor; b) Decoder

Как результат, рассматривалась итоговая комбинированная ВОЛП общей протяженностью 1 км,

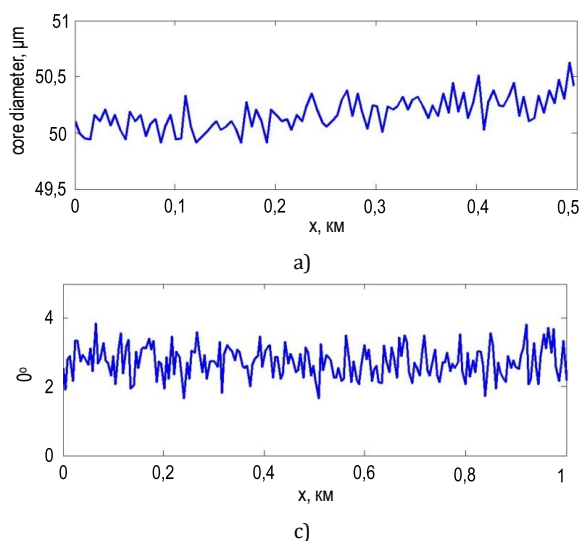


Рис. 3. Статистика распределения значений разброса: а-б) диаметра сердцевины МОКВ-шифратора; с-д) углового рассогласования стыков регулярных участков представления исследуемой ВОЛП

Fig. 3. Statistics of Variation Distribution: a-b) of Encryptor Optical Fiber Core Diameter; c-d) of Angular Misalignment at Splices of Link Regular Spans

составленная из последовательно соединенных МОКВ-шифратора и МОКВ-дешифратора длиной 500 м каждое. Здесь нерегулярная структура ОВ была представлена в виде флуктуаций диаметра сердцевины, при этом распределение значений указанного параметра задавалось на основе серии протоколов датчиков контроля внешнего диаметра ОВ, измеряемого в процессе вытяжки строительной длины световода [21, 22]. Пример статистики распределения значений разброса диаметра сердцевины МОКВ-шифратора приведен на рисунках 3а и 3б. В свою очередь, как было отмечено выше, микро- и макроизгибы ОВ, а также кручение и тяжение световода, которые неизбежно возникают на практике при установке ОК и являются дополнительными факторами взаимодействия и смещения модовых компонентов оптического сигнала, представлены в данной модели в виде стыков регулярных участков линии, выполненные с некоторым малым угловым рассогласованием. В данном случае использовался нормальный закон распределения случайной величины, при этом математическое ожидание было выбрано равным $3,0^\circ$, а дисперсии – $0,5^\circ$. Распределение значений углового рассогласования стыков регулярных участков представления исследуемого ОВ и гистограмма статистики этого распределения приведены на рисунках 3с и 3д.

Предполагается, что ввод излучения с выхода лазера в многомодовое ОВ-линии осуществляется без применения специализированных устройств согласования непосредственно через типовую проходную оптическую розетку. При этом на первом этапе полагается, что торец феррула коннектора МОКВ-шифратора не загрязнен, не поврежден, полностью удовлетворяет по прохождению тестов на чистоту всех трех зон феррула ABC [23].

Сам источник волоконно-оптической системы передачи (ВОСП) спецификации 10GBase-LX – лазерный диод (ЛД), излучение, на выходе которого может содержать до 2 поперечных мод (LP_{01} и LP_{11}) – пигментирован стандартным одномодовым ОВ рек. ITU-T G.652, торец феррула коннектора которого также является идеально чистым. В качестве альтернативы можно рассмотреть ввод излучения в торец коннектора многомодового ОВ-линии через согласующее устройство ЛД или непосредственно в передающий модуль, что также характерно для большинства штатных трансиверов активного оборудования ВОСП [24]. Таким образом, оба варианта подключения ЛД к линии рассматриваются как эквивалентное соединение одномодового ОВ и многомодового МОКВ, выполненное с угловым рассогласованием $4,2^\circ$ [7]. Результаты расчета динамики оптического импульса гауссовой формы исходной длительности $\tau_{05} = 90,91$ пс (10 Гбит/с) при распространении по описанной ВОЛП с криптоволокнами без учета влияния состояния торцевой поверхности коннектора на входе МОКВ-шифратора, подключаемого к ЛД через типовое разъемное соединение, в виде диаграммы представлены на рисунке 4.

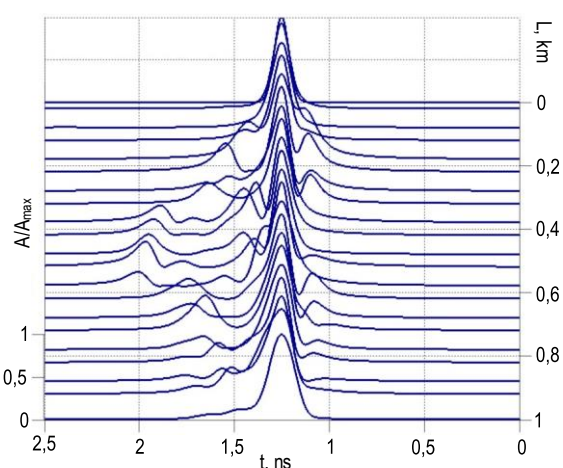


Рис. 4. Результаты расчета динамики оптического импульса системы 10GBase-LX, распространяющегося по 1 км ВОЛП, без учета влияния торцевой поверхности коннектора

Fig. 4. Results of 10GBase-LX Optical Pulse Dynamics Computation under Propagation over 1 km Fiber Optic Link without Taking into Account Connector Ferrule End-Face Condition

Анализ полученных результатов показывает, что при распространении по МОКВ-шифратору сигнал претерпевает сильные искажения за счет проявления эффекта ДМЗ, а также процессов взаимодействия и смешения модовых составляющих, в то время как на выходе МОКВ-дешифратора аналогичной протяженности с реверсивной диаграммой ДМЗ относительно МОКВ-шифратора удается практически полностью восстановить форму огибающей импульса.

На следующем этапе рассматривался более сложный ввод № 2 оптического сигнала с выхода

ЛД в МОКВ-шифратор линии: торец феррула коннектора пигтейла ЛД также выбирался как тщательным образом очищенный и прошедший тест по всем трем зонам ABC, в то время как феррул коннектора МОКВ-шифратора, напротив, был сильно загрязнен и «провалил» тесты также по всем трем зонам ABC. Здесь и далее использовались реальные фотографии торцов коннекторов [16–18, 20], полученные ранее с помощью штатного полевого комплекта видеодиагностики разъемных соединений [19]. Исходные фотографии торцов феррул указанных коннекторов представлены на рисунках 5а и 5b, соответственно. В свою очередь, результирующие бинарные изображения торцов феррул данных коннекторов после удаления ореолов границ сердцевин и оболочки и последующей локализации артефактов, выполненные в соответствии с ранее разработанной методикой [20], представлены на рисунках 5с и 5d. А в качестве примера на рисунке 6 приведено радиальное распределение полей высших мод LP_{13} LP_{23} , возбуждаемых в МОКВ-шифраторе, искаженных за счет существенного загрязнения торцевой поверхности феррула.

Результаты расчета динамики оптического импульса вышеуказанной ВОСП 10GBase-LX при существенном загрязнении торца феррула коннектора на входе МОКВ-шифратора в процессе распространения по описанной комбинированной ВОЛП с криптоволокнами представлены на рисунке 7. Здесь хорошо видно, что характер искажений огибающей оптического импульса отличается относительно предыдущих условий ввода, а результирующая огибающая сигнала на выходе ВОЛП за счет компенсации ДМЗ в МОКВ-дешифраторе также не совпадает с формой импульсного отклика, регистрируемого на выходе исследуемой ВОЛП при исходных условиях ввода.

Очевидно, что с точки зрения искажения радиального распределения поля возбуждаемых ЛД в МОКВ-шифраторе ВОЛП наибольшее негативное влияние на изменение условий ввода оказывает сильное загрязнение непосредственно в центре торца феррула – фактически в зоне, ограниченной радиусом не более 200 мкм (как показывает сопоставление рисунков 5 и 6) относительно центра сердцевин ОВ. Поэтому на следующем этапе был рассмотрен экстремально сильно загрязненный коннектор, который так же, как и в предыдущем случае не прошел тесты на чистоту всех трех зон ABC, но при этом отличается от ввода № 2 существенно бóльшим загрязнением именно в центральной зоне сердцевин. На рисунке 8 приведены (слева–направо): а) фотография торца феррула такого коннектора, б) бинарное изображение и с) пример искаженного радиального распределения поля одной из высших мод – LP_{03} .

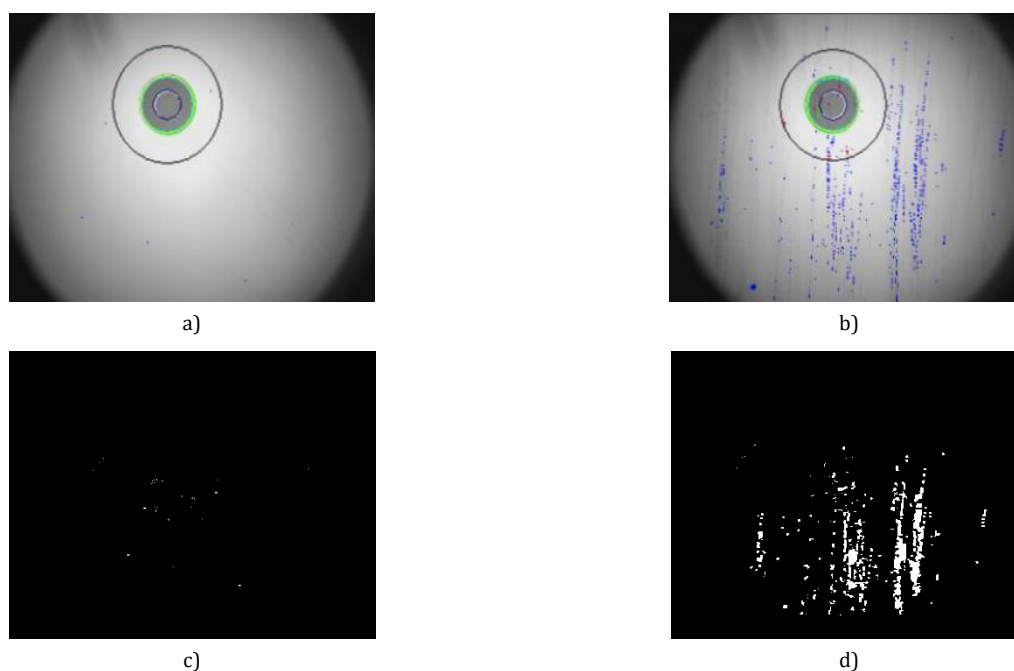


Рис. 5. Исходное и результирующее изображение: а) пигтейл ЛД; б) коннектор на вводе МОКВ-шифратора

Fig. 5. Initial and Processed Image of: a) LD Pigtail; b) Connector at the input of Encryptor Fiber

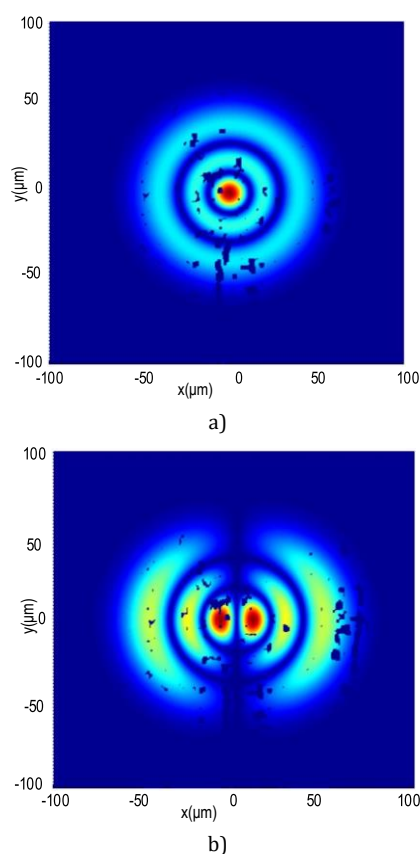


Рис. 6. Искаженные за счет загрязнения торцевой поверхности феррула поля возбуждаемых в МОКВ-шифраторе мод высших порядков: а) LP_{03} ; б) LP_{13}

Fig. 6. Radial Higher-Order Mode Field Distributions, Distorted by Contaminations over Connector Ferrule End Face: a) LP_{03} ; b) LP_{13}

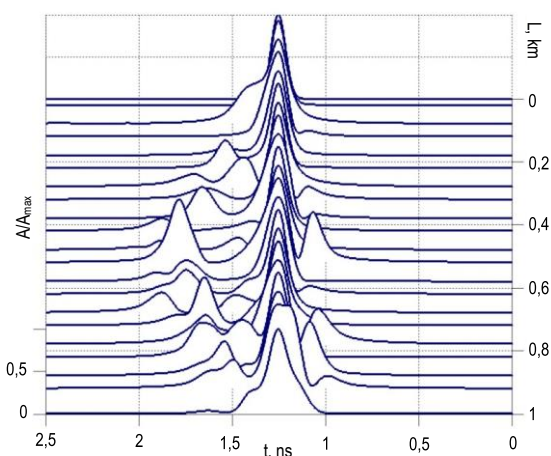


Рис. 7. Результаты расчета динамики оптического импульса системы 10GBase-LX, распространяющегося по 1 км ВОЛП, при существенном загрязнении торцевой поверхности коннектора

Fig. 7. Results of 10GBase-LX Optical Pulse Dynamics Computation during Propagation over 1 km Fiber Optic Link under Strong Contamination of Connector Ferrule End-Face

В качестве дополнения к проведению сравнительного анализа влияния характера и степени загрязнения торцевой поверхности коннектора на изменения условий ввода оптического сигнала в ОВ-линии, также предлагается рассмотреть коннектор, «проваливший» тесты в зонах «А» и «В», но прошедший тест на чистоту в зоне «С» при локальном искажении радиального распределения поле мод в периферийной зоне сердцевины ОВ (ввод № 4) (см. рисунки 8d, 8e и 8f).

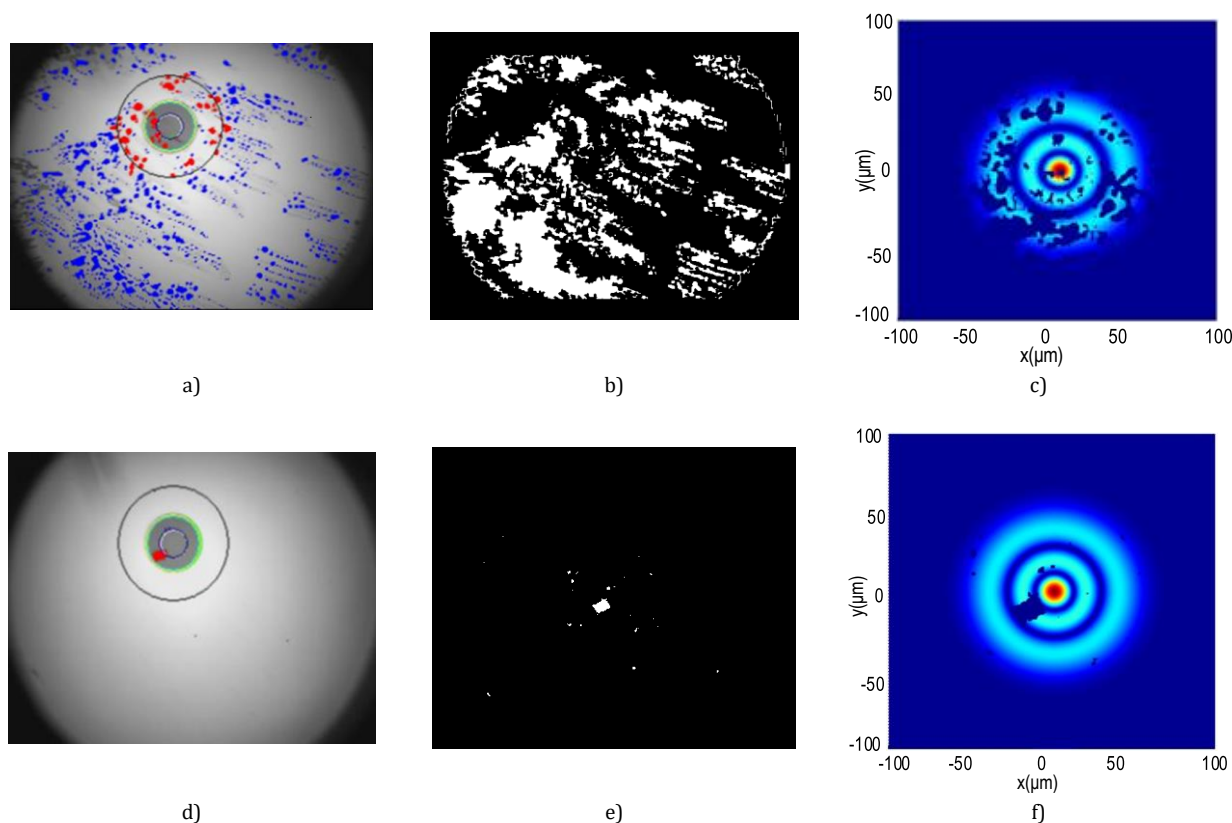


Рис. 8. Экстремально сильно (a, b и c) и умеренно загрязненная (d, e и f) торцевая поверхность феррула коннектора МОКВ-шифратора

Fig. 8. Extremely Strong (a, b and c) and Weakly Contaminated (d, e and f) Encryptor Fiber Connector Ferrule End-Face

Результаты расчета огибающей оптического импульса ВОСП 10GBase-LX на выходе исследуемой комбинированной ВОЛП общей протяженностью $L = 1,000$ км для всех вышеописанных 4 вариантов условий ввода приведены на рисунке 9. Отдельно на рисунке 10 также сведены (слева-направо) расчетные огибающие оптического сигнала в условных «контрольных точках», представляющих интерес: а) ближе к середине МОКВ-шифратора – $L = 0,220$ км; б) ближе к выходу – $L = 0,280$ км; с) ближе к середине – $L = 0,720$ км.

Анализ полученных результатов наглядно демонстрирует необходимость контроля качества подготовки (очистки) торцов феррул волоконно-оптических коннекторов разъемных соединений линейного тракта ВОЛП с многомодовыми ОВ, функционирующих в маломодовом режиме передачи сигналов мультигабитных ВОСП, трансиверы которых оснащены когерентными источниками оптического излучения. Применительно к рассматриваемому случаю исследуемой модельной комбинированной ВОЛП с криптоволокнами, хорошо видно, что для всех трех сопоставляемых вариантов ввода с загрязненными коннекторами на входе МОКВ-шифратора (причем во всех трех случаях ни один из них не прошел тест на чистоту

в зоне «А») характер и степень проявления искажения оптического импульса проявляется неодинаково и существенно отличается для случая чистого торца феррула.

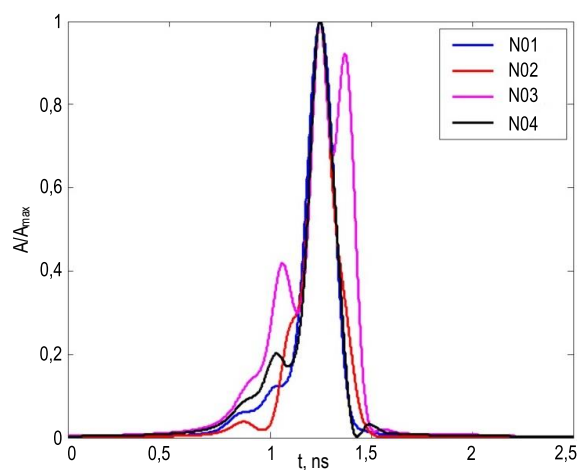


Рис. 9. Результаты расчета огибающей оптического импульса при различных условиях ввода, определяемых характером и степенью загрязнения торцевой поверхности феррула коннектора входа МОКВ-шифратора

Fig. 9. Results of 10GBase-LX Optical Pulse Envelope Computation under Various Launching Conditions, Depending on Encryptor Fiber input Connector Ferrule End-Face Contamination

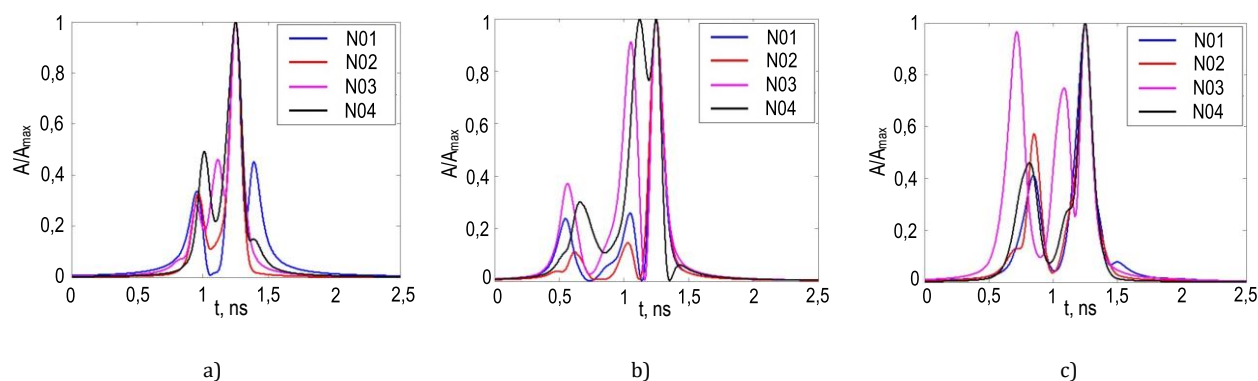


Рис. 10. Результаты расчета огибающей оптического импульса при различных условиях ввода, определяемых характером и степенью загрязнения торцевой поверхности феррула коннектора входа МОКВ-шифратор: а) 0,220 км; б) 0,480 км; в) 0,720 км

Fig. 10. Results of Optical Pulse Envelope Computation under Various Launching Conditions, Depending on Encryptor Fiber input Connector Ferrule End-Face Contamination: a) 0,220 km; b) 0,480 km; c) 0,720 km

Так, для одной и той же «контрольной точки» ВОЛП наблюдается существенно расхождение как по амплитуде (0,5 и более), так и по положению периферийных пиков импульсного отклика (1 нс и более), что объясняется неодинаковым перераспределением мощности возбуждаемых в МОКВ-шифраторе мод ввиду различного искажения их радиального распределения полей, обусловленных наличием загрязненных областей торцевой поверхности феррула для рассматриваемых вариантов подключения ЛД к многомодовой ОВ-линии.

В то же время, сопоставление полученных в результате проведенного моделирования огибающих оптического импульса непосредственно на выходе комбинированной ВОЛП показывает потенциальную возможность проведения процедур «шифрования» и «дешифрования» оптического сигнала канала передачи конфиденциальной информации путем подбора соответствующей комбинации профилей показателя преломления пары МОКВ-шифратор/дешифратор. Безусловно, экстремально сильно загрязненная торцевая поверхность феррула коннектора вблизи положения центра ОВ приводит к существенным искажениям оптического импульса, особенно при распространении в маломодовом режиме: и для ввода № 3, и для ввода № 4 загрязнение центральной зоны было настолько критично, что искаженный при распространении в МОКВ-шифратор сигнал не смог восстановить свою огибающую в МОКВ-дешифратор на приемной стороне ВОЛП при общем тренде компрессии в квазигауссову форму. При этом для ввода № 2, несмотря на также «проваленные» тесты по всем трем зонам АВС, сигнал, формально, характеризуется квазигауссовой формой с увеличением дисперсии до 75,08 пс при значении этого же параметра для ввода № 1 («чистые» коннекторы) 70,80 пс.

Заключение

Разработана модель кусочно-регулярной ВОЛП с многомодовыми ОВ, функционирующей в маломодовом режиме, дополненная, в отличие от известных решений, возможностью учета влияния на условия ввода сигнала с выхода когерентного источника в ОВ-линии состояния торцевой поверхности феррул коннекторов, и на ее основе – модель канала передачи конфиденциальной информации, защищенного на физическом уровне, реализуемого на базе ВОЛП с МОКВ.

Подтверждена необходимость контроля качества подготовки (очистки) торцов феррул коннекторов разъёмных соединений линейного тракта ВОЛП с многомодовыми ОВ, функционирующих в маломодовом режиме передачи сигналов мультигигабитных ВОСП, трансиверы которых оснащены когерентными источниками оптического излучения.

Сопоставление полученных в результате проведенного моделирования огибающих оптического импульса непосредственно на выходе комбинированной ВОЛП показывает потенциальную возможность проведения процедур шифрования и дешифрования оптического сигнала канала передачи конфиденциальной информации путем подбора соответствующей комбинации профилей показателя преломления пары МОКВ-шифратор/дешифратор.

Даже для экстремально сильно загрязненной торцевой поверхности феррула коннектора непосредственно вблизи положения центра ОВ отмечается общий тренд компрессии искаженного импульса в квазигауссову форму, несмотря на то, что он не смог восстановить исходную форму огибающей при прохождении МОКВ-дешифратора. При этом даже для достаточно существенно загрязненного ввода с формально «проваленными» тестами по всем трем зонам АВС феррула, сигнал на выходе ВОЛП, формально, характеризуется квазигауссовой формой с увеличением дисперсии до 75,08 пс при значении этого же параметра для ввода с «чистым» коннектором 70,80 пс.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа подготовлена при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90150 «Аспиранты».

Список используемых источников

1. Бурдин А.В., Губарева О.Ю., Пашин С.С., Пугин В.В. Организация защищенного канала передачи конфиденциальной информации с помощью специализированного волоконно-оптического линейного тракта // Инфокоммуникационные технологии. 2017. Т. 15. № 4. С. 337–349. DOI:10.18469/ikt.2017.15.4.04
2. Bourdine A.V., Evtushenko A.S., Gubareva O.Yu., Minaeva A.Yu., Pashin S.S., Praporshchikov D.E. Secure data transmission channel protected by special fiber optic link based on optical crypto-fibers // Proceedings of the XVth International Scientific and Technical Conference on Optical Technologies in Telecommunications (Kazan, Russian Federation, 20–23 November 2017). SPIE, 2018. Vol. 10774. DOI:10.1117/12.2318579
3. Семенов А.Б. Волоконно-оптические подсистемы современных СКК. М.: Академия Айти; ДМК Пресс, 2007. 632 с.
4. Bottacchi S. Multi-Gigabit Transmission over Multimode Optical Fibre: Theory and Design Methods for 10GbE Systems. West Sussex: John Wiley & Sons Ltd., 2006. 654 p.
5. Смирнов И.Г. Структурированные кабельные системы – проектирование, монтаж, сертификация. М.: AESP, 2007. 348 с.
6. Семенов А.Б., Стрижаков С.К., Сунчелей И.П. Структурированные кабельные системы. М.: ДМК Пресс, 2002. 640 с.
7. Bourdine A.V. Modeling and Simulation of Piecewise Regular Multimode Fiber Links Operating in a Few-Mode Regime // Advances in Optical Technologies. 2013. Vol. 2013. DOI:10.1155/2013/469389
8. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.
9. Снайдер А., Лав Дж. Теория оптических волноводов. Пер. с англ. М.: Радио и связь, 1987. 656 с.
10. Срапионов В.А. Связь мод в стыках оптических волокон с разбросом параметров // Электросвязь. 1985. № 10. С. 10–12.
11. Meunier J.P., Wang Z.H. Evaluation of Tilt or Offset Loss between Two Single-mode Graded-index Optical Waveguides // Proceedings of the International China Fibercom (Shanghai, China, 15–18 May 1994). 1994. PP. 356–362.
12. Бурдин А.В., Дельмухаметов О.Р. Расчет параметров передачи направляемых мод высших порядков на основе комбинации модифицированного приближения Гаусса и метода конечных элементов // Телекоммуникации. 2010. № 9. С. 33–40.
13. Адамс М. Введение в теорию оптических волноводов. Пер. с англ. М.: Мир, 1984. 512 с.
14. Yabre G. Comprehensive Theory of Dispersion in Graded-Index Optical Fibers // IEEE Journal of Lightwave Technology. 2000. Vol. 18. Iss. 2. PP. 166–177.
15. Bourdine A.V. Mode coupling at the splice of diverse optical fibers // Proceedings of the Optical Technologies for Telecommunications (Ufa, Russian Federation, 17–18 November 2012). SPIE, 2012. Vol. 8787. DOI:10.1117/12.2018553
16. Бурдин А.В., Пашин С.С. Оценка коэффициента отражения на разъемном соединении одномодовых оптических волокон по результатам анализа фотографий торцевых поверхностей феррул коннекторов // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 16–27. DOI:10.31854/1813-324X-2020-6-4-16-27
17. Bourdine A.V., Pashin S.S., Zaitseva E.S., Vasilets A.S., Antonov S.A. Fast and simple method for estimation of the insertion loss at the connection of singlemode optical fibers with contaminated ferrule end faces // Proceedings of the XVIIth International Scientific and Technical Conference on Optical Technologies for Telecommunications (Kazan, Russian Federation, 19–21 November 2019). SPIE, 2020. Vol. 11516. DOI:10.1117/12.2566456
18. Bourdine A.V., Bylina M.V., Pashin S.S., Praporshchikov D.E., Zaitseva E.S. Method for estimation of reflection on fiber optic connection based on ferrule end-face photo-image analysis // Proceedings of the VIIIth International Scientific and Technical Conference on Optical Technologies for Communications (Samara, Russian Federation, 17–20 November 2020). SPIE, 2021. Vol. 11793. DOI:10.1117/12.2597068
19. Westover FBP P-5000 FiberCheck2™. Руководство пользователя. Пер. с англ. 2008.
20. Bourdine A.V., Pashin S.S., Giniatulina A.M., Vasilets A.A., Antonov S.A. Development and approbation of procedure for automated localization of fiber optic connector contaminated ferrule end face image artifacts // Proceedings of the XVIth International Scientific and Technical Conference on Optical Technologies in Telecommunications (Ufa, Russian Federation, 20–22 November 2018). SPIE, 2019. Vol. 11146. DOI:10.1117/12.2527547
21. Lyytikainen K.J. Control of complex structural geometry in optical fibre drawing. D.Sc Thesis. Sydney: School of Physics and Optical Fibre Technology Centre University of Sydney, 2004. 273 p.
22. Demidov V.V., Ter-Nersesyants E.V., Bourdine A.V., Burdin V.A., Minaeva A.Yu., Matrosova A.S., et al. Methods and technique of manufacturing silica graded-index fibers with a large central defect of the refractive index profile for fiber-optic sensors based on few-mode effects // Proceedings of the XIVth International Scientific and Technical Conference on Optical Technologies in Telecommunications (Samara, Russian Federation, 22–24 November 2016). SPIE, 2017. Vol. 10342. DOI:10.1117/12.2270784
23. Standard 61300-3-35. Fibre optic interconnecting devices and passive components: Basic test and measurement procedures. Part 3-35. Examinations and measurements. Visual inspection of fibre optic connectors and fibre-stub transceivers. Iss. 1.0. 2009. 42 p.

* * *

Research of Fiber Optic Connector Ferrule End-Face Degradation Influence on Optical Pulse Distortion during Propagation over Indoor Multi-Gigabit Optical Network Links with Crypto-Fibers

A. Bourdine^{1, 2} ^{*}, S. Pashin² 

¹Research and Production Association S.I. Vavilov State Optical Institute,
St. Petersburg, 192171, Russian Federation

²Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443010, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-18-30

Received 23rd August 2021

Revised 8th October 2021

Accepted 13th October 2021

For citation: Bourdine A., Pashin S. Research of Fiber Optic Connector Ferrule End-Face Degradation Influence on Optical Pulse Distortion during Propagation over Indoor Multi-Gigabit Optical Network Link with Crypto-Fibers. *Proc. of Telecom. Universities*. 2021;7(4):18–30. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-18-30

Abstract: This article presents results of approbation of developed model of piece-wise regular fiber optic link, operating in a few-mode regime, with series-connected couple of special multimode optical crypto-fibers “encryptor-decoder”. Unlike the previously developed solution, the model was modified with an ability to take into account influence of fiber optic connector end-face contamination on laser-excited optical signal launching conditions. We present comparison results of computed optical pulse response envelops, distorted during propagation over 10GBase-LX network fiber optic links, containing optical crypto-fibers, depending on various conditions of transceiver laser source connector ferrule end-face contamination

Keywords: ferrule, fiber optic connector, ferrule end-face contamination, fiber optic connection, mode coupling coefficient, structural cable systems, differential mode delay.

FUNDING

This research was funded by RFBR according to the research project № 19-37-90150 «Post-Graduates».

References

1. Bourdine A.V., Gubareva O.Yu., Pugin V.V., Pashin S.S. Secure Data Transmission over Specialized Fiber-Optic Link. *Infokommunikacionnye tehnologii*. 2017;15(4):337–349. (in Russ.) DOI:10.18469/ikt.2017.15.4.04
2. Bourdine A.V., Evtushenko A.S., Gubareva O.Yu., Minaeva A.Yu., Pashin S.S., Praporshchikov D.E. Secure data transmission channel protected by special fiber optic link based on optical crypto-fibers. *Proceedings of the XVth International Scientific and Technical Conference on Optical Technologies in Telecommunications, 20–23 November 2017, Kazan, Russian Federation*. SPIE; 2018. vol.10774. DOI:10.1117/12.2318579
3. Semenov A.B. *Fiber-Optic Subsystems of Modern Structured Cabling Systems*. Moscow: Academy IT Publ.; DMK Press Publ.; 2007. 632 p. (in Russ.)
4. Bottacchi S. *Multi-Gigabit Transmission over Multimode Optical Fibre: Theory and Design Methods for 10GbE Systems*. West Sussex: John Wiley & Sons Ltd.; 2006. 654 p.
5. Smirnov I.G. *The Structured Cabling System – Design Work, Jointing, Certification*. Moscow: AESP Press Pub.; 2007. 348 p. (in Russ.)
6. Semenov A.B., Strizhakov S.K., Sunchelej I.R. *The Structured Cabling System*. Moscow: DMK Press Publ.; 2002. 640 p. (in Russ.)
7. Bourdine A. Modeling and Simulation of Piecewise Regular Multimode Fiber Links Operating in a Few-Mode Regime. *Advances in Optical Technologies*. 2013;2013. DOI:10.1155/2013/469389
8. Agrawal G. *Nonlinear Fiber Optics*. Moscow: Mir Publ.; 1996. 323 p. (in Russ.)

9. Snyder A., Love J. *Theory of Optical Waveguides*. Translated from English. Moscow: Radio i sviaz Publ.; 1987. 656 p. (in Russ.)
10. Srapionov V.A. Mode Coupling at Optical Fiber Junctions with Parameter Scatter. *Elektrosviaz*. 1985;10:10–12. (in Russ.)
11. Meunier J.P., Wang Z.H. Evaluation of Tilt or Offset Loss between Two Single-mode Graded-index Optical Waveguides. *Proceedings of the International China Fibercom, 15–18 May 1994, Shanghai, China*. 1994. p.356–362.
12. Bourdine A.V., Delmukhametov O.R. Calculation of the Transmission Parameters Higher-Order Guided Modes Based on Combination of the Modified Gauss Approximation and the Finite Element Method. *Telekommunikatsii (Telecommunications)*. 2010;9:33–40. (in Russ.)
13. Adams M. *Introduction to the Theory of Optical Waveguides*. Translated from English. Moscow: Mir Publ.; 1984. 512 p. (in Russ.)
14. Yabre G. Comprehensive Theory of Dispersion in Graded-Index Optical Fibers. *IEEE Journal of Lightwave Technology*. 2000;18(2):166–177.
15. Bourdine A.V. Mode coupling at the splice of diverse optical fibers. *Proceedings of the Optical Technologies for Telecommunications, 17–18 November 2012, Ufa, Russian Federation*. SPIE; 2012. vol.8787. DOI:10.1117/12.2018553
16. Bourdine A., Pashin S. Method for Estimation of Reflection on Fiber Optic Connection Based on Analysis of Images of End Surfaces of Ferrule Connectors. *Proc. of Telecom. Universities*. 2020;6(4):16–27. (in Russ.) DOI:10.31854/1813-324X-2020-6-4-16-27
17. Bourdine A.V., Pashin S.S., Zaitseva E.S., Vasilets A.S., Antonov S.A. Fast and simple method for estimation of the insertion loss at the connection of singlemode optical fibers with contaminated ferrule end faces. *Proceedings of the XVIIth International Scientific and Technical Conference on Optical Technologies for Telecommunications, 19–21 November 2019, Kazan, Russian Federation*. SPIE; 2020. vol.11516. DOI:10.1117/12.2566456
18. Bourdine A.V., Bylina M.V., Pashin S.S., Praporshchikov D.E., Zaitseva E.S. Method for estimation of reflection on fiber optic connection based on ferrule end-face photo-image analysis. *Proceedings of the VIIIth International Scientific and Technical Conference on Optical Technologies for Communications, 17–20 November 2020, Samara, Russian Federation*. SPIE; 2021. vol.11793. DOI:10.1117/12.2597068
19. Westover FBP P-5000 FiberCheck2™ User guide. Translated from English. 2008. (in Russ.)
20. Bourdine A.V., Pashin S.S., Giniatulina A.M., Vasilets A.A., Antonov S.A. Development and approbation of procedure for automated localization of fiber optic connector contaminated ferrule end face image artifacts. *Proceedings of the XVIth International Scientific and Technical Conference on Optical Technologies in Telecommunications, 20–22 November 2018, Ufa, Russian Federation*. SPIE; 2019. vol.11146. DOI:10.1117/12.2527547
21. Lyytikainen K.J. *Control of complex structural geometry in optical fibre drawing*. D.Sc Thesis. Sydney: School of Physics and Optical Fibre Technology Centre University of Sydney; 2004. 273 p.
22. Demidov V.V., Ter-Nersesyants E.V., Bourdine A.V., Burdin V.A., Minaeva A.Yu., Matrosova A.S., et al. Methods and technique of manufacturing silica graded-index fibers with a large central defect of the refractive index profile for fiber-optic sensors based on few-mode effects. *Proceedings of the XIV International Scientific and Technical Conference on Optical Technologies in Telecommunications, 22–24 November 2016, Samara, Russian Federation*. SPIE; 2017. vol.10342. DOI:10.1117/12.2270784
23. *Standard 61300-3-35. Fibre optic interconnecting devices and passive components: Basic test and measurement procedures. Part 3-35. Examinations and measurements. Visual inspection of fibre optic connectors and fibre-stub transceivers*. Iss. 1.0. 2009. 42 p.

Сведения об авторах:

БУРДИН
Антон Владимирович

доктор технических наук, доцент, заместитель генерального директора по научной работе и развитию Научно-производственного объединения «Государственный оптический институт им. С.И. Вавилова», профессор кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, bourdine@yandex.ru
 <https://orcid.org/0000-0001-8737-5486>

ПАШИН
Станислав Сергеевич

аспирант кафедры линий связи и измерений в технике связи, заместитель директора центра стратегических инициатив Поволжского государственного университета телекоммуникаций и информатики, pashinstanislav@outlook.com
 <https://orcid.org/0000-0002-7898-974X>

Имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации

А.К. Канаев^{1, 2}, Е.В. Опарин³, Е.В. Опарина²

¹ЗАО «Институт телекоммуникаций»,
Санкт-Петербург, 194100, Российская Федерация

²Петербургский государственный университет путей сообщения Императора Александра I,
Санкт-Петербург, 190031, Российская Федерация

³«Гипротрансигналсвязь» – филиал АО «Росжелдорпроект»,
Санкт-Петербург, 192007, Российская Федерация

*Адрес для переписки: ОпаринЕ@mail.ru

Информация о статье

Поступила в редакцию 29.09.2021

Поступила после рецензирования 18.11.2021

Принята к публикации 24.11.2021

Ссылка для цитирования: Канаев А.К., Опарин Е.В., Опарина Е.В. Имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 31–42. DOI:10.31854/1813-324X-2021-7-4-31-42

Аннотация: В данной статье приводится обзор взаимодействия противоборствующих сторон и основных этапов конфронтации организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации. Разработана имитационная модель, отражающая все этапы борьбы, позволяющая в зависимости от ресурсов организованного злоумышленника и системы обеспечения информационной безопасности получать вероятностно-временные характеристики результатов противоборства. Проведено моделирование при различных сценариях организации атаки на всех этапах противоборства, начиная от подавляющего преимущества организованного злоумышленника и заканчивая подавляющим преимуществом системы обеспечения информационной безопасности. Полученные результаты в общем случае могут быть использованы администраторами информационной безопасности и сетевыми администраторами для внесения корректив в стратегию организации защиты системы управления сетью тактовой сетевой синхронизации.

Ключевые слова: сеть тактовой сетевой синхронизации, телекоммуникационная система, система управления, атака, уязвимость, злоумышленник, система обеспечения информационной безопасности.

Введение

Одной из основных подсистем телекоммуникационной системы (ТКС) является сеть тактовой сетевой синхронизации (ТСС), которая выполняет функции формирования, передачи и распределения сигналов синхронизации, необходимых для поддержания работоспособного состояния всех цифровых устройств ТКС. Сеть ТСС находится в тесной взаимосвязи с другими подсистемами ТКС, оказывает существенное влияние на их работу и на функционирование всей ТКС в целом. Показатели качества услуг электросвязи неразрывно связаны с

показателями качества функционирования сети ТСС, а сигналы синхронизации и полезные информационные сигналы передаются, как правило, в одних и тех же цифровых потоках и по одним и тем же направляющим системам. Возникновение отказов на сети ТСС способно привести к значительному ухудшению качества передаваемой информации вплоть до полного отказа в предоставлении телекоммуникационных услуг [1, 2].

В силу указанных особенностей сеть ТСС является потенциально привлекательным местом проникновения в ТКС со стороны организованных

злоумышленников с целью оказать деструктивное и разрушающее воздействие. Особая опасность воздействия на сеть ТСС состоит в том, что влияние носит косвенный характер, при котором разрушение сети ТСС приводит к последующему возникновению отказов в ТКС. При возникновении подобных ситуаций могут возникать значительные затруднения по восстановлению процесса функционирования ТКС, так как зачастую невозможно достоверно определить причину возникновения отказов [1, 3].

Анализ различных потенциальных вариантов атак на сеть ТСС, таких как манипуляция синхросигналами, спуфинг в сети ТСС, атака повторного воспроизведения, атака подмены роли устройств и маршрутов в сети ТСС, перехват и удаление сообщений, показал, что наиболее опасной атакой на сеть ТСС, способной нанести максимальный ущерб при ее реализации, является атака на систему управления (СУ) ТСС. При четком соблюдении нормативных документов по построению сети ТСС, она в процессе своего функционирования является самовосстанавливающей системой. Отказ отдельного элемента сети ТСС даже высокого уровня иерархии, а также направляющих систем, систем размножения, распределения и восстановления сигналов синхронизации не приводит моментально к отказу всей сети ТСС. В то время как получение контроля злоумышленником над системой управления ТСС способно моментально привести к значительным отказам и приостановке процесса функционирования всей ТСС [3, 4].

Обзор характеристик противоборствующих сторон

Рассмотрим функционирование сети ТСС в условиях воздействия организованного злоумышленника как процесс взаимодействия сторон, имеющих кардинально противоположные цели. С одной стороны, присутствует организованный злоумышленник, стремящийся осуществить внедрение в СУ сетью ТСС и провести ряд деструктивных воздействий, снизить уровень показателей процесса функционирования сети ТСС, а с другой стороны, в составе ТКС присутствует система обеспечения информационной безопасности (СОИБ), стремящаяся предотвратить проникновение злоумышленника, локализовать его действия, обнаружить и идентифицировать его.

Система СОИБ должна выполнять ряд функций, среди которых основными являются [5–7]:

- осуществление заданной политики безопасности;
- оперативное и обоснованное управление всеми средствами информационной безопасности в соответствии с заданной политикой безопасности;

– осуществление постоянного мониторинга и аудита состояния информационной безопасности в сети ТСС.

К основным задачам системы СОИБ можно отнести:

- управление политикой безопасности, формирование локальных политик безопасности для отдельных комплексов технических средств, устройств и доведения ее до всех устройств локального управления и средств защиты;
- управление конфигурацией объектов и субъектов доступа (управление составом, версиями, компонентами сетевых элементов, устройств защиты информации и их программного обеспечения);
- обеспечение предоставления сервисов защиты распределенным прикладным системам, а также регистрацию защищенных приложений и их ресурсов;
- управление средствами криптографической защиты информации, в частности управление распределением и рассылкой ключей;
- пособытийное протоколирование;
- аудит безопасности, обеспечивающий получение и оценку объективных данных о текущем состоянии защищенности сети ТСС;
- мониторинг безопасности сети ТСС, обеспечивающий получение информации в реальном времени о состоянии сетевых элементов, активности сетевых устройств и о событиях в контексте информационной безопасности;
- поддержка регламентных мероприятий (смена паролей, устройств защиты).

Выполнение заданных функций и решение указанных задач реализуется с помощью элементов, входящих в состав подсистемы СОИБ, а именно: управления доступом; антивирусной защиты; обнаружения вторжений; обеспечения целостности; контроля (анализа) защищенности; безопасного межсетевого взаимодействия; регистрации и учета.

Организованный злоумышленник может характеризоваться различным образом. Основные характеристики организованного злоумышленника представлены на рисунке 1.

По наличию права постоянного или разового доступа в зону технологической сети СУ ТСС злоумышленники подразделяются на два класса:

- злоумышленники, не имеющие прямого доступа к оборудованию технологической сети СУ ТСС и реализующие угрозы из внешних сетей связи (внешние злоумышленники);
- злоумышленники, имеющие доступ к оборудованию технологической сети СУ ТСС и реализующие угрозы непосредственно в технологической сети СУ ТСС (внутренние злоумышленники).

На начальной стадии реализации атаки злоумышленники могут иметь различные возмож-

ности доступа к оборудованию технологической сети СУ ТСС:

- отсутствие прямого доступа (данный уровень характерен для внешних злоумышленников);
- уровень ограниченного доступа (данный уровень характерен для внутренних злоумышленников, которые являются рядовыми сотрудниками организаций по обслуживанию сети ТСС);
- уровень с полномочиями системного администратора (данный уровень характерен для внутренних злоумышленников, которые могут являться администраторами по настройке оборудования сети ТСС, данные злоумышленники могут знать топологию и структуру сети ТСС, характеристики используемого оборудования синхронизации, но в то же время обладать ограниченными сведениями по организации защиты от угроз информационной безопасности);
- уровень с полномочиями администратора безопасности (данный уровень характерен для внутренних злоумышленников, обладающих полной информацией о структуре и архитектуре системы СОИБ).

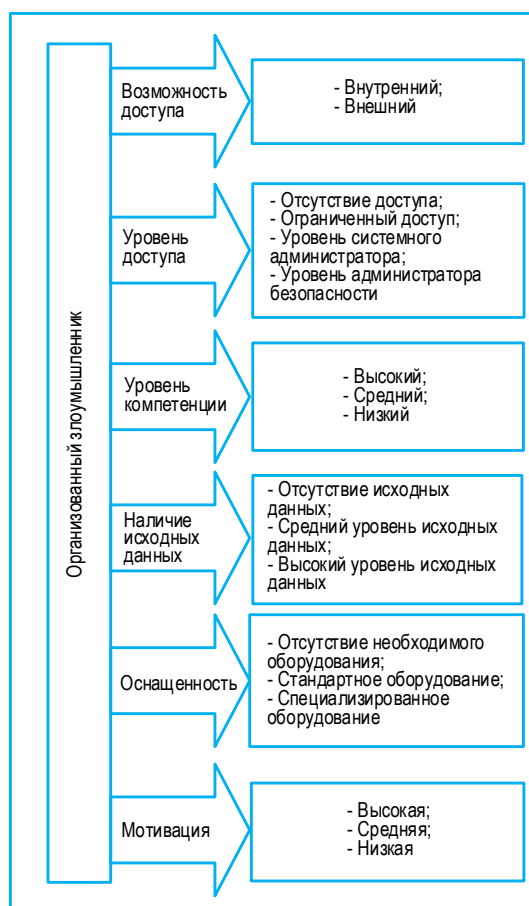


Рис. 1. Основные характеристики организованного злоумышленника

Fig. 1. Key Characteristics of an Organized Attacker

Уровень компетенции злоумышленников также может быть различным. Часть злоумышленников может обладать существенными знаниями о

предметной области функционирования сети ТСС и архитектуре информационных систем, а также иметь значительные навыки программирования. В то же время существуют злоумышленники, использующие готовые программные решения и не понимающие сути происходящих процессов.

Наличие исходных данных об объекте атаки у злоумышленника также может быть различным: от полного отсутствия сведений до наличия полного комплекта документации по процессу функционирования сети ТСС. Инструментарий у злоумышленников также может различаться: от базовых программно-аппаратных комплексов до специализированного оборудования, выполненного на заказ. Существенную роль при реализации атаки также играет мотивация злоумышленника. При более высокой мотивации следует ожидать более интенсивных атак.

Результат процесса взаимодействия организованного злоумышленника и системы СОИБ во многом определяются способностью сторон к добычанию сведений о противоположной стороне, эффективностью применения активных средств воздействия, способностью прогнозировать ситуации, принимать обоснованные и своевременные решения.

Несмотря на противоположность целей, организованного злоумышленника и систему СОИБ можно представить как субъекты, содержащие в себе механизмы выработки управленческих решений, инструменты по добычанию, обработке и передаче информации о противоположной стороне, и инструменты активного воздействия на противоположную сторону.

Процесс взаимодействия организованного злоумышленника и СОИБ

Проведенный анализ различных сценариев атак и мероприятий защиты от них позволил сформировать следующую модель процесса взаимодействия организованного злоумышленника и системы СОИБ. В основе построения данной модели лежит задание графа конфликтно обусловленных состояний, показанного на рисунке 2.

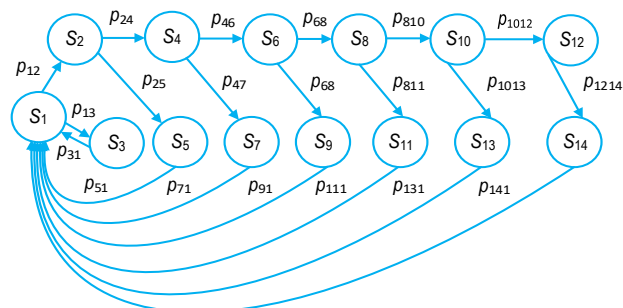


Рис. 2. Процесс взаимодействия организованного злоумышленника и системы СОИБ

Fig. 2. The Process of Interaction between an Organized Attacker and the IS Maintenance System

Как правило, злоумышленник реализует атаку в несколько этапов. Основными этапами при этом являются [1, 2, 4]:

- получение исходных данных об объекте атаки из открытых источников и методами социальной инженерии;
- поиск активных узлов и автоматизированных рабочих мест управления технологической сетью ТСС;
- определение структуры технологической сети СУ сетью ТСС;
- определение точек входа в технологическую сеть СУ сетью ТСС;
- анализ уязвимостей точек входа в технологическую сеть СУ сетью ТСС и поиск инструментария по их реализации;
- обход системы обнаружения вторжений и непосредственная реализация атаки.

Каждый из указанных этапов может быть либо реализован злоумышленником, в результате чего он перейдет к следующему, либо система СОИБ обнаружит вторжение, локализует злоумышленника и восстановит процесс функционирования сети ТСС в соответствии с нормативными значениями.

С учетом вышеизложенного модель процесса взаимодействия организованного злоумышленника и системы СОИБ будет включать следующие состояния:

S_1 – исходное состояние, которое характеризуется процессом функционирования сети ТСС в соответствии с нормативными значениями и отсутствием активных действий со стороны злоумышленника и системы СОИБ;

S_2 – злоумышленник получил необходимые ему данные о СУ сетью ТСС из открытых источников и методами социальной инженерии;

S_3 – система СОИБ локализовала злоумышленника на этапе сбора данных из открытых источников и методами социальной инженерии;

S_4 – злоумышленник осуществил поиск активных узлов и автоматизированных рабочих мест (АРМ) технологической сети СУ сетью ТСС;

S_5 – система СОИБ локализовала злоумышленника на этапе поиска активных узлов и АРМ технологической сети СУ сетью ТСС;

S_6 – злоумышленник определил структуру технологической сети СУ сетью ТСС;

S_7 – система СОИБ локализовала злоумышленника на этапе определения структуры технологической сети СУ сетью ТСС;

S_8 – злоумышленник определил точки входа в технологическую сеть СУ сетью ТСС;

S_9 – система СОИБ локализовала злоумышленника на этапе определения точек входа в технологическую сеть СУ сетью ТСС;

S_{10} – злоумышленник провел анализ уязвимостей точек входа в технологическую сеть СУ сетью ТСС и осуществил поиск инструментария по их реализации;

S_{11} – система СОИБ локализовала злоумышленника на этапе анализа уязвимостей точек входа в технологическую сеть СУ сетью ТСС;

S_{12} – злоумышленник осуществил обход системы обнаружения вторжений и реализовал атаку;

S_{13} – система СОИБ локализовала злоумышленника на этапе обхода системы обнаружения вторжений;

S_{14} – система СОИБ локализовала злоумышленника на этапе реализованной атаки.

Переход процесса взаимодействия организованного злоумышленника и системы СОИБ в состояние S_{12} будет означать победу злоумышленника, а переход в состояния $S_3, S_5, S_7, S_9, S_{11}, S_{13}$ будет означать победу системы СОИБ.

Для исследования процесса противоборства организованного злоумышленника и системы СОИБ была построена имитационная модель (рисунок 3) в среде AnyLogic [8, 9]. Исходные данные для проведения имитационного моделирования приведены в таблице 1.

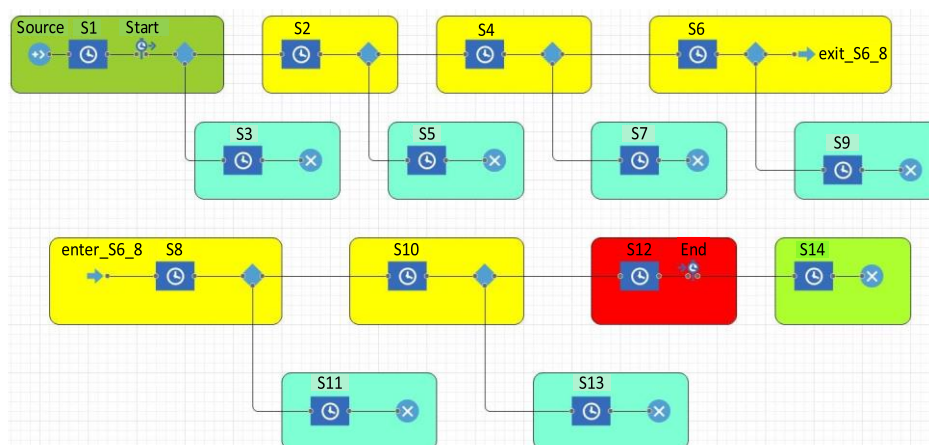


Рис. 3. Имитационная модель процесса противоборства организованного злоумышленника и системы обеспечения информационной безопасности

Fig. 3. Simulation Model of the Process of Confrontation between an Organized Attacker and an Information Security System

ТАБЛИЦА 1. Исходные данные для проведения имитационного моделирования

TABLE 1. Initial Data for Simulation

№ п/п	Название состояния	Условное обозначение		Значение	Единицы измерения
1.	Исходное состояние, которое характеризуется процессом функционирования сети ТСС в соответствии с нормативными значениями и отсутствием активных действий со стороны злоумышленника и системы СОИБ	S_1		normal(6,168)	час
2.	Состояние, когда злоумышленник получил необходимые ему данные о СУ сетью ТСС из открытых источников и методами социальной инженерии	S_2		uniform(600,840)	час
3.	Состояние, когда система СОИБ локализовала злоумышленника на этапе сбора данных из открытых источников и методами социальной инженерии	S_3		normal(0.2,1)	час
4.	Состояние, когда злоумышленник осуществил поиск активных узлов и АРМов управления технологической сетью ТСС	S_4		uniform(21,27)	час
5.	Состояние, когда система СОИБ локализовала злоумышленника на этапе поиска активных узлов и АРМов технологической сети СУ сетью ТСС	S_5		normal(0.4,2)	час
6.	Состояние, когда злоумышленник определил структуру технологической сети СУ сетью ТСС	S_6		uniform(9,15)	час
7.	Состояние, когда система СОИБ локализовала злоумышленника на этапе определения структуры технологической сети СУ сетью ТСС	S_7		normal(0.4,4)	час
8.	Состояние, когда злоумышленник определил точки входа в технологическую сеть СУ сетью ТСС	S_8		uniform(21,27)	час
9.	Состояние, когда система СОИБ локализовала злоумышленника на этапе определения точек входа в технологическую сеть СУ сетью ТСС	S_9		normal(0.4,6)	час
10.	Состояние, когда злоумышленник провел анализ уязвимостей точек входа в технологическую сеть СУ сетью ТСС и осуществил поиск инструментария по их реализации	S_{10}		uniform(36,60)	час
11.	Состояние, когда система СОИБ локализовала злоумышленника на этапе анализа уязвимостей точек входа в технологическую сеть СУ сетью ТСС	S_{11}		normal(0.4,10)	час
12.	Состояние, когда злоумышленник осуществил обход системы обнаружения вторжений и реализовал атаку	S_{12}		uniform(1,3)	час
13.	Состояние, когда система СОИБ локализовала злоумышленника на этапе обхода системы обнаружения вторжений	S_{13}		normal(0.4,12)	час
14.	Состояние, когда система СОИБ локализовала злоумышленника на этапе реализованной атаки	S_{14}		normal(1,24)	час

Исходные данные взяты, исходя из практики эксплуатации сетей ТСС и анализа проведения различных атак организованных злоумышленников, а также результатов локализации данных атак средствами СОИБ. Состояния S_2 , S_4 , S_6 , S_8 , S_{10} , S_{12} характеризуют действия организованного злоумышленника. Учитывая, что организационно-технические возможности злоумышленника зара-

нее не известны, в качестве распределения времени пребывания в данных состояниях было взято равномерное распределение. Состояния S_1 , S_3 , S_5 , S_7 , S_9 , S_{11} , S_{13} , S_{14} характеризуют действия системы СОИБ. В данных состояниях система технической эксплуатации ТСС восстанавливает и поддерживает нормативный режим функционирования ТСС, поэтому в качестве распределения времени пре-

бывания в данных состояниях было взято нормальное распределение.

Переходные вероятности из одного состояния в другое (1) указывают на характер противоборства между злоумышленником и системой СОИБ, а также на ресурсы противоборствующих сторон.

Следует отметить, что чем глубже злоумышленник преодолевает рубежи обороны СУ ТСС, тем, как правило, противодействие со стороны системы СОИБ возрастает. Результаты проведенного моделирования приведены на рисунках 4–7.

$$P = \begin{pmatrix} 0 & 0,9 & 0,1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0,7 & 0,3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0,6 & 0,4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,5 & 0,5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,3 & 0,7 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,05 & 0,95 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (1)$$

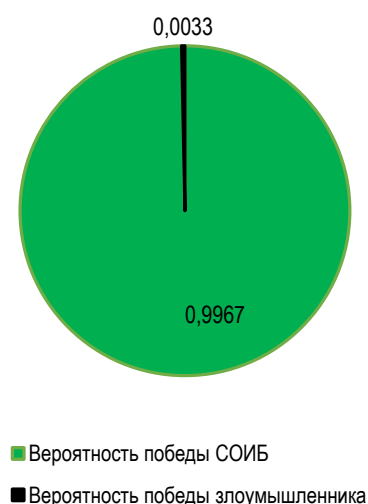


Рис. 4. Оценка вероятностей достижения цели злоумышленником и СОИБ

Fig. 4. Assessment of the Probabilities of Achieving a Goal by an Attacker and an Information Security System

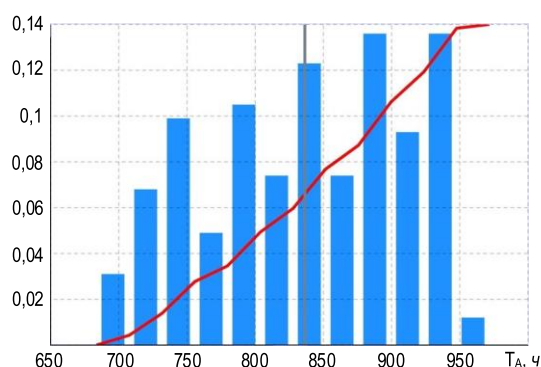


Рис. 6. Гистограмма времени реализации атаки

Fig. 6. Histogram of Attack Implementation Time

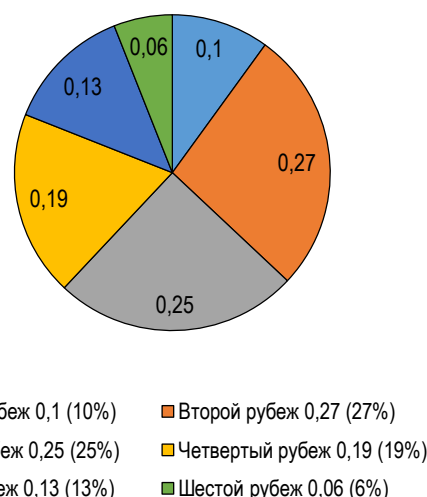


Рис. 5. Оценка отраженных атак относительно стадии их выявления

Fig. 5. Assessment of Reflected Attacks in Relation to the Stage of their Detection

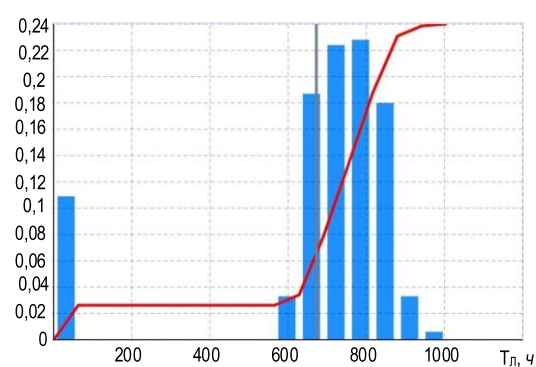
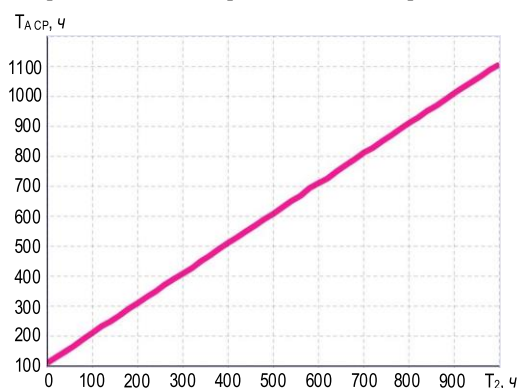


Рис. 7. Гистограмма времени локализации атаки

Fig. 7. Histogram of Attack Localization Time

Данная модель позволяет оценивать вероятностно-временные характеристики процесса противоборства между организованным злоумышленником и системой СОИБ. В статье приведена оценка среднего времени реализации атаки, среднего времени локализации деятельности злоумышленника, а также вероятностей завершения и отражения атаки. Результаты проведенного моделирования показывают, что среднее время реализации атаки T_{A_CP} на сеть ТСС составляет 836 ч, минимальное время составляет 700 ч, а максимальное – 957 ч. Среднее время локализации злоумышленника составляет 673 ч, при этом интервал локализации варьируется от 600 до 1000 ч. Также из гистограммы времени локализации атаки видно, что значительное число атак отражается на ранних стадиях.

Данная модель может служить основой для оценки степени защищенности СУ ТСС, причем как комплексно, так и для каждого отдельного рубежа защиты. Имея в наличии статистику отраженных и завершённых атак, а также нормативные значения показателей защищенности, на основе полученных результатов можно адекватно оценить средства защиты, их ресурсный потенциал, сделать вывод об их модернизации или распределения имеющихся мощностей по отдельным рубежам защиты. При оперативном определении характера атаки применяемых злоумышленником технических средств, приведенная модель может служить основой для прогнозирования результатов атаки, времени ее завершения или отражения.



Влияние отдельных состояний на длительность реализации атаки организованным злоумышленником

Злоумышленник, осуществляющий атаку на СУ сети ТСС, имеет стремление сократить длительность всей атаки и получить доступ к сети ТСС в максимально короткие сроки. Финансовые, технические и материальные ресурсы, находящиеся в распоряжении злоумышленника, могут быть различным образом распределены между состояниями для выполнения задачи получения доступа. С учетом ограниченности финансовых, технических и материальных ресурсов злоумышленник стремится выработать такую стратегию расходования ресурсов, чтобы осуществить доступ в максимально короткие сроки.

Построенная имитационная модель позволяет оценивать среднюю длительность реализации атаки организованным злоумышленником в зависимости от длительности нахождения процесса противоборства в отдельном состоянии. Отметим, что сокращение времени нахождения в конкретном состоянии, как правило, связано с более интенсивным расходованием ресурсов для данного состояния.

Таким образом, злоумышленник может распределять имеющиеся ресурсы для решения разноплановых задач по отдельным состояниям в соответствии с выбранной стратегией сокращения длительности получения доступа. Результаты моделирования приведены на рисунке 8.

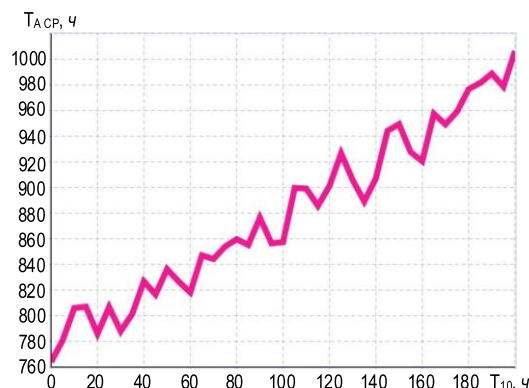


Рис. 8. Зависимость среднего времени атаки организованным злоумышленником от длительности нахождения в состояниях S_2 и S_{10}

Fig. 8. Dependence of the Average Attack Time by an Organized Attacker on the Duration of Being in States S_2 and S_{10}

По результатам моделирования видно, что в соответствии с приведенными исходными данными (см. таблицу 1) и матрицей переходных вероятностей (1), среднее время атаки организованным злоумышленником существенно зависит от времени пребывания в состоянии S_2 и меньше от пребывания в остальных состояниях. Полученный результат можно объяснить тем, что в состоянии S_2 злоумышленник осуществляет сбор исходных данных об объекте атаки и в данном состоянии он наименее подвержен обнаружению. Учитывая эти ре-

зультаты, злоумышленник может наиболее рационально использовать существенную часть ресурсов в те моменты времени, когда готовит свою атаку, т. к. сокращение времени пребывания в состоянии S_2 существенно повлияет на сокращение длительности всей атаки. Если у злоумышленника есть определенные требования к длительности цикла реализации атаки, он может выбирать соответствующую стратегию расходования ресурсов и пребывания в конкретных состояниях для получения доступа к сети ТСС.

Влияние отдельных состояний на длительность локализации организованного злоумышленника системой обеспечения информационной безопасности

В свою очередь, сетевые администраторы и администраторы безопасности имеют стремление сократить время обнаружения злоумышленника, его локализации и поддержания процесса функционирования сети ТСС. Ресурсы, находящиеся в распоряжении сетевых администраторов и администраторов безопасности, также ограничены и могут быть различным образом распределены между состояниями для выполнения общей задачи. С

учетом ограниченности финансовых, технических и материальных ресурсов в системе СОИБ, сетевые администраторы и администраторы безопасности стремятся выработать такую стратегию расходования ресурсов, чтобы сократить время обнаружения организованного злоумышленника.

Построенная имитационная модель позволяет оценивать среднее время локализации злоумышленника в зависимости от длительности нахождения в отдельном состоянии. Результаты моделирования приведены на рисунках 9–11.

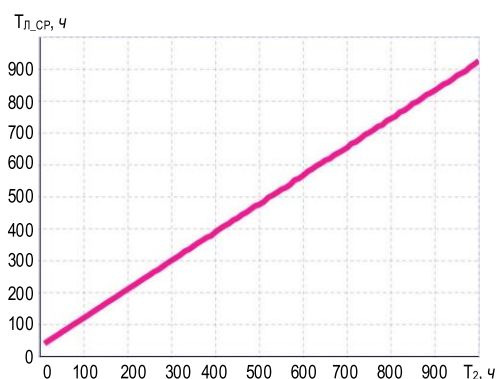


Рис. 9. Зависимость среднего времени локализации злоумышленника от длительности нахождения в состояниях S_2 и S_3

Fig. 9. Dependence of the Average Time of an Attacker's Localization on the Duration of Being in States S_2 and S_3

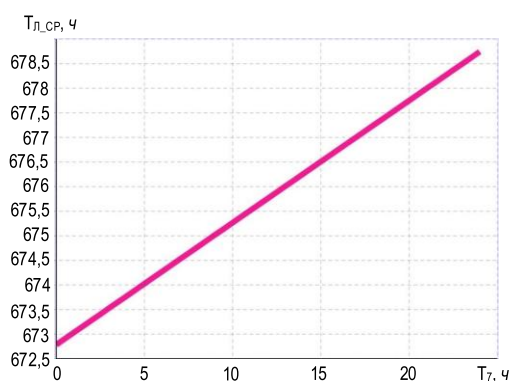
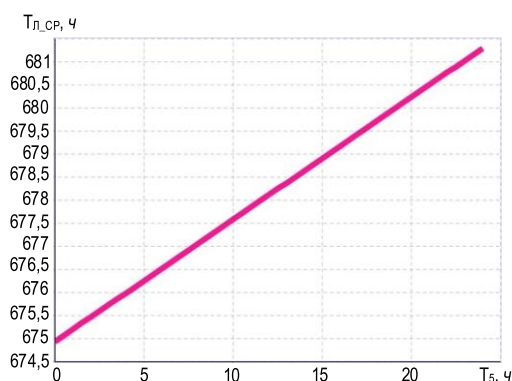


Рис. 10. Зависимость среднего времени локализации злоумышленника от длительности нахождения в состояниях S_5 и S_7

Fig. 10. Dependence of the Average Time of an Intruder's Localization on the Duration of Being in States S_5 and S_7

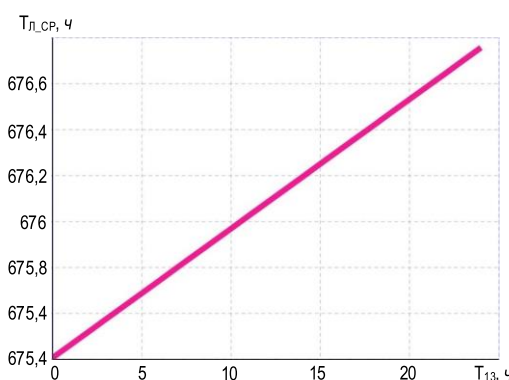
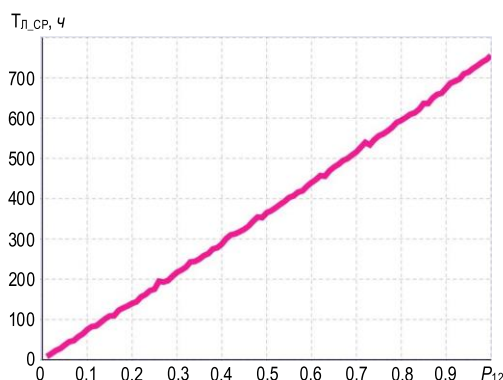


Рис. 11. Зависимость среднего времени локализации злоумышленника от длительности нахождения в состояниях S_{11} и S_{13}

Fig. 11. Dependence of the Average Time of an Attacker's Localization on the Duration of Being in States S_{11} and S_{13}

Среднее время локализации злоумышленника существенно зависит от времени пребывания в состоянии S_2 . Данный факт объясняется тем, что в указанном состоянии злоумышленник занимает активную позицию по сравнению с функционированием средств защиты и его деятельность на текущем этапе наиболее скрытна. Злоумышленник может долго выжидать, подбирая наиболее подходящий момент для атаки, что, соответственно, сказывается на общем времени его локализации. В остальных состояниях злоумышленник более активен, а значит, более заметен, и вынужден действовать быстро. В целом с возрастанием времени пребывания в состояниях, время локализации злоумышленника возрастает, но с разной интенсивностью. Отслеживая динамику данных интенсивностей, сетевые администраторы и администраторы безопасности могут оптимально распределить ресурсы по рубежам защиты, с целью наиболее оперативной локализации злоумышленника.



Длительность времени локализации злоумышленника в зависимости от соотношения сил на различных этапах противоборства

Существенную роль на длительность времени локализации злоумышленника оказывают характеристики самого злоумышленника, системы СОИБ и соотношение их ресурсов на различных этапах противоборства. Данное влияние выражается в значениях переходных вероятностей между состояниями процесса противоборства. Высокие значения ресурсов и подготовленности, как правило, характерны для повышенных значений переходных вероятностей, связанных с деятельностью злоумышленника или системы СОИБ.

Представленная имитационная модель противоборства злоумышленника и системы СОИБ позволяет отслеживать взаимосвязь между значениями переходных вероятностей и средним временем локализации злоумышленника. Примеры данных взаимосвязей приведены на рисунке 12.

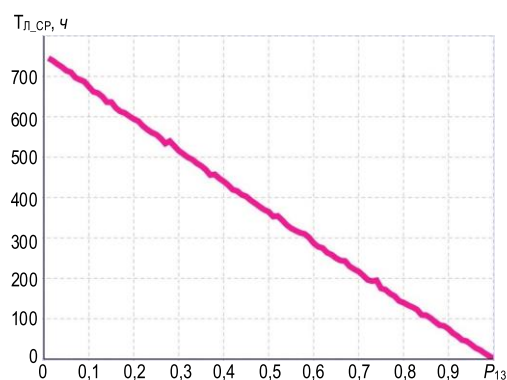


Рис. 12. Зависимость среднего времени локализации злоумышленника от вероятности переходов p_{12} и p_{13}

Fig. 12. Dependence of the Average Time of Localization of an Attacker on the Probability of Transitions p_{12} and p_{13}

Исходя из результатов приведенного моделирования, видно, что на отдельных этапах противоборства, с ростом оснащенности и ресурсов системы СОИБ среднее время его локализации уменьшается. Наоборот, в случаях, когда злоумышленник может навязать борьбу, среднее время локализации злоумышленника возрастает.

Указанные взаимосвязи и значения переходных вероятностей, исходя из требований к длительности времени локализации злоумышленника, могут служить основой для изменения технических характеристик отдельных подсистем системы СОИБ на различных рубежах защиты. Производя модернизацию отдельных подсистем системы СОИБ, возможно добиться изменения значений переходных вероятностей, а, следовательно, привести вероятность отражения атаки и длительность локализации злоумышленника к нормативным значениям.

Рассматривать среднее время атаки от значений переходных вероятностей нет особой необходимости, так как на рассмотрение попадают только реализованные атаки, при которых на каждом этапе атаки злоумышленник оказался сильнее системы СОИБ. При этом общее время атаки складывается из времен тех операций, которые осуществил злоумышленник в каждом состоянии. Данное положение подтверждается следующими графиками (рисунок 13).

Заключение

Сеть ТСС является важной подсистемой ТКС, непосредственно влияющей на качество предоставления услуг связи, в связи с чем она является потенциальным объектом атаки со стороны организованных злоумышленников. Особый класс угроз по отношению к сети ТСС представляют собой угрозы при реализации атак на СУ ТСС, способных нанести значительный вред процессу функционирования сети ТСС.

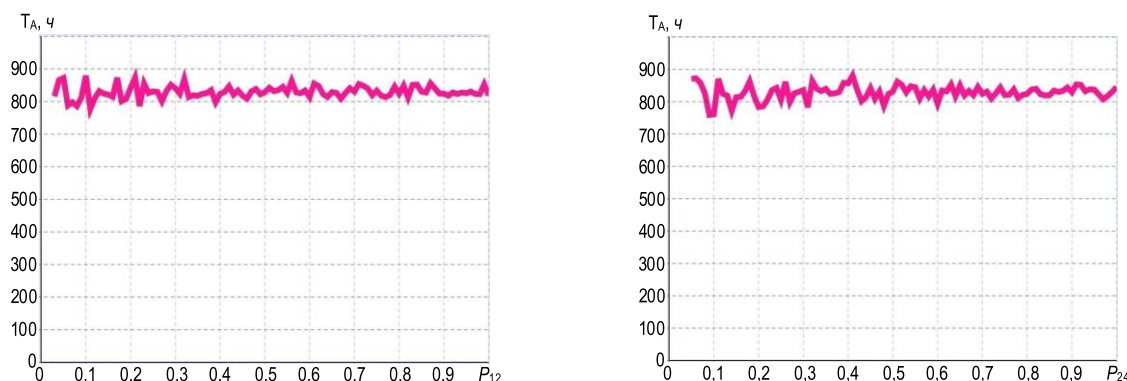


Рис. 13. Зависимость среднего времени атаки организованным злоумышленником от вероятности переходов p_{12} и p_{24}

Fig. 13. Dependence of the Average Attack Time by an Organized Attacker on the Probability of Transitions p_{12} and p_{24}

В работе получена имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атаки на систему управления сетью тактовой сетевой синхронизации. В качестве исходных данных для построения модели взяты результаты анализа отдельных средств защиты СУ сети ТСС и всей сети ТСС, статистики архива отраженных и завершенных атак, а также различных методов тестирования. Данная модель включает в себя все этапы противоборства, а также учитывает ресурсы противоборствующих сторон на различных этапах борьбы, выраженные через значения переходных вероятностей и длительности времен нахождения в состояниях.

Полученная модель позволяет производить оценку результатов противоборства на различных этапах борьбы, а также в результате всего противостояния в целом в зависимости от характеристик организованного злоумышленника и системы СОИБ. В результате проведенного моделирования получены зависимости длительностей реализации атаки и длительностей локализации злоумышленника при различных сценариях противоборства, а также характеристиках злоумышленника и системы СОИБ. Полученная имитационная модель и результаты моделирования могут быть использованы администраторами безопасности и сетевыми администраторами для внесения корректив в стратегию защиты СУ ТСС.

Вопросы моделирования угроз информационной безопасности, а также процессов взаимодействия систем СОИБ и организованных злоумышленников активно освещены как в зарубежной, например [10–11], так и в отечественной литературе [12–16]. Анализ различных литературных источников показал, что для исследования вопросов информационной безопасности, учитывая особую актуальность данных вопросов, применяются практически все методы моделирования

Тем не менее, вопросам информационной безопасности в сетях ТСС и системах передачи точного времени пока уделено недостаточно внимания. В связи с чем в данной статье и представлены результаты по формированию модели противоборства организованного злоумышленника и системы СОИБ. Аппарат имитационного моделирования выбран, учитывая особую сложность существующих и перспективных сетей ТСС, а также систем их управления при многообразии различных вариантов атак.

Представляемый математический аппарат для описания процесса взаимодействия системы СОИБ и организованных злоумышленников в сетях ТСС применен впервые. В качестве перспективной области применения можно отметить сеть ТСС железнодорожного транспорта, которая уже сейчас насчитывает тысячи элементов, а после планируемой в ближайшие годы модернизации может значительно вырасти.

Список используемых источников

1. Давыдкин П.Н., Колтунов М.Н., Рыжков А.В. Тактовая сетевая синхронизация. М.: Эко-Трендз, 2004. 205 с.
2. Канаев А.К., Опарин Е.В. Предложения по построению интеллектуальной системы поддержки принятия решений по управлению сетью тактовой сетевой синхронизации // Труды учебных заведений связи. 2017. Т. 3. № 4. С. 43–53.
3. Буренин А.Н., Курносов В.И. Теоретические основы управления современными телекоммуникационными сетями. М.: Наука, 2011. 464 с.
4. Канаев А.К., Опарин Е.В., Сахарова М.А. Полумарковская модель действий злоумышленника при атаке на систему управления сетью тактовой сетевой синхронизации // Информация и космос. 2020. № 4. С. 46–56.
5. Коцыняк М.А., Осадчий А.И., Коцыняк М.М., Лаута О.С., Дементьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2014. 126 с.

6. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2017. 434 с.
7. Ефремов М.А., Калущий И.В., Таныгин М.О., Фрундин А.Г. Обзор подходов к определению актуальных угроз информации телекоммуникационным системам и предложения по их совершенствованию // Телекоммуникации. 2017. № 5. С. 27–33.
8. Киселева М.В. Имитационное моделирование систем в среде AnyLogic. Екатеринбург: УГТУ – УПИ, 2009. 88 с.
9. Лимановская О.В., Алферьева Т.И. Моделирование производственных процессов в AnyLogic 8.1: лабораторный практикум. Екатеринбург: Издательство Уральского университета, 2019. 136 с.
10. Zedan A. El-Farra, N.H. A machine-learning approach for identification and mitigation of cyberattacks in networked process control systems // Chemical Engineering Research and Design. 2021. Vol. 176. PP. 102–115. DOI:10.1016/j.cherd.2021.09.016
11. Khazaei J. Cyberattacks with limited network information leading to transmission line overflow in cyber-physical power systems // Sustainable Energy, Grids and Networks. 2021. Vol. 27. DOI:10.1016/j.segan.2021.100505
12. Kothenko I., Saenko I., Lauta O., Karpov M. Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks // Energies. 2021. Vol. 14. Iss. 18. DOI:10.3390/en14185963
13. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. 2021. № 1. СС. 36–44. DOI:10.34832/ELSV.2021.14.1.004
14. Котенко И., Саенко И., Лаута О., Крибель А. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6(98). С. 64–71. DOI:10.22184/2070-8963.2021.98.6.64.70
15. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. СС. 66–73. DOI:10.34219/2078-8320-2021-12-4-66-73
16. Буйневич М.В., Власов Д.С. Аналитический обзор моделей инсайдеров информационных систем // Информатизация и связь. 2020. № 6. С. 92–98.

* * *

A Simulation Model of the Confrontation between an Organized Attacker and an Information Security System in the Implementation of an Attack on a Network Management System of Clock Network Synchronization

A. Kanaev^{1, 2} , E. Oparin³ , E. Oparina² 

¹Institute of Telecommunications, CJSC,
St. Petersburg, 194100, Russian Federation

²Emperor Alexander I St. Petersburg State Transport University,
St. Petersburg, 190031, Russian Federation

³Giprotranssignalsvyaz – branch of Roszheldorproekt, JSC,
St. Petersburg, 192007, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-31-42

Received 29th September 2021

Revised 18th November 2021

Accepted 24th November 2021

For citation: Kanaev A., Oparin E., Oparina E. A Simulation Model of the Confrontation between an Organized Attacker and an Information Security System in the Implementation of an Attack on a Network Management System of Clock Network Synchronization. *Proc. of Telecom. Universities*. 2021;7(4):31–42. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-31-42

Abstract: This article provides an overview of the interaction between the warring parties and the main stages of the confrontation between the organized attacker and the information security system in the implementation of an attack on the network management system of clock network synchronization. A simulation model has been developed that reflects all stages of the struggle, which allows, depending on the resources of an organized attacker

and the information security system, to obtain probabilistic and temporal characteristics of the results of the confrontation. Simulation has been carried out for various scenarios of organizing an attack at all stages of the confrontation, from the overwhelming advantage of an organized malefactor to the overwhelming advantage of an information security system. The results obtained in the general case can be used by security administrators and network administrators to make adjustments to the strategy of organizing the protection of the network management system of clock network synchronization.

Keywords: clock network synchronization network, telecommunication system, control system, attack, vulnerability, attacker, information security system.

References

1. Davydkin P.N., Koltunov M.N., Ryzhkov A.V. *Clock Network Synchronization*. Moscow: Eco-Trends Publ.; 2004. 205 p. (in Russ.)
2. Kanaev A., Oparin E. Proposals for Intellectual System Construction of Support of Decision-Making Management of Network Synchronization. *Proc. of Telecom. Universities*. 2017;3(4):43–53. (in Russ.)
3. Burenin A.N., Kurnosov V.I. *Theoretical Foundations of Modern Telecommunication Networks Management*. Moscow: Nauka Publ.; 2011. 464 p. (in Russ.)
4. Kanaev A.K., Oparin E.V., Sakharova M.A. Semi-Markov Model of an Attacker's Actions in an Attack on a Network Management System of Clock Network Synchronization. *Information and Space*. 2020;4:46–56. (in Russ.)
5. Kotsynyak M.A., Osadchiy A.I., Kotsynyak M.M., Laut O.S., Dementyev V.E., Vasyukov D.Yu. *Ensuring the Stability of Information and Telecommunication Networks in the Context of Information Confrontation*. St. Petersburg: Leningrad Branch of the Central Research Institute of Communications Publ.; 2014. 126 p. (in Russ.)
6. Biryukov A.A. *Information Security: Defense and Attack*. Moscow: DMK Press Publ.; 2017. 434 p. (in Russ.)
7. Yefremov M.A., Kalutskiy I.V., Tanygin M.O., Frundin A.G. Approach Review for Actual Threat Allocation for Telecommunication System Information and Suggestions for System Improvement. *Telecommunications*. 2017;5:27–33. (in Russ.)
8. Kiseleva M.V. *Simulation Modeling of Systems in the Anylogic Environment*. Ekaterinburg: Ural State Technical University Publ.; 2009. 88 p. (in Russ.)
9. Limanovskaya O.V., Alferieva T.I. *Modeling Production Processes in AnyLogic 8.1: Laboratory Practice*. Yekaterinburg: Ural Federal University Publ.; 2019. 136 p. (in Russ.)
10. Zedan A. El-Farra, N.H. A machine-learning approach for identification and mitigation of cyberattacks in networked process control systems. *Chemical Engineering Research and Design*. 2021;176:102–115. DOI:10.1016/j.cherd.2021.09.016
11. Khazaei J. Cyberattacks with limited network information leading to transmission line overflow in cyber-physical power systems. *Sustainable Energy, Grids and Networks*. 2021;27. DOI:10.1016/j.segan.2021.100505
12. Kothenko I., Saenko I., Laut O., Karpov M. Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks. *Energies*. 2021;14(18). (in Russ.) DOI:10.3390/en14185963
13. Saenko I.B., Laut O.S., Karpov M.A., Kribel A.M. Model of Threats to Information and Telecommunication Network Resources as a Key Asset of Critical Infrastructure. *Electrosvyaz*. 2021;1:36–44. (in Russ.) DOI:10.34832/ELSV.2021.14.1.004
14. Kothenko I., Saenko I., Laut O., Kribel A. The Method of Early Detection of Cyber Attacks Based on Integration of Fractal Analysis and Statistical Methods. *Last mile*. 2021;6(98):64–71. (in Russ.) DOI:10.22184/2070-8963.2021.98.6.64.70
15. Buinevich M.V., Pokussov V.V., Izrailov K.E. Threats Model of Information and Technical Interaction in the Integrated Information Protection System. *Informatizaciya i svyaz*. 2021;4:66–73. (in Russ.) DOI:10.34219/2078-8320-2021-12-4-66-73
16. Buinevich M.V., Vlasov D.S. Analytical Review of Models of Information Systems. *Informatizaciya i svyaz*. 2020;6: 92–98. (in Russ.)

Сведения об авторах:

КАНАЕВ
Андрей Константинович

доктор технических наук, профессор, заместитель генерального директора по спецпроектам ЗАО «Институт телекоммуникаций», профессор кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, Kanaev@itian.ru
 <https://orcid.org/0000-0002-1578-2629>

ОПАРИН
Евгений Валерьевич

кандидат технических наук, инженер I категории отдела связи «Гипротрансигналсвязь» – филиал АО «Росжелдорпроект», OnapuH@mail.ru
 <https://orcid.org/0000-0003-4622-9161>

ОПАРИНА
Екатерина Владимировна

кандидат технических наук, старший преподаватель кафедры «Механика и прочность материалов и конструкций» Петербургского государственного университета путей сообщения Императора Александра I, sirayaekaterina@mail.ru
 <https://orcid.org/0000-0003-3380-506X>

Расчет зоны покрытия DRM-передатчиков, работающих в режиме устойчивости Е

Ю.А. Ковалгин¹, С.А. Соколов²

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

²ООО «Дигитон Системс», Санкт-Петербург, 191123, Российская Федерация

*Адрес для переписки: kowalgin@sut.ru

Информация о статье

Поступила в редакцию 17.08.2021

Поступила после рецензирования 02.11.2021

Принята к публикации 08.11.2021

Ссылка для цитирования: Ковалгин Ю.А., Соколов С.А. Расчет зоны покрытия DRM-передатчиков, работающих в режиме устойчивости Е // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 43–53. DOI:10.31854/1813-324X-2021-7-4-43-53

Аннотация: Изложен метод расчета зоны покрытия DRM-передатчиков, работающих в диапазоне ОВЧ, основанный на учете первичных сведений, имеющихся в рекомендациях ITU-R P.1546-7 и ITU-R BS.1660-8. Приведены результаты вычислений и натурных измерений, подтверждающие достоверность получаемых результатов.

Ключевые слова: цифровое DRM-радиовещание, система DRM, зона покрытия передатчика.

Введение

Внедрение систем цифрового радиовещания (ЦРВ) проходит в жесткой конкурентной борьбе с аналоговой техникой [1, 2]. С внедрением систем ЦРВ в нашей стране пока не все еще до конца ясно. В настоящее время в нашей стране разрешен ввоз оборудования и проведение экспериментальных передач в диапазоне ОВЧ в трех стандартах: DAB, DRM и РАВИС. С 2019 г. в Санкт-Петербурге на частотах 95,7 и 95,9 МГц работает опытная зона аналого-цифрового радиовещания в формах DRM- и ОВЧ-ЧМ. Дальнейшее внедрение ЦРВ в данном формате тормозится не только из-за отсутствия массового производства DRM-приемников, соответствующих нормативных документов, но и методики расчета зоны покрытия цифровых передатчиков, без чего невозможно грамотное частотное планирование сетей цифрового DRM-радиовещания в диапазоне ОВЧ.

Цель статьи состоит в разработке и экспериментальной проверке метода расчета зоны покрытия DRM-передатчиков, работающих в диапазоне ОВЧ.

Основная часть

В соответствии с требованиями нормативных документов на границе зоны покрытия должна обеспечиваться минимальная напряженность поля сигнала передатчика в точке приема и требуемое стандартом минимальное отношение сигнал/шум,

необходимое для передачи аудиоконтента с заданным качеством. Эти условия на границе зоны покрытия должны выполняться одновременно.

Расчет зоны покрытия DRM-передатчика для конкретной территории (города, населенного пункта) можно разделить на следующие основные этапы (рисунок 1).

Этап 1, подготовительный

Этап выполняется при разработке технического задания. На этом этапе происходит выбор и обоснование исходных данных для расчета (шаги 1–3 на рисунке 1) таких как:

- значение несущей частоты радиоканала выбирается на основе тщательного анализа существующей электромагнитной обстановки на выбранной территории, при этом учитываются источники помех от станций, работающих в совмещенных и соседних радиоканалах, уровни атмосферных и промышленных шумов, их распределение по территории покрытия;
- число и качество передаваемых звуковых программ;
- объем, виды и качество приема сопутствующей мультисервисной информации;
- значение максимальной скорости цифровых потоков, необходимой для передачи требуемой ин-

формации с необходимым качеством, последнее зависит от вида модуляции и скорости кода цифрового потока;

- зона покрытия выбирается с учетом особенностей распределения населения по покрываемой территории, зависит также от рельефа местности и наличия искусственных препятствий для профилей трасс в разных радиальных направлениях;
- высота подвеса передающей антенны и рельеф местности определяют максимальный возможный радиус зоны покрытия в диапазоне ОВЧ;
- условия приема звуковых программ и сопутствующей информации;
- требуемая минимальная напряженность поля сигнала передатчика и отношение сигнал/шум в зоне покрытия, зависят от условий приема;
- вид модуляции поднесущих частот и скорость кода при передаче цифровых потоков определяют максимальную скорость цифровых потоков при передаче звуковых программ и мультисервисной информации (берутся из стандарта на систему ЦРВ);
- число радиальных направлений для оценки изменения напряженности поля в зоне покрытия;
- построение с использованием соответствующего программного обеспечения профилей трасс для каждого из выбранных радиальных направлений, уточнение эффективной высоты передающей антенны.

Очевидно, что радиус зоны покрытия r_0 в диапазоне ОВЧ не должен превышать расстояние оптической видимости r_1 . В [3] рекомендуется для цифровых систем вещания максимальный размер радиуса зоны покрытия передатчика выбирать из условия: $r_0 = m \cdot r_1 = (0,6...0,8) \cdot r_1$. Все же эта Рекомендация относится к системам цифрового телевидения, также работающим в диапазоне ОВЧ.

Этап 2, основной (шаги 4–7 на рисунке 1)

Этап включает собственно расчет зоны покрытия для разных условий приема и режимов работы передатчика. К числу исходных данных здесь следует отнести: значения прогнозируемой медианной напряженности поля сигнала передатчика мощностью 1 кВт с расстоянием; величины поправок и стандартных отклонений, обусловленные условиями приема и особенностями распространения радиоволн; значения требуемой минимальной медианной напряженности поля сигнала передатчика в месте приема, зависящие от характеристик приемника и передатчика, определяющие, в конечном итоге число и качество передаваемых программ и дополнительной мультимедийной информации. Остановимся подробнее на каждом из перечисленных моментов.

1) Расчет прогнозируемой медианной напряженности поля сигнала передатчика (см. шаг 4 на рисунке 1).

Первичными данными служат кривые изменения напряженности поля сигнала передатчика $E_{\text{пер}}$,

дБ(мкВ/м), с расстоянием d (км) в течение заданного времени T (%) и для заданного процента мест приема L (%) на обслуживаемой территории.

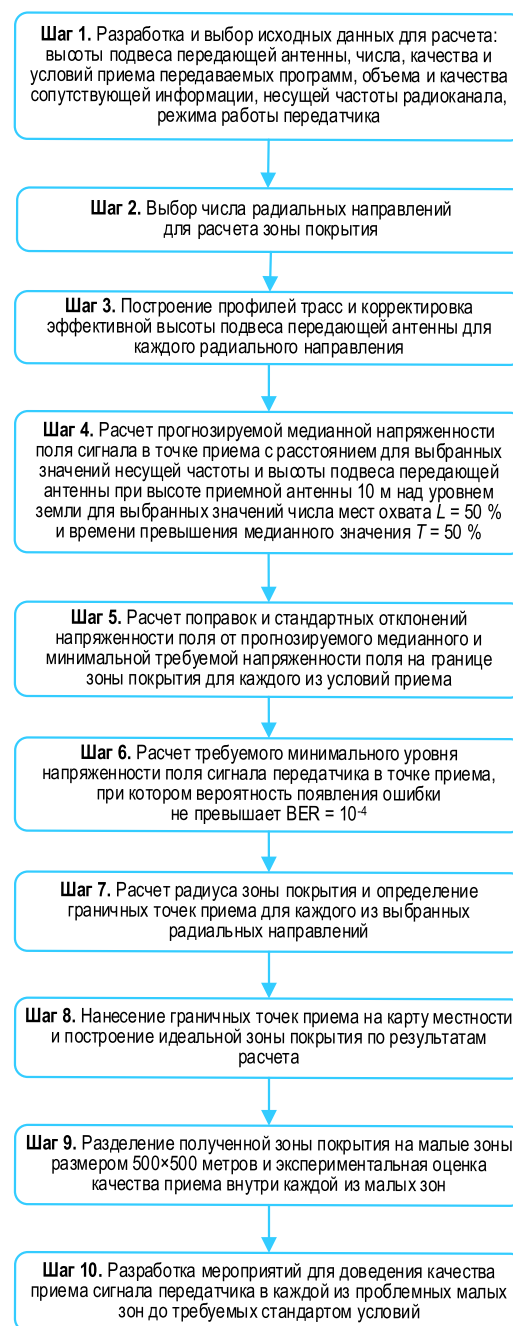


Рис. 1. Пошаговая схема расчета зоны покрытия цифрового передатчика

Fig. 1. Step-by-Step Scheme for Digital Station Coverage Calculation

Данные кривые приведены в Приложениях 2–4 Рекомендации [4]. Они представляют собой верхние пределы прогнозируемых медианных значений напряженности поля при эффективной излучаемой мощности (ЭИМ) передатчика $P_{\text{эим}} = 1$ кВт для так называемых номинальных частот 100, 200 и 600 МГц диапазона ОВЧ. Параметром каждой кривой является эффективная высота подвеса передающей антенны $h_{1\text{эфф}}$ (м). Ее значения – ряд дискретных чисел: 10; 20; 37,5; 75; 150; 300; 600 и 1200 м.

Данные кривые соответствуют значениям медианной напряженности поля, превышаемой в 50 % мест приема и в течение 50, 10 и 1 % времени, соответственно. В нашем случае необходимо выбрать кривые, для которых значения T и L составляют 50 %, как это требуют рекомендации по частотному планированию. Итак, самый первый шаг – это получение числовых данных для зависимости $E_{\text{пер}}(f, h_{1\text{эфф}}, h_2, d, T = 50 \%, L = 50 \%, P_{\text{эим}} = 1 \text{ кВт})$ на основе сведений, представленных в Рекомендации [4]. Кривые получены с учетом среднего высотного строения и средней высоты растительности. Это среднестатистические данные, требующие уточнения для каждого конкретного региона путем проведения соответствующих измерений. На начальном этапе расчета не учитываются особенности рельефа местности, распределение растительности по обслуживаемой территории, влияние возможных препятствий на пути распространения радиоволн, эффекты многолучевости. При указанных допущениях зона покрытия имеет форму круга.

Расчет прогнозируемой медианой напряженности поля для отсутствующих в рекомендации значений $h_{1\text{эфф}}$ и f при $T = 50 \%, L = 50 \%$ выполняется путем интерполяции и экстраполяции данных для имеющихся кривых по методике, приведенной в Рекомендации [4]. Эта процедура подробно описана в данной Рекомендации и не требует дополнительного пояснения.

Заметим, что потери при распространении радиоволн в свободном пространстве зависят также от диэлектрической проницаемости среды ϵ и проводимости почвы σ , значения которых являются функцией частоты f , состава и структуры почвы, температуры и особенностей климата конкретного региона. Эти значения для каждого конкретного региона дает Рекомендация [5].

Формула для расчета прогнозируемой медианной напряженности поля передатчика от расстояния, дБ(мкВ/м) , имеет вид:

$$E_{\text{пер}}(d) = E_{\text{пер}}(f, h_{1\text{эфф}}, h_2, d, T, L, P_{\text{эим}} = 1 \text{ кВт}) + 10\lg P_{\text{кВт}} + 10\lg G - 10\lg A + 10\lg D(\varphi), \quad (1)$$

где $E_{\text{пер}}(f, h_{1\text{эфф}}, h_2, d, T, L, P_{\text{эим}} = 1 \text{ кВт})$ – прогнозируемая медианная напряженность поля, дБ(мкВ/м) , создаваемая передатчиком с эффективной излучаемой мощностью $P_{\text{эим}} = 1 \text{ кВт}$ на расстоянии d (км) с несущей частотой f (МГц) при высотах подвеса передающей и приемной антенн $h_{1\text{эфф}}$ и h_2 (м), соответственно, для времени превышения медианного значения T (50%) и для числа мест в зоне покрытия L (50%); G и A – коэффициенты усиления передающей антенны и затухание в фидере (дБм); $D(\varphi)$ – характеристика направленности антенны, также по мощности (дБ); $P_{\text{кВт}}$ – мощность передатчика в кВт.

Важно, что значения прогнозируемой напряженности поля сигнала передатчика, приведенные в Рекомендации [6], относятся к медианному значению

при условии, что приемная антенна находится на высоте $h_2 = 10 \text{ м}$ над уровнем Земли.

2) Расчет поправок и стандартных отклонений, обусловленных условиями приема и особенностями распространения радиоволн (см. шаг 5 на рисунке 1).

К их числу относятся значения поправок на антропогенный (промышленный) шум, принимаемый антенной приемника $P_{\text{ММН}}$ (дБ), коэффициент местоположения C_l (дБ), потери напряженности поля при уменьшении высоты приемной антенны L_h (дБ), потери при проникновении в здания L_b (дБ). Значения этих поправок приведены в Рекомендации [6] только для трех значений эталонных частот 65, 100 и 200 МГц. Для других значений несущих частот величины этих поправок рассчитывают, используя для каждого из условий приема метод интерполяции или экстраполяции, изложенный в Рекомендациях [4] и [7].

Величины стандартных отклонений напряженности поля от медианных значений в месте приема, такие как: отклонение напряженности поля во времени σ_m (дБ), отклонения при прохождении через строения σ_b (дБ), отклонения на промышленный шум $\sigma_{\text{ММН}}$ (дБ) для системы DRM, приведены в Рекомендации [6] также только для эталонных частот 65, 100 и 200 МГц. Для других значений несущих частот эти величины по-прежнему вычисляются методом экстраполяции или интерполяции по методике, изложенной в Рекомендациях [4] и [7] отдельно для каждого из условий приема.

Расчет суммарного стандартного отклонения напряженности поля $\Delta_{\text{max}}(L, T, f)$ от минимального медианного значения для разных условий приема выполняется согласно [6, 8] по формуле:

$$\Delta_{\text{max}}(L, T, f) = \sqrt{\sigma_m^2 + \sigma_{\text{ММН}}^2 + \sigma_b^2}, \quad (2)$$

где $\sigma_m, \sigma_{\text{ММН}}, \sigma_b$ – стандартные отклонения, определяемые для каждого вида поправки из условий приема.

При расчетах считается, что эффективное напряжение радиосигнала на входе радиоприемника $U_{\text{сэфф}}$ имеет логарифмически нормальное распределение и поправочный коэффициент местоположений C_l для системы DRM вычисляется по формуле:

$$C_l = \mu \cdot \Delta_{\text{max}}(L, T, f), \quad (3)$$

где μ – коэффициент распределения для разных условий приема указан в таблице 1; $\Delta_{\text{max}}(L, T, f)$ – суммарное стандартное отклонение напряженности поля в месте приема.

В системах цифрового радиовещания поправочный коэффициент местоположений C_l имеет разное значение в зависимости от условий приема.

Суммарное значение поправок P_{Σ} для каждого из условий приема будет равно их сумме (дБ):

$$P_{\Sigma} = P_{\text{ММН}} + L_h + L_b + C_l, \quad (4)$$

ТАБЛИЦА 1. Коэффициент распределения μ для разных условий приема [6, 8]TABLE 1. Distribution Factor μ for the different Location Probabilities [6, 8]

Процент местоположений приема L , %	Условия приема	Коэффициент распределения μ
70	фиксированный прием (FX)	0,524
95	на переносные устройства (PO, PI, PO-H, PI-H)	1,645
99	на мобильные устройства (MO)	2,327

3) Расчет минимального уровня напряженности поля сигнала передатчика в точке приема (см. шаг 6 на рисунке 1).

Он определяет минимальное медианное значение напряженности поля сигнала передатчика на границе зоны покрытия, при котором вероятность появления битовой ошибки не превышает $BER = 10^{-4}$; определяется характеристиками приемника, скоростью кода цифровых потоков, а также видом модуляции поднесущих частот радиосигнала DRM-передатчика и условиями приема.

Расчет минимального уровня напряженности поля для высоты приемной антенны, равной 10 м над уровнем моря и для 50 % времени и 50 % мест охвата в зоне покрытия последовательно выполняется согласно [6, 8, 9] по приведенным формулам.

Входная мощность шума приемника $P_{ш.пр}$ (дБВт) определяется как:

$$P_{ш.пр} = F + 10\lg(k \cdot T_0 \cdot B), \quad (5)$$

где $F = 7$ дБ – коэффициент шума приемника (дБ); k – постоянная Больцмана (Дж/К), $k = 1,38 \cdot 10^{-23}$; T_0 – абсолютная температура (К); B – ширина полосы пропускания приемника (Гц), в нашем случае при $B = 100$ кГц и $T_0 = 290$ К имеем $P_{ш.пр} = -146,98$; данный параметр не зависит от характеристик передатчика, определяется только коэффициентом шума приемника и полосой частот радиоканала.

Минимальный уровень мощности полезного сигнала на входе приемника $P_{s,min}$, дБ(Вт) определяется по выражению:

$$P_{s,min} = (C/N)_{min} + P_{ш.пр}, \quad (6)$$

где $(C/N)_{min}$ – минимальное отношение сигнал/шум на входе декодера приемника (дБ), требуемое для получения битовой ошибки на выходе декодера не более чем $BER = 10^{-4}$ (зависит от вида модуляции и скорости кода, т. е. от помехозащищенности цифрового потока).

Минимальная плотность потока мощности (величина вектора Пойнтинга), в месте приема φ_{min} , дБ(Вт/м²), вычисляется в следующем виде:

$$\varphi_{min} = P_{s,min} - A_a + L_f, \quad (7)$$

где L_f – потери в фидере приемника (дБ) зависят от выбранного значения несущей частоты f , а не от вида модуляции и скорости кода; A_a – эффективная апертура антенны (дБм²), при этом:

$$A_a = 10\lg[(1,64/4\pi) \cdot (300/f)^2] + G_0, \quad (8)$$

где f – центральная (несущая) частота радиоканала (МГц); G_0 – усиление антенны относительно полуволнового вибратора (дБ); оба параметра зависят от частоты, но не зависят от вида модуляции и скорости кода.

Требуемый минимальный уровень напряженности поля сигнала передатчика в месте расположения приемной антенны E_{min} , дБ(мкВ/м):

$$E_{min} = \varphi_{min} + 10\lg Z_{\text{св}} [\text{дБ(Ом)}] + 20\lg(1\text{В}/1\text{мкВ}), \quad (9)$$

где $Z_{\text{св}} \approx 120\pi$ – волновое сопротивление в свободном пространстве (Ом); в итоге имеем:

$$E_{min} = \varphi_{min} + 145,8 [\text{дБ(Ом)}],$$

после подстановки имеем:

$$E_{min} = P_{s,min} - 10\lg[(1,64/4\pi) \cdot (300/f)^2] - G_0 + L_f + 145,8. \quad (10)$$

4) Расчет радиуса зоны покрытия DRM-передатчика (см. шаг 7 на рисунке 1).

В Рекомендации [6] требуемый минимальный медианный уровень напряженности поля сигнала передатчика для разных условий приема рассчитывается по приведенным ниже выражениям.

Для фиксированного приема, дБ(мкВ/м):

$$E_{med} = E_{min} + P_{MMN} + C_l. \quad (11)$$

Для портативного наружного и мобильного приемов (дБ(мкВ/м):

$$E_{med} = E_{min} + P_{MMN} + C_l + L_h. \quad (12)$$

Для портативного внутреннего приема:

$$E_{med} = E_{min} + P_{MMN} + C_l + L_h + L_b. \quad (13)$$

На границе зоны покрытия должны одновременно выполняться следующие условия:

$$E_{пер}(d) = E_{med} + \Delta_{max}(L, T, f), \text{ дБ(мкВ/м)}, \quad (14)$$

$$(C/N)_{гр} = (C/N)_{треб}, \text{ дБ},$$

где E_{med} – минимальное медианное значение напряженности поля сигнала передатчика, необходимое для работы приемника при величине битовой ошибки не более, чем $BER = 10^{-4}$; $\Delta_{max}(L, T, f)$ – суммарное стандартное отклонение прогнозируемой напряженности поля сигнала передатчика от минимального медианного значения для несущей частоты f при определенных значениях процентов мест приема L и времени T , в течение которого это значение превышает; $(C/N)_{гр}$ – отношение сигнал/шум на границе зоны покрытия; $(C/N)_{треб}$ – то же самое, но требуемое стандартом системы DRM.

Величина $(C/N)_{\text{гр}}$ на границе зоны покрытия, как известно, равна [4]:

$$(C/N)_{\text{гр}} = E_{\text{тр}} - (20 \lg (\sqrt{E_{\text{аш}}^2 + E_{\text{иш}}^2 + E_{\text{мс}}^2})), \quad (15)$$

где $E_{\text{аш}}$ и $E_{\text{иш}}$ – напряженности поля атмосферного и промышленного шумов, соответственно; $E_{\text{мс}}$ – напряженность поля помех мешающих станций; $E_{\text{тр}}$ – требуемая напряженность поля сигнала передатчика в месте приема, дБ(мкВ/м), при которой вероятность появления битовой ошибки не превышает 10^{-4} .

Значения промышленного шума приведены в Рекомендации [6], кроме того, они могут быть рассчитаны также в соответствии с Рекомендацией [10], этот расчет также не требует отдельного пояснения. Мощность передатчика (кВт), необходимая для получения зоны покрытия с радиусом r , определяется выражением:

$$P = 10^{B_1/10}, \quad (16)$$

где

$$B_1 = E_{\text{мед}} - E_{\text{пер}}(f, h_{1\text{эфф}}, h_2, d, T, L, P_{\text{эим}} = 1 \text{ кВт}) - 10 \lg G + 10 \lg A - 10 \lg D(\varphi) - \Delta_{\text{max}}(L, T, f), \quad (17)$$

дБ(мкВ/м)

Радиус зоны покрытия r передатчика (км) может быть найден по формуле:

$$r = d_{\text{inf}} \cdot 10^B, \quad (18)$$

где $B = [(E_{\text{пер}}(d) - E_{\text{inf}}) \cdot \lg(d_{\text{sup}}/d_{\text{inf}})] / (E_{\text{sup}} - E_{\text{inf}})$; $E_{\text{пер}}(d)$ – требуемая минимальная напряженность поля сигнала передатчика на границе зоны покрытия с учетом суммарного стандартного отклонения $\Delta_{\text{max}}(L, T, f)$ и поправок на условия приема; E_{sup} и E_{inf} – значения минимальной напряженности поля сигнала передатчика для расстояний d_{sup} и d_{inf} ; d_{sup} и d_{inf} – ближайшие большее и меньшее расстояния.

Этап 3. Коррекция результатов вычислений (шаги 8–10 на рисунке 1)

На этом этапе для каждого выбранного радиального направления строится профиль трассы, и в случае необходимости уточняется эффективная высота подвеса передающей антенны $h_{1\text{эфф}}$. Для построения профиля трассы можно, например, воспользоваться ПО Radio Mobile. При наличии прямой видимости между передающей и приемной антеннами учитывается только фактор прямой видимости. При наличии препятствий на пути распространения радиоволн радиус зоны покрытия уменьшается или появляются малые зоны отсутствия приема внутри общей зоны покрытия, что требует соответствующего увеличения мощности передатчика или, что часто выгоднее, применения дополнительных маломощных передатчиков для обслуживания выявленных *малых зон*. Эта дополнительная коррекция, если это необходимо, выполняется для каждой такой малой зоны и носит в каждом отдельном случае индивидуальный характер.

Заметим также, что в отличие от зоны покрытия, в зоне обслуживания дополнительно должна быть обеспечена возможность приема требуемого числа звуковых программ и сопутствующей им мультимедийной информации с заданным качеством. А это последнее зависит от выбранного режима работы DRM-передатчика. Вид модуляции и скорость кода DRM-передатчика определяют максимально возможную скорость цифрового потока при выбранном режиме работы DRM-передатчика (таблица 3), а это, в свою очередь, однозначно связано с возможным числом и качеством передаваемых программ и сопутствующей им дополнительной мультимедийной информации.

Оценка достоверности изложенного выше метода расчета зоны покрытия

Выполним, опираясь на вышеизложенное, расчет радиуса зоны покрытия DRM-передатчика, работающего на несущей частоте 95,7 МГц при высоте подвеса передающей антенны 278 м над уровнем Земли, затухании фидера 1,575 дБм и усилении передающей антенны 6 дБм, ибо для этого случая имеются данные натурных измерений. Мощность DRM-передатчика примем равной 640 Вт.

В таблице 2 (первые 5 строк) – это значения прогнозируемой медианной напряженности поля при эффективной излучаемой мощности передатчика 1 кВт для несущей частоты 95,7 МГц. Они получены на основе данных Рекомендации [4] для $T = 50\%$ и $L = 50\%$. В двух последних строках таблицы 2 приведены расчетные значения прогнозируемой медианной напряженности поля передатчика мощностью 640 Вт при затухании в фидере 1,575 дБм, усилении передающей антенны 6 дБм для двух значений высоты подвеса приемной антенны над уровнем Земли (10 и 1,5 м) также для $T = L = 50\%$. В Рекомендации [6] уже даны значения минимального уровня напряженности поля на входе приемника, при котором вероятность появления битовой ошибки не превышает значений, требуемых стандартом на систему DRM. Однако они имеются для каждого вида модуляции только для одного значения скорости кода. Заметим, что от вида модуляции и скорости кода зависит значение только одного параметра приемника, $(C/N)_{\text{min}}$.

Очевидно, что для другого значения скорости кода при выбранном виде модуляции это значение может быть найдено как:

$$E_{\text{мед}2} = E_{\text{мед}1} - (\text{SNR}_1 - \text{SNR}_2), \quad (19)$$

где $E_{\text{мед}1}$ – минимальная медианная напряженность поля для выбранного вида модуляции и скорости кода при требуемом стандартом отношении сигнал/шум равном SNR_1 ; $E_{\text{мед}2}$ – то же самое, но для другого значения скорости кода и требуемого стандартом отношении сигнал/шум равном SNR_2 для того же вида модуляции.

ТАБЛИЦА 2. Прогнозируемая медианная напряженность поля сигнала передатчика, дБ(мкВ/м), превышаемая в течение 50 % времени и для 50 % мест приема в зоне покрытия

TABLE 2. Predictable Median Field-Strength Level, dB(μ V/m), Exceeded for 50 % of Time and for 50 % of Locations

Несущая частота, МГц / Эффективная высота передающей антенны, м	Расстояние до передатчика, км								
	1	5	10	20	30	40	50	60	70
Эффективная излучаемая мощность передатчика 1 кВт, высота подвеса приемной антенны 10 м над уровнем Земли									
100 / 300	103	87	79	69,5	62	55	50	45	40,5
100 / 150	100	82,5	74,5	62,5	54	48	42,5	38,5	35
95,7 / 300	102,98	86,98	78,98	69,48	61,98	55	49,98	44,98	40,48
95,7 / 150	99,98	81,98	74,48	62,48	53,98	48	42,48	38,48	34,98
95,7 / 278	102,65	86,43	78,49	68,7	61,1	54,2	49,16	44,27	39,88
Мощность передатчика 640 Вт, затухание в фидере 1,575 дБм, усиление антенны 6 дБм, высота подвеса приемной антенны 10 м над уровнем Земли									
95,7 / 278	105,14	90,92	80,97	71,2	63,6	57	51,64	46,75	42,36
высота подвеса приемной антенны 1,5 м над уровнем Земли									
95,7 / 278	95,34	81,12	71,17	61,4	53,8	47,2	41,8	37	32,56

Минимальные значения отношения сигнал/шум, обеспечивающие получение вероятности появления битовой ошибки, не превышающей 10^{-4} , как это и требуется стандартом, приведены в таблице 3. Они получены экспериментальным путем и позволяют, используя приведенное выше выражение (19) и сведения из Рекомендации [6] (см. таблицы 39–44), найти минимальное значение напряженности поля сигнала передатчика в месте приема для других значений скорости кода, не представленных в данной Рекомендации. И затем, зная для каждого из условий приема значения поправок, по формулам 11–13, рассчитать требуемое минимальное медианное значение напряженности поля сигнала передатчика на границе зоны покрытия. Результаты этих вычислений сведены в таблице 4.

Данные таблицы 4 – это по сути дела полные исходные данные для расчета радиуса зоны покрытия цифрового DRM-передатчика. При этом расчет требуемой мощности передатчика для обеспечения заданного радиуса зоны покрытия может быть выполнен по формулам 16, 17. И наоборот, если же требуется рассчитать радиус зоны покрытия при известных значениях мощности передатчика, потерях в фидере, усилении и характеристики направленности передающей антенны, то он выполняется по формулам 1, 2, 14, 18.

Основные результаты вычислений, необходимые для оценки соответствия результатов расчетов данных измерений, приведены ниже. На рисунке 2 даны результаты вычислений прогнозируемой напряженности поля передатчика с расстоянием: кривая E – медианное значение напряженности поля сиг-

нала передатчика с эффективной излучаемой мощностью 1 кВт при высоте подвеса передающей антенны 278 м для условия стационарного приема (FX, $L = 50 \%$, $T = 50 \%$) при высоте приемной антенны 10 м; кривая E1 – то же самое, но для передатчика мощностью 640 Вт при усилении передающей антенны 6 дБм и потерях в фидере 1,575 дБм (ненаправленное излучение); кривая E3 – для мобильного приема (MO) при $L_h = 9,796$ дБ (таблица 4).

ТАБЛИЦА 3. Значения требуемого SNR для разных режимов модуляции и кодирования в канале MSC в условиях стационарного приема на штыревую антенну в помещении на расстоянии 12 км от телебашни в Санкт-Петербурге, несущая частота DRM-передатчика 95,7 МГц [11]

TABLE 3. Required SNR for Different Modulation and Coding Modes in the MSC Channel, Fixed Reception on a Whip Antenna Indoors at a Distance 12 km from the TV Tower in St. Petersburg, the Carrier Frequency of the DRM Transmitter is 95,7 MHz [11]

Модуляция	Скорость		Требуемое значение SNR, дБ
	Кода	Цифрового потока в канале MSC, кбит/с	
4-QAM	0,250 (PL0)	37,3	2,27
4-QAM	0,333 (PL1)	49,7	2,71
4-QAM	0,400 (PL2)	59,6	2,93
4-QAM	0,500 (PL3)	74,5	4,09
16-QAM	0,330 (PL0)	99,4	7,64
16-QAM	0,411 (PL1)	122,4	9,22
16-QAM	0,500 (PL2)	149,1	10,24
16-QAM	0,625 (PL3)	186,4	11,40

ТАБЛИЦА 4. Требуемый минимальный медианный уровень напряженности поля сигнала передатчика для разных условий приема, видов модуляции поднесущих частот и скоростей кода для несущей частоты 95,7 МГц при вероятности появления битовой ошибки на выходе приемника не более $BER = 10^{-4}$ (система DRM)

TABLE 4. Minimum Median Field-Strength Level for the Different Receiving Scenarios, Modes and Code Rates, the Carrier Frequency of the DRM Transmitter is 95,7 MHz, Average Coded Bit Error Ratio $BER = 10^{-4}$ (bit) (DRM System)

№ п/п	Значения исходных данных		Условия приема					
			FX	PI	PI-H	PO	PO-H	MO
1.	Потери в фидере	L_c , дБ	1,37	0,00	0,00	0,00	0,00	0,274
2.	Усиление приемной антенны	G_0 , дБ	0,00	-2,20	-19,4	-2,20	-19,4	-2,20
3.	Эффективный раскрыв антенны	A_a , дБм ²	1,081	-1,12	-18,319	-1,12	-18,319	-1,12
4.	Минимальный уровень напряженности поля сигнала передатчика на принимающей антенне при модуляции QAM-4 для скорости кода:	E_{min} , дБ(мкВ/м)						
	0,25		2,97	9,799	26,999	9,799	26,999	8,273
	0,33		3,41	10,239	27,439	10,239	27,439	8,713
	0,40		3,63	10,459	27,659	10,459	27,659	8,933
	0,50		4,79	11,619	28,819	11,619	28,819	10,093
5.	Минимальный уровень напряженности поля сигнала передатчика на принимающей антенне при модуляции QAM-16 для скорости кода:	E_{min} , дБ(мкВ/м)						
	0,333		7,409	15,79	32,939	15,79	32,939	13,413
	0,411		8,989	17,37	34,519	17,37	34,519	14,993
	0,50		10,009	18,39	35,539	18,39	35,539	16,013
	0,625		11,169	19,55	36,699	19,55	36,699	17,2977
6.	Поправка на промышленный шум	P_{MMN} , дБ	10,935	10,935	0,00	10,935	0,00	10,935
7.	Потери при уменьшении высоты антенны	L_h , дБ	0,00	9,796	16,796	9,796	16,796	9,796
8.	Потери при прохождении через строения	L_b , дБ	0,00	8,898	8,898	0,00	0,00	0,00
9.	Поправочный коэффициент местоположений	C_l , дБ	3,092	10,887	7,928	9,703	6,209	12,738
10.	Суммарное значение поправок	P_Σ , дБ	14,027	40,516	33,622	30,434	23,005	33,469
11.	Вероятность охвата мест	%	70	95	95	95	95	99
12.	Коэффициент распределения	μ	0,52	1,64	1,64	1,64	1,64	2,33
13.	Стандартное отклонение напряженности поля DRM	σ_m , дБ	3,776	3,776	3,776	3,776	3,776	3,776
14.	Стандартное отклонение MMN	σ_{MMN} , дБ	4,53	4,53	0,00	4,53	0,00	4,53
15.	Стандартные отклонения при потерях при прохождении через строения	σ_b , дБ	0,00	3,00	3,00	0,00	0,00	0,00
16.	Суммарное стандартное отклонение напряженности поля	$\Delta_{max}(L, T, f)$, дБ	5,897	6,617	4,82	5,897	3,776	5,897
17.	Минимальный медианный уровень напряженности поля сигнала передатчика в месте приема для модуляции QAM-4 при скорости кода:	E_{min} , дБ(мкВ/м)						
	0,25		16,997	50,315	60,621	40,23	50,004	41,742
	0,33		17,437	50,755	61,061	40,673	50,444	42,182
	0,40		17,657	50,975	61,281	40,893	50,664	42,402
	0,5		18,817	52,135	62,441	42,953	51,824	43,562
18.	Минимальный медианный уровень напряженности поля сигнала передатчика в месте приема для модуляции QAM-16 при скорости кода:	E_{min} , дБ(мкВ/м)						
	0,333		21,436	56,306	66,561	46,224	55,944	46,882
	0,411		23,016	57,886	68,141	47,804	57,524	48,462
	0,500		24,036	58,906	69,161	48,824	58,544	49,482
	0,625		25,196	60,066	70,321	49,984	59,704	50,759

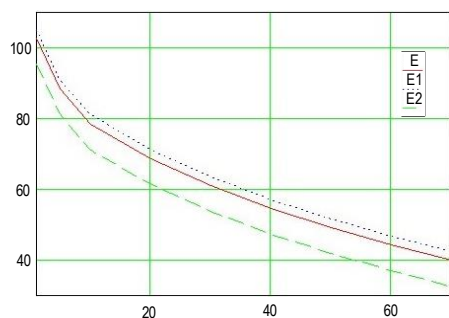


Рис. 2. Кривые изменения прогнозируемой напряженности поля сигнала передатчика с расстоянием

Fig. 2. Curves of the Predicted Field-Strength Level for the Different Distance

На рисунке 3 также демонстрируются полученные расчетным путем зависимости требуемой мощности передатчика от величины радиуса зоны покрытия для мобильного приема (несущая частота – 95,7 МГц, высота подвеса передающей антенны – 278 м) при модуляции QAM-4, скорости кода $R = 0,25$, где верхняя кривая с учетом суммарных стандартных отклонений – $[\Delta_{\max}(L, T, f) = 5,897$ дБ], нижняя кривая без учета суммарных стандартных отклонений – $[\Delta_{\max}(L, T, f) = 0$ дБ].

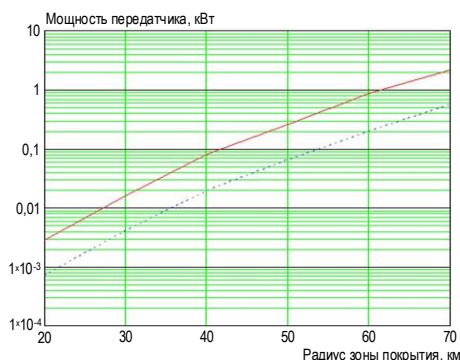


Рис. 3. Кривые требуемой мощности передатчика от величины радиуса зоны покрытия при модуляции QAM-4

Fig. 3. Curves of the Required Transmitter Power for the Different Coverage Radius for 4-QAM Modulation

На рисунке 4 – то же самое, но для модуляции QAM-16 при скорости кода $R = 0,625$ как с учетом, так и без учета возможных суммарных стандартных отклонений. Мощность передатчика здесь отложена в логарифмическом масштабе, а радиус зоны покрытия – в линейном масштабе.

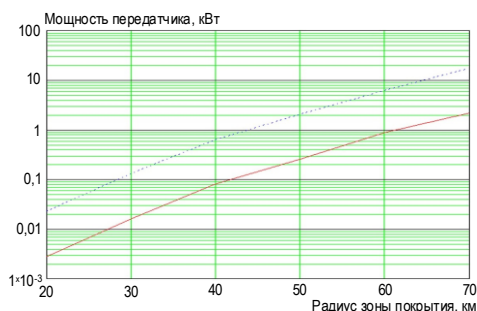
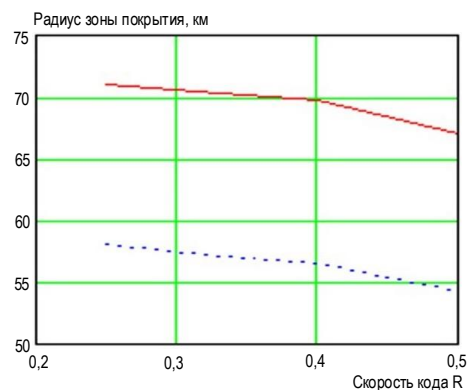


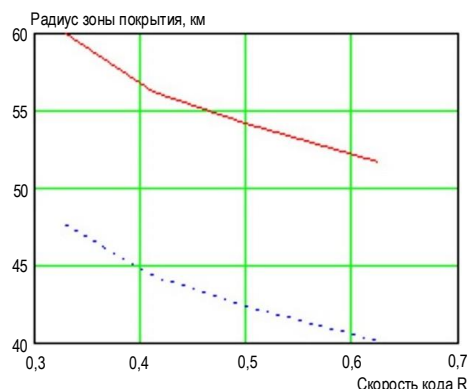
Рис. 4. Кривые требуемой мощности передатчика от величины радиуса зоны покрытия при модуляции QAM-16

Fig. 4. Curves of the Required Transmitter Power for the Different Coverage Radius for 16-QAM Modulation

На рисунке 5 приведены зависимости радиуса зоны покрытия от скорости кода при модуляциях QAM-4 (см. рисунок 5a) и QAM-16 (см. рисунок 5b) (передатчика мощностью 640 Вт) для мобильного приема с учетом суммарных стандартных отклонений (нижняя кривая – $\Delta_{\max}(L, T, f) = 5,895$ дБ) и без их учета (верхняя кривая – $\Delta_{\max}(L, T, f) = 0$ дБ). Масштаб линейный по обеим осям.



a)



b)

Рис. 5. Зависимость радиуса зоны покрытия DRM-передатчика мощностью 640 Вт от скорости кода цифрового потока в канале MSC: а) для модуляции QAM-4; б) для модуляции QAM-16

Fig. 5. 640 W DRM Transmitter Coverage Radius for the different Code Rate in the MSC Channel: a) 4-QAM Modulation; b) 16-QAM Modulation

Натурные измерения для передатчика мощностью 640 Вт при высоте подвеса передающей антенны над уровнем Земли 278 м, усилении антенны 6 дБм, потерях в фидере 1,575 дБм были проведены в условиях мобильного приема. Для измерений в опытной зоне цифрового DRM-радиовещания использовался профессиональный контрольно-измерительный приемник Rfmondial Model RF-SE19 с питанием от бортовой сети автомобиля и четвертьволновой калиброванной антенной типа Kathrein K 51 16 4/510 351 с антенным фактором $K = 7,69$ дБ(1/м). Ослабление сигнала в кабеле, соединяющем антенну и высокочастотный вход приемника, было измерено анализатором ZVL Network Analyzer компании «Rohde & Schwarz» и составило 0,49 дБ на частоте 96 МГц. Несущая частота передатчика составляла 95,7 МГц.

Сравнение прогнозируемых (теоретических) значений и результатов измерений для мобильного приема (мощность DRM-передатчика 640 Вт, усиление антенны 6 дБм, потери в фидере 1,575 дБм, высота подвеса передающей антенны 278 м) представлено в таблице 5 [12–14].

ТАБЛИЦА 5. Сравнение прогнозируемых (рассчитанных) данных и результатов измерений

TABLE 5. Comparison of Predicted (Calculated) and Measurement Results

Вид модуляции, скорость кода	Радиус зоны покрытия, км		
	Результаты расчета без учета / с учетом отклонений*		Результаты измерений (по данным [12–14]) по направлениям
QAM-4, $R = 0,25$	71,3	58	67 – западное 64 – северное
QAM-16, $R = 0,625$	52	40	49 – северное 57 – юго-западное 54 – юго-восточное 64 – восточное

* суммарные стандартные напряженности поля в месте приема

Примечание: расчет выполнен с использованием данных Рекомендаций МСЭ-R P.1546-7 [4], [6] и [7]

Анализ полученных результатов позволяет сделать следующее заключение.

Во-первых, при модуляции QAM-4 и скорости кода $R = 0,25$ максимальный размер радиуса зоны покрытия ограничивается в нашем случае значением оптической видимости. Именно по этой причине для передатчика мощностью 640 Вт при $r_1 = 278$ м и $r_2 = 45$ м (средний подъем рельефа для профиля трассы при удалении от телебашни) максимальное значение радиуса зоны покрытия не должно превышать значение 65...67 км, что хорошо согласуется с данными измерений.

Во-вторых, результаты натурных измерений показали [11], что при мобильном приеме минимальное медианное значение напряженности поля передатчика на границе зоны покрытия составляет около 30 дБ(мкВ/м) при модуляции QAM-4 и $R = 0,25$ (наилучшая помехозащищенность) и около 40 дБ(мкВ/м) при модуляции QAM-16 и $R = 0,625$ (наихудшая помехозащищенность). Эти данные учитывают потери напряженности поля сигнала передатчика с уменьшением высоты подвеса приемной антенны, в нашем случае они составляют для диапазона ОВЧ II (87,5...108 МГц) при мобильном приеме 9,796 дБ (таблица 4). Заметим, что значения требуемой минимальной медианной напряженности поля сигнала передатчика (см. таблицу 4) для разных условий приема учитывают этот факт, а именно, они приведены к условию расположения приемной антенны на высоте 10 м над уровнем Земли, т. к. кривые распространения радиоволн, представленные в [4], получены именно для этого условия.

В-третьих, кроме того, в [6] при расчете требуемой минимальной медианной напряженности поля сигнала передатчика учтены потери на аппаратную реализацию неидеального приемника, они приняты

равными 3 дБ. Контрольно-измерительный приемник Rfmondial Model RF-SE19 по своим характеристикам приближается к идеальному случаю: он имеет предельно достижимые сегодня параметры. Именно по этой причине при сравнении расчетных и экспериментальных данных можно эти потери не учитывать, что приведет при измерениях к несколько большему значению радиуса зоны покрытия. Напомним также, что кривые распространения радиоволн, использованные при проведении вышеизложенных расчетов (Рекомендация [4]), представляют собой среднестатистические данные. Они получены для условий умеренного климата, характерного для Европы и Северной Америки. Кривые для морских трасс были построены на основе данных, полученных главным образом в регионах Северного и Средиземного моря. По этой причине реальные прогнозируемые значения медианной напряженности поля для конкретного региона могут иметь отличия от значений, приведенных в данной Рекомендации. В нашем случае для региона Санкт-Петербурга результаты теоретического расчета, выполненные с их использованием, дают погрешность (см. таблицу 5), не превышающую 10 %, что вполне достаточно для практических целей. Все же для уточнения возможной ошибки в оценке радиуса зоны покрытия полезно предварительно провести измерения реальной напряженности поля сигнала передатчика с расстоянием, сравнить полученные значения с данными Рекомендации [4], что позволит уточнить реальный размер зоны покрытия. Кривые, приведенные в данной Рекомендации, оцифрованы, что удобно для их практического применения.

В-четвертых, для условия мобильного приема при использовании DRM-передатчика мощностью 640 Вт при высоте подвеса передающей антенны 278 м, усилении антенны 6 дБм и потерях в фидере 1,575 дБм:

- при модуляции QAM-4 и скорости кода $R = 0,25$ радиус зоны покрытия с учетом суммарного стандартного отклонения напряженности поля передатчика оставляет около 58 км, что меньше радиуса оптической видимости;

- при модуляции QAM-16 и скорости кода $R = 0,625$ радиус зоны покрытия составляет около 40 км с учетом потерь на аппаратную реализацию и суммарное стандартное отклонение, а без учета этих двух факторов он равен 58 км и также остается меньше радиуса оптической видимости;

- переход от модуляции QAM-4 к модуляции QAM-16 уменьшает радиус зоны покрытия передатчика при мобильном приеме на 10...12 км.

В-пятых, для уточнения возможной ошибки в оценке радиуса зоны покрытия DRM-передатчика для других регионов полезно предварительно провести измерения реальной напряженности поля передатчика с расстоянием, сравнить полученные значения с данными Рекомендации [4], что позволит уточнить реальный размер зоны покрытия.

При этом сам изложенный здесь метод расчета радиуса зоны покрытия не требует изменений.

В-шестых, полученные данные позволяют утверждать, что наиболее предпочтительным является применение модуляции QAM-4 и скорости кода 0,25. В этом случае при равенстве зон покрытия будет иметь место наибольший энергетический выигрыш цифрового DRM-радиовещания по сравнению

с ЧМ-радиовещанием. Однако при этом возможна передача только одной программы с качеством не хуже, чем при ЧМ-радиовещании, но при существенно меньшей полосе частот радиоканала, что несомненно является неоспоримым преимуществом системы DRM. Увеличение числа передаваемых программ требует повышения мощности передатчика при сохранении прежнего размера зоны покрытия, что с энергетической точки зрения не всегда является оправданным.

Список используемых источников

1. Ковалгин Ю.А. Цифровое радиовещание: системы и технологии. М.: Горячая линия – Телеком, 2021. 580 с.
2. Соколов С.А., Мышьянов С.В., Ковалгин Ю.А. Исследование аналого-цифровой DRM/ЧМ-зоны радиовещания в полосе частот 87,5–108 МГц // Электросвязь. 2021. № 4. С. 30–36. DOI:10.34832/ELSV.2021.17.4.003
3. Носов В.И., Сартаков К.И. Оптимизация параметров сети цифрового ТВ-вещания на основе коэффициента использования потенциала передающих станций // Вестник СибГУТИ. 2016. № 2. С. 41–50.
4. Рекомендация МСЭ R P.1546-7 (08/2019) Метод прогнозирования для трасс связи "пункта с зоной" для наземных служб в диапазоне частот от 30 МГц до 3000 МГц.
5. Рекомендация МСЭ R P.527-6 (09/2021) Электрические характеристики земной поверхности.
6. Рекомендация МСЭ R BS.1660-8 (06/2019) Техническая основа для планирования наземного цифрового звукового радиовещания в полосе ОВЧ.
7. Рекомендация МСЭ R P.528-3 (02/2012) Кривые распространения радиоволн для воздушной подвижной и радионавигационной служб, работающих в диапазонах ОВЧ, УВЧ и СВЧ.
8. Planning Parameters for DRM Mode E ('DRM+') concerning the use in VHF bands I, II and III. V 3.0 – 04/05/2011.
9. Методика частотного планирования радиоэлектронных средств цифрового телевизионного вещания стандарта DVB-H. Разработана федеральным государственным унитарным предприятием «Научно-исследовательский институт радио». Утверждена решением ГКРЧ от 10 марта 2011 г. (протокол № 11-11-4).
10. Rec. ITU-R P.372-14 (08/2019) Radio nouse.
11. Ковалгин Ю.А., Соколов С.А., Мышьянов С.В., Свинына О.А., Кукушкинов А.Е., Сабанова А.И., и др. Разработка рекомендаций по внедрению в Российской Федерации цифрового стандарта радиовещания DRM+: отчет о НИР. СПб.: СПбГУТ, 2015. 169 с.
12. Ковалгин Ю.А., Соколов С.А., Мышьянов С.В., Мошков В.В., Гуминский О.А. Построение опытной аналого-цифровой зоны радиовещания DRM+/УКВ ЧМ в диапазоне 87,5–108 МГц: отчет о НИР. СПб.: Дигитон Системс, 2019. 223 с.
13. Соколов С.А., Мышьянов С.В., Сироткин А.В., Рогинский К.М. Организация мультиплекса медийных сервисов для цифрового радиовещания в стандарте DRM: отчет о НИР. СПб.: Дигитон Системс, 2020. 165 с.
14. Мышьянов С.В. Экспериментальное исследование влияния схем модуляции кодирования на размер зоны обслуживания цифрового радиовещания стандарта DRM в диапазоне ОВЧ. Часть 1 // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 101–112. DOI:10.31854/1813-324X-2021-7-3-101-11

* * *

Calculation DRM Station Coverage for Robustness Mode E

Y. Kovalgin¹ , S. Sokolov² 

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

²Digiton Systems, LLC
St. Petersburg, 191123, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-43-53

Received 17th August 2021

Revised 2nd November 2021

Accepted 8th November 2021

For citation: Kovalgin Y., Sokolov S. Calculation DRM Station Coverage for Robustness Mode E. *Proc. of Telecom. Universities*. 2021;7(4):43–53. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-43-53

Abstract: A method for calculating a DRM station coverage for the VHF bands is presented, based on the ITU-R P.1546-7 and ITU-R BS.1660-8 recommendations. It is shown that the results of coverage calculations and field measurements confirm the reliability of the suggested method.

Keywords: digital radio broadcasting, DRM system, planning broadcasting network, VHF bands.

References

1. Kovalgin Yu.A. *Digital Broadcasting: Systems and Technologies*. Moscow: Goriachaia liniia – Telekom Publ.; 2021. 580 p. (in Russ.)
2. Sokolov S.A., Myshyanov S.V., Kovalgin Yu.A. Results of the DRM Simulcast Field Trials in 87.5–108 MHz Band. *Elec-trosvyaz*. 2021;4: 30–36. (in Russ.) DOI:10.34832/ELSV.2021.17.4.003
3. Nosov V., Sartakov K. Network parameters optimization of digital TV broadcasting on the basis of transmitting station efficiency potential. *Vestnik SibGUTI*. 2016;2:41–50. (in Russ.)
4. Rec. ITU-R P.1546-7 (08/2019). *Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 3 000 MHz*.
5. Rec. ITU-R P.527-6 (09/2021) *Electrical characteristics of the surface of the Earth*.
6. Rec. ITU-R BS.1660-8 (06/2019) *Technical basis for planning of terrestrial digital sound broadcasting in the VHF band*.
7. Rec. ITU-R P.528-3 (02/2012) *Propagation curves for aeronautical mobile and radionavigation services using the VHF, UHF and SHF bands*.
8. *Planning Parameters for DRM Mode E ('DRM+') concerning the use in VHF bands I, II and III*. V 3.0 – 04/05/2011.
9. *Methodology for Frequency Planning of Radio Electronic Means of Digital Television Broadcasting of the DVB-H Standard*. Developed by the Federal State Unitary Enterprise Radio Research Institute. Approved by the decision of the State Commission for Radio Frequencies. 10th March 2011. (in Russ.)
10. Rec. ITU-R P.372-14 (08/2019) *Radio noise*.
11. Kovalgin Yu.A., Sokolov S.A., Myshyanov S.V., Svinina O.A., Kukshinov A.E., Sabanova A.I., et al. *Development of Recommendations for the Implementation of the Digital Radio Broadcasting Standard DRM+ in the Russian Federation. Report on Research Work*. St. Petersburg: The Bonch-Bruевич Saint-Petersburg State University of Telecommunications Publ.; 2015. 169 p. (in Russ.)
12. Kovalgin Yu.A., Sokolov S.A., Myshyanov S.V., Moshkov V.V., Guminsky O.A. *Construction of an Experimental Analog-Digital Broadcasting Zone DRM+ / VHF FM in the range of 87,5–108 MHz. Report on Research Work*. St. Petersburg: Digiton Systems Publ.; 2019. 223 p. (in Russ.)
13. Sokolov S.A., Myshyanov S.V., Sirotkin A.V., Roginskiy K.M. *Organization of Multiplex Media Services for Digital Broadcasting in the DRM Standard. Report on Research Work*. St. Petersburg: Digiton Systems Publ.; 2020. 165 p. (in Russ.)
14. Myshyanov S. Experimental Research of Modulation-Coding Schemes Influence on Size of the DRM Digital Radio Broadcasting Service Area in the VHF Band. Part 1. *Proc. of Telecom. Universities*. 2021;7(3):101–112. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-101-112

Сведения об авторах:

КОВАЛГИН
Юрий Алексеевич

доктор технических наук, профессор, профессор кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kowalgin@sut.ru

 <https://orcid.org/0000-0002-6753-8062>

СОКОЛОВ
Сергей Анатольевич

генеральный директор ООО «Дигитон Системс», sokoloff@yandex.ru

 <https://orcid.org/0000-0002-3112-6883>

Управление орбитальным каналным ресурсом на основе немарковских приоритетных систем массового обслуживания.

Часть 2. Методика диспетчеризации

А.А. Ковальский^{1*}, Г.А. Митряев¹, А.В. Питрин¹

¹Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, 197198, Российская Федерация

*Адрес для переписки: sake636@mail.ru

Информация о статье

Поступила в редакцию 06.10.2021

Поступила после рецензирования 08.11.2021

Принята к публикации 12.11.2021

Ссылка для цитирования: Ковальский А.А., Митряев Г.А., Питрин А.В. Управление орбитальным каналным ресурсом на основе немарковских приоритетных систем массового обслуживания. Часть 2. Методика диспетчеризации // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 54–62. DOI:10.31854/1813-324X-2021-7-4-54-62

Аннотация: В статье разработана методика диспетчеризации орбитального каналного ресурса с оперативным назначением приоритетов на основе расчета параметров немарковской модели обслуживания с ограниченным временем пребывания заявки в системе. Представленная методика отличается от известных тем, что в ней учитываются приоритетность абонентов сети, высокая динамика движения потребителей информации, среднее время ожидания при обслуживании и распределении орбитального каналного ресурса спутниковой командно-ретрансляционной системы. Проведен анализ влияния показателей качества обслуживания потоков информационных данных. Показано, что разработанная методика приоритетной диспетчеризации позволяет обеспечить требования, предъявляемые к качеству обслуживания потоков информационных данных. Проведен комплекс экспериментальных исследований, которые подтвердили возможность обеспечения требуемого уровня устойчивости при ухудшении радиоэлектронной обстановки. Сформированы практические предложения по совершенствованию комплекса координации и распределения ресурсов спутниковой командно-ретрансляционной системы.

Ключевые слова: спутниковая командно-ретрансляционная система, приоритетная диспетчеризация, орбитальный каналный ресурс, приоритетное обслуживание.

ВВЕДЕНИЕ

В настоящее время решение задач информационного обеспечения государственных структур из космоса осуществляется с использованием орбитальной группировки (ОГ) космических аппаратов различного целевого назначения, в том числе и дистанционного зондирования Земли (ДЗЗ). Перспективная спутниковая командно-ретрансляционная система (СКРС), прототипом которой является многофункциональная космическая система ретрансляции «Луч», призвана решить задачу обеспечения профильных ведомств Российской Федерации информационными данными в заданные сроки с требуемым качеством.

Проведенный в работе [1] системный анализ процесса целевого функционирования СКРС в условиях сложной радиоэлектронной обстановки (РЭО), которая непосредственно реализует функцию передачи высокоскоростных потоков информационных данных между абонентами системы, показал, что ключевым показателем качества функционирования подсистемы ретрансляции СКРС является показатель устойчивости. Данный показатель определяет способность системы выполнять свои функции при выходе из строя части элементов сети в результате воздействия внутренних и внешних дестабилизирующих факторов, в том числе и в сложных условиях РЭО.

В работе [1] проведено обоснование проблемной ситуации, которое заключается в необходимости обеспечения требуемого уровня устойчивости подсистемы ретрансляции СКРС высокоскоростных потоков информационных данных от космических аппаратов ДЗЗ и невозможности на основе существующего научно-методического аппарата планирования орбитального канального ресурса СКРС обеспечить своевременную передачу запланированного объема информационных данных в условиях сложной РЭО. Сделаны выводы об особенностях этапа координационного планирования средств подсистемы ретрансляции, заключающихся в распределении орбитального канального ресурса СКРС на основе немарковских приоритетных систем обслуживания.

К числу особенностей описываемой проблемной ситуации, определяющих актуальность исследований в направлении разработки и реализации новых подходов к организации оперативного управления орбитального канального ресурса СКРС на основе приоритетной диспетчеризации, относятся:

- увеличение на порядок численности ОГ космических аппаратов ДЗЗ и необходимость передачи значительных объемов информационных данных (до десятков терабайт) в сутки;
- уменьшенная длительность пребывания в зоне действия приемного луча перспективного космического аппарата ретрансляции (КАР) по сравнению с глобальным приемным лучом действующего космического аппарата ретрансляции, за счет использования гибридной зеркальной антенны (ГЗА), обеспечивающей пространственную защиту от помех;
- необходимость принятия решения о предоставлении доступа к ресурсу ретранслятора в условиях ограниченности зоны радиовидимости и влияния сложной РЭО (рисунок 1).

На рисунке 1 обозначены зоны радиовидимости лучей СКРС в динамически изменяющихся условиях РЭО. Так, зелеными и красными цветами обозначены зоны с удовлетворительной и неудовлетворительной помеховой обстановкой, соответственно. Передача информационных данных в красных зонах невозможна или нецелесообразна ввиду невыполнения требований по своевременности доставки сообщений. В желтых зонах работа по передаче информационных данных возможна, но скорость передачи существенно ограничена.

Управление орбитального канального ресурса в настоящее время осуществляется по плану задействования космических и наземных средств. Программа составляется и утверждается на сутки. Такой вариант управления ресурсом эффективно работает в условиях небольшого количества функционирующих космических аппаратов ДЗЗ. Однако перспективы развития ОГ космических аппаратов ДЗЗ таковы, что уже к 2030 г. планируется возрастание ОГ в 3–4 раза, что существенно увеличит информационную нагрузку на подсистему ретрансляции СКРС.

В целях уменьшения влияния РЭО на антенну КАР, основной особенностью проектируемой системы должно стать применение многолучевой ГЗА, обеспечивающей пространственную селекцию космических радиолучей за счет оперативного отключения радионаправлений при обнаружении мешающих радиоизлучений [2, 3].

Отключение отдельных лучей при жестком планировании фактически приводят к «простою» системы на время перепланирования. Используемая в настоящее время модель распределения ресурса не позволяет оперативно перераспределять потоки информационных данных, а время, необходимое для организационно-технической реализации перепланирования ресурса составляет до 3 часов.

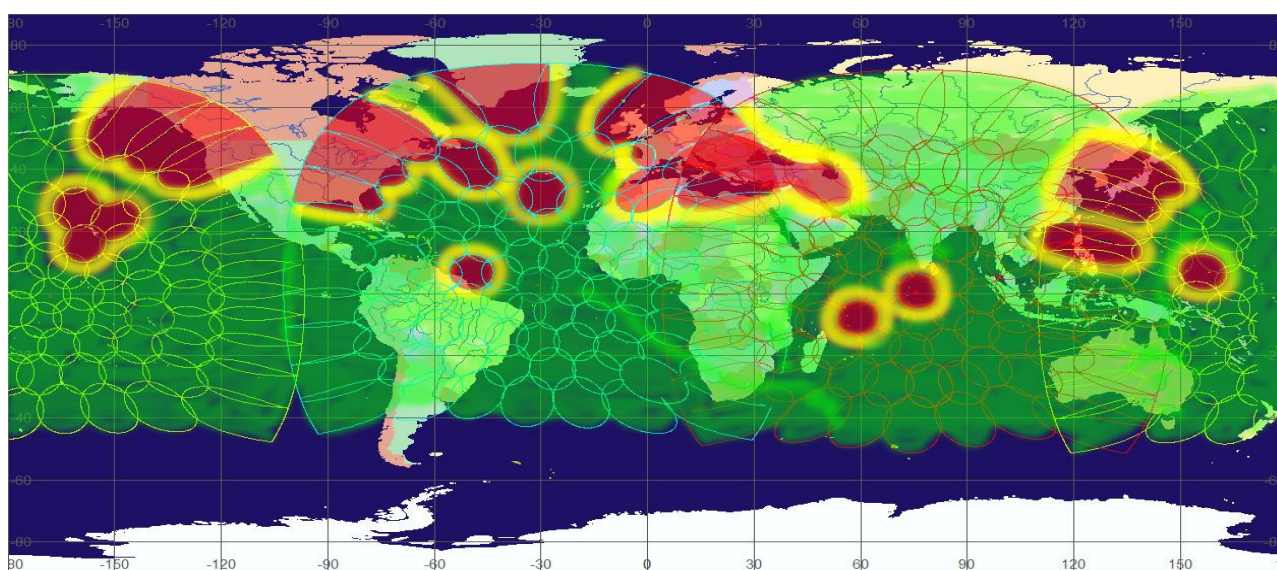


Рис. 1. Зоны радиовидимости лучей СКРС в сложных условиях РЭО

Fig. 1. Zones of Radio Visibility of Beams Satellite Command Relay System in Difficult Conditions of Radio Electronic Equipment

Все описанные факторы позволили сформулировать проблемную ситуацию, заключающуюся в необходимости обеспечения требуемого уровня устойчивости подсистемы ретрансляции высокоскоростных потоков информационных данных от космических аппаратов ДЗЗ и невозможности на основе существующего научно-методического аппарата планирования орбитального канального ресурса СКРС обеспечить своевременную передачу требуемого объема информационных данных в условиях сложной РЭО [1].

Данная работа продолжает исследования по разработке моделей распределения ограниченного орбитального канального ресурса и методов оперативной диспетчеризации потоков неоднородной информации в условиях сложной РЭО [1].

ОПИСАНИЕ МЕТОДИКИ ПРИОРИТЕТНОЙ ДИСПЕТЧЕРИЗАЦИИ

Для решения поставленной задачи, в работе [1] разработана модель оперативного распределения орбитального канального ресурса подсистемы ретрансляции на основе приоритетных систем обслуживания, в которой в отличие от известных моделей, время пребывания заявки в системе ограничено, сняты ограничения на вид распределения времени обслуживания заявок, а также получено выражение для вычисления начальных моментов распределения времени ожидания сообщений различных приоритетов.

Использование модели позволяет оценить вероятность несвоевременной доставки информационных данных, а также обеспечить требуемые показатели качества обслуживания приоритетных потоков и за счет этого обеспечить требуемую связность и устойчивость СКРС в целом.

На основе предложенной модели проведена разработка методики приоритетной диспетчеризации орбитального канального ресурса с оперативным назначением приоритетов на основе расчета параметров немарковской модели обслуживания с ограниченным временем пребывания заявки в системе. При разработке данной методики использованы подходы, изложенные в работах [4–10].

Элементом СКРС, решающим задачи распределения орбитального канального ресурса, должен являться программный комплекс координации и распределения ресурса.

Структурно методика приоритетной диспетчеризации орбитального канального ресурса СКРС состоит из 6 этапов. Произведем описание этапов предложенной методики.

Этап 1. Анализ характеристик потоков информационных данных в подсистеме ретрансляции СКРС

В рамках данного этапа производится определение характеристик потоков информационных данных на основе анализа статистики, полученной с использованием штатных средств дистанционного мониторинга и управления. Результатами выполнения первого этапа являются параметры входных потоков (средняя интенсивность поступления заявок k -го приоритета, поступающих от μ -го космического аппарата ДЗЗ), а также параметры аппроксимации потоков информационных данных вероятностными распределениями:

$$W(\tau) = e^{-\mu\tau} \sum_{i=0}^{k-1} \frac{(\mu\tau)^i}{i!}.$$

Этап 2. Анализ характеристик радиоэлектронной обстановки при функционировании СКРС

На данном этапе производится уточнение вероятностных характеристик деструктивных воздействий на подсистему ретрансляции СКРС на основе исходных данных о РЭО и функционировании каналов связи СКРС» [1, 5, 6].

Этап 3. Анализ характеристик процесса оперативного назначения приоритетов в подсистеме ретрансляции СКРС

На данном этапе производится оценивание работоспособности лучей ГЗА, время остаточного радиоконтакта каждого космического аппарата ДЗЗ в зоне работоспособных (непораженных) лучей КАР, а также оценить наличие заявок на обслуживание в системе:

$$S(t) = \langle T_{ка}(t), T_{зс}(t), M_{св}(t), V_{тр}(t) \rangle.$$

Этап 4. Формирование классов «срочных» и «несрочных» сообщений

Текущий этап реализует решение двух дополнительных оптимизационных задач, где $\bar{P}_{\nu\chi}^{hc}$ – вероятность несвоевременной доставки в зоне радиоконтакта χ -го луча ν -го КАР; $\bar{P}_{\lambda}^{hc}$ – вероятность несвоевременной доставки в зоне радиоконтакта λ -го пункта приема/передачи информации (ППИ); $W_1(t)$ и $W_2(t)$ – функции распределения несвоевременной доставки:

$$\begin{aligned} \bar{P}_{\nu\chi}^{hc}(t_{\nu\chi}^n) &= D_z(t_{\nu\chi}^n) \int_0^{t_{\nu\chi}^n} [1 - W_1(t)] dD_z(t) + \bar{D}_z(t_{\nu\chi}^n) \int_{t_{\nu\chi}^n}^{t_{\nu\chi}^n} [1 - W_2(t)] dD_z(t) \xrightarrow{t_{\nu\chi}^n} \min, \\ \bar{P}_{\lambda}^{hc}(t_{\lambda}^n) &= D_z(t_{\lambda}^n) \int_0^{t_{\lambda}^n} [1 - W_1(t)] dD_z(t) + \bar{D}_z(t_{\lambda}^n) \int_{t_{\lambda}^n}^{t_{\lambda}^n} [1 - W_2(t)] dD_z(t) \xrightarrow{t_{\lambda}^n} \min. \end{aligned}$$

Также необходимо отметить, что в разработанной методике назначение и коррекция приоритетов в обслуживании производится по критерию не превышения вероятности несвоевременной доставки сообщения от источника к потребителю от требуемой.

Этап 5. Распределение орбитального канального ресурса СКРС

На данном этапе реализуется выполнение целевой функции задачи диспетчеризации орбитального канального ресурса с оперативным назначением приоритетов, определяющей максимальный объем информации, передаваемой в течение остаточного времени радиоконтакта, где S – штраф, назначаемый менее приоритетным информационным направлением связи, для которых остаточное время радиоконтакта превышает расчетное пороговое время:

$$\sum_{v=1}^N \sum_{\chi=1}^K \sum_{\mu=1}^M [c_{v\chi\mu}^{\text{кар}}(t) t_{v\chi\mu}^{\text{кар}}] \left[S \frac{(t_{v\chi}^{\text{п}} - t_{v\chi\mu}^{\text{кар}})}{|t_{v\chi}^{\text{п}} - t_{v\chi\mu}^{\text{кар}}|} u_{v\chi\mu}^{\text{кар}}(t) \right] + \sum_{\mu=1}^M \sum_{\lambda=1}^L [c_{\mu\lambda}^{\text{зс}}(t) t_{\mu\lambda}^{\text{зс}}] \left[S \frac{(t_{\mu}^{\text{п}} - t_{\mu\lambda}^{\text{зс}})}{|t_{\mu}^{\text{п}} - t_{\mu\lambda}^{\text{зс}}|} u_{\mu\lambda}^{\text{зс}}(t) \right] \xrightarrow{\{U^{\text{ка}}, U^{\text{зс}}\} \in U_{\Delta}} \max. \quad (1)$$

Целевая функция (1) дополняется системой ограничений:

1) $\sum_{v=1}^N \sum_{\chi=1}^K u_{v\chi\mu}^{\text{кар}}(t) + \sum_{\lambda=1}^L u_{\mu\lambda}^{\text{ппи}}(t) \leq 1, \mu = \overline{1, M}$ – ограничение на одновременность работы μ -го космического аппарата ДЗЗ;

2) $\sum_{\mu=1}^M u_{v\chi\mu}^{\text{кар}}(t) \leq 1, \chi = \overline{1, K}, v = \overline{1, N}$ – ограничение на одновременность работы χ -го луча v -го космического аппарата ретрансляции только по одному космическому аппарату ДЗЗ;

3) $\sum_{\chi=1}^K \sum_{\mu=1}^M u_{v\chi\mu}^{\text{кар}}(t) \leq 1, v = \overline{1, N}$ – ограничение на одновременность задействования v -го космического аппарата ретрансляции;

4) $\sum_{\mu=1}^M u_{\mu\lambda}^{\text{ппи}}(t) \leq 1, \lambda = \overline{1, L}$ – ограничение на одновременность задействования λ -го ППИ, где $u_{\mu\lambda}^{\text{ппи}}(t) \in \{0, 1\}, \mu = \overline{1, M}, \lambda = \overline{1, L}$;

5) $V_{\mu} - \sum_{v=1}^N \sum_{\chi=1}^K [c_{v\chi\mu}^{\text{кар}}(t) t_{v\chi\mu}^{\text{кар}}] + \sum_{\lambda=1}^L [c_{\mu\lambda}^{\text{ппи}}(t) t_{\mu\lambda}^{\text{ппи}}] \geq 0$ – ограничение на объем передаваемой информации.

Задача (1) с заданной системой ограничений относится к классу задач булева программирования и решается с использованием метода ветвей и границ [11–16]. Также необходимо отметить, что в рамках данного этапа решается задача диспетчеризации орбитального канального ресурса при обслуживании потоков, реализованной в виде блочного алгоритма, который функционирует параллельно в темпе поступления исходных данных от абонентов (рисунок 2, где КА – космические аппараты; ОКР – орбитальный канальный ресурс; РВ – реальное время).

Алгоритм диспетчеризации орбитального канального ресурса при обслуживании потоков ИД предусматривает решение в режиме реального времени следующих задач:

– блоки 1–3: прием заявки на предоставление КАР орбитального канального ресурса для обслуживания космических аппаратов ДЗЗ;

– блок 4: определение требуемого времени для передачи данных времени;

– блок 5: проверка нахождения космических аппаратов ДЗЗ в зоне радиовидимости пункта приема/передачи информации;

– блок 6: сравнение скоростей передачи информационных данных через пункт приема/передачи информации и космические аппараты ДЗЗ;

– блоки 7–8: проверка параметров КАР в зоне радиовидимости пункта приема/передачи информации;

– блоки 9–12: разбиение потока заявок на 2 класса приоритетов – срочных и несрочных;

– блоки 13, 16: сброс заявок низших приоритетов;

– блоки 14, 15: постановка заявки в очередь или прекращение обслуживания менее приоритетного космического аппарата ДЗЗ;

– блоки 17, 18: коммутация космического аппарата ДЗЗ с космическим аппаратом КАР и космическим аппаратом ДЗЗ с ППИ;

– блоки 19–21: проверка качества обслуживания.

Этап 6. Оценивание устойчивости подсистемы ретрансляции СКРС в условиях сложной РЭО, для этого воспользуемся формулой общего вида [17–22]:

$$P_y(S(t), P^{\text{пр}}) = \left(1 - \prod_{j=1}^J (1 - P_{y_j}) \right) = \left(1 - \prod_{j=1}^J (1 - K_{\Gamma_j} P_{\text{св}_j}) \right).$$

Все перечисленные задачи не являются характерными для комплекса координации и распределения ресурса, реализованного в настоящее время. Использование алгоритма, а также предложенной

методики в целом позволит оперативно назначать приоритеты потокам информационных данных, что исключит «простой» СКРС, возникающий при организационно-техническом планировании орбитального канального ресурса, а также поможет оптимизировать процесс динамического перераспределения орбитального канального ресурса.

В условиях сложной РЭО предложенный алгоритм позволит выполнить требования, предъявляемые к качеству обслуживания потоков информационных данных (в первую очередь – своевременность доставки) и за счет этого обеспечит требуемую связность (вероятность связности) сети связи и, соответственно, устойчивость СКРС в целом.

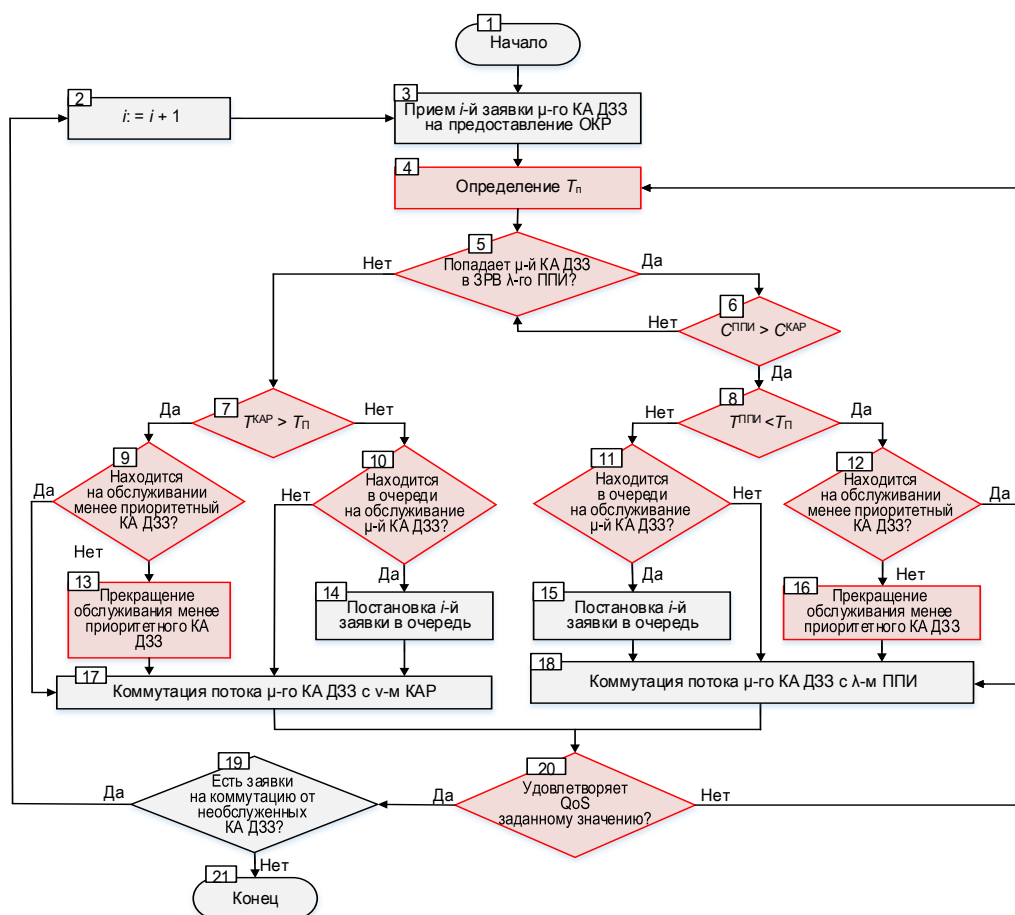


Рис. 2. Алгоритм диспетчеризации орбитального канального ресурса СКРС при обслуживании потоков информационных данных

Fig. 2. Algorithm for Scheduling the Orbital Channel Resource of the Satellite Command Relay System When Servicing Information Data Streams

АПРОБАЦИЯ РАЗРАБОТАННОЙ МЕТОДИКИ

Для оценки эффективности практического использования полученных результатов по совершенствованию комплекса координации и планирования ресурсов СКРС в работе проведен комплекс экспериментальных исследований, которые показали возможность обеспечения требуемого уровня устойчивости при ухудшении РЭО. Оценивание устойчивости подсистемы ретрансляции СКРС проводилось на основе анализа суммарного суточного объема передаваемых потоков информационных данных от космических аппаратов ДЗЗ, а также из расчета задействования СКРС при обслуживании 40 космических аппаратов ДЗЗ. В качестве исходных для формализации топологической и технической структур СКРС использован граф распределе-

ния потоков информационных данных, изображенный на рисунке 3, где СР – спутник-ретранслятор; ЦСОИ – центр сбора и обработки информации; КА – космические аппараты.

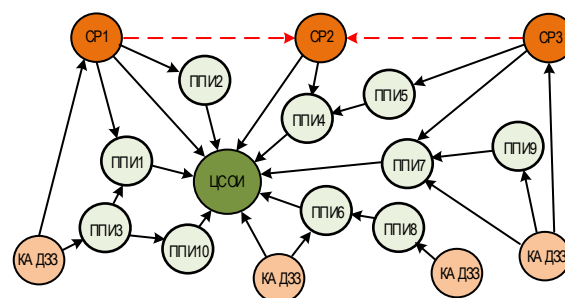


Рис. 3. Граф распределения потоков информационных данных в СКРС

Fig. 3. Graph of Distribution Data Streams in the Satellite Command Relay System

ной методики устойчивость подсистемы ретрансляции СКРС будет снижаться в среднем в пределах от 0,4 до 0,6 в среднем 3–4 раза на 0,5–1 часа. Так, время устойчивой работы СКРС при использовании методики приоритетной диспетчеризации орбитального канального ресурса составит 22 ч. 40 мин., а объем переданной информации сократятся с 8,3 Тбайт (41,5 %) до 1,6 Тбайт (8 %), что показывает ее эффективность. Использование предложенной методики позволяет обеспечить требуемый уровень устойчивости подсистемы ретрансляции СКРС в условиях сложной РЭО за счет оперативной диспетчеризации орбитального канального ресурса.

ЗАКЛЮЧЕНИЕ

В результате проведения исследований получены следующие основные результаты.

Во-первых, разработана методика диспетчеризации орбитального канального ресурса с оперативным назначением приоритетов на основе расчета параметров немарковской модели обслуживания с ограниченным временем пребывания заявки в системе, которая отличается от известных методов тем, что в ней учитывается приоритетность различных абонентов сети с учетом высокой динамики их движения и среднее время ожидания в системе обслуживания с приоритетом при распределении орбитального канального ресурса СКРС.

Во-вторых, проведен анализ влияния показателей качества обслуживания потоков информационных

данных. Показано, что разработанная методика приоритетной диспетчеризации позволяет обеспечить требования, предъявляемые к качеству обслуживания потоков информационных данных.

В-третьих, проведен комплекс экспериментальных исследований, которые показали возможность обеспечения требуемого уровня устойчивости при ухудшении РЭО, который позволил сформировать практические предложения по совершенствованию программного комплекса координации и распределения ресурса СКРС.

Научная новизна разработанной методики диспетчеризации орбитального канального ресурса состоит в том, что в ней учитывается приоритетность различных абонентов сети с учетом высокой динамики их движения и среднее время ожидания в системе обслуживания с приоритетом при распределении орбитального канального ресурса спутниковой командно-ретрансляционной системы.

Использование разработанной методики позволяет обеспечить требуемые показатели качества обслуживания приоритетных потоков информационных данных и за счет этого обеспечить требуемую связность системы и, соответственно, устойчивость СКРС в целом.

Дальнейшие исследования в данной предметной области целесообразно проводить в направлении разработки математических моделей планирования ограниченного ресурса подсистемы ретрансляции с учетом аварий (выхода из строя) инфраструктуры СКРС.

Список используемых источников

1. Ковальский А.А., Митряев Г.А., Питрин А.В. Управление орбитальным канальным ресурсом на основе немарковских приоритетных систем массового обслуживания. Часть 1. Модель оперативного распределения // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 38–46. DOI:10.31854/1813-324X-2021-7-3-38-46
2. Владимиров В.И. Информационные основы радиоподавления линий радиосвязи в динамике информационного конфликта. Воронеж: ВАИУ, 2003. 139 с.
3. Макаренко С.И. Исследование влияния преднамеренных помех на возможности по ретрансляции сообщения и показатели качества обслуживания канального уровня модели OSI для системы связи со случайным множественным доступом абонентов // Информационные технологии моделирования и управления. 2010. № 6(65). С. 807–815.
4. Камнев В.Е., Черкасов В.В., Чечин Г.В. Спутниковые сети связи. М.: «Альпина Паблишер», 2004. 536 с.
5. Косяков Е.Н., Митряев Г.А. Метод приоритетной диспетчеризации орбитального канального ресурса на основе немарковских приоритетных систем обслуживания // Известия института инженерной физики. 2018. № 4. С. 43–49.
6. Жуков С.Е., Ковальский А.А., Митряев Г.А., Квасов М.Н. Оперативное распределение радиоресурса системы спутниковой связи в целях обеспечения управления космическими аппаратами // Труды Научно-исследовательского института радио. 2017. № 2. С. 29–36.
7. Ковальский А.А., Зиннуров С.Х., Митряев Г.А. Решение задачи оптимального планирования радиоресурса спутниковой системы связи для сеансов управления орбитальной группировкой космических аппаратов // Труды учебных заведений связи. 2018. Т. 4. № 1. С. 67–74. DOI:10.31854/1813-324X-2018-1-67-74
8. Новиков Е.А., Ковальский А.А., Митряев Г.А. Алгоритм и методика оперативного планирования и распределения радиоресурса системы спутниковой связи для организации устойчивого управления орбитальной группировкой космических аппаратов // Труды Военно-космической академии имени А.Ф. Можайского. 2019. № 3(666). С. 68–76.
9. Цветков К.Ю., Косяков Е.Н., Новиков Е.А., Павлов А.Р., Зиннуров С.Х. Оптимизация параметров распределения канального ресурса спутника-ретранслятора при организации малоканальных сетей для передачи самоподобного трафика. Свидетельство о государственной регистрации программы для ЭВМ № 2015615146 от 08.05.2015.
10. Михайлов Р.Л., Макаренко С.И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. № 4. 2013. С. 69–79.
11. Абрамов П.Б. Марковские модели немарковских процессов: монография. Воронеж: Издательско-полиграфический центр «Научная книга», 2015. 204 с.

12. Рыжиков Ю.И., Уланов А.В. Применение гиперэкспоненциальной аппроксимации в задачах расчета немарковских систем массового обслуживания // Вестник Томского государственного университета Управление, вычислительная техника и информатика. 2016. № 3(36). С. 60–65. DOI:10.17223/19988605/36/6
13. Романенко В.А. Системы и сети массового обслуживания. Самара: Издательство Самарского университета, 2021. С. 21–21.
14. Petrović G., Petrović N., Marinković Z. Application of the Markov theory to queuing networks // Facta Universitatis, Series: Mechanical Engineering. 2008. Vol. 6. Iss. 1. PP. 45–56.
15. Bolch G., Greiner S., de Meer H., Trivedi K.S. Queueing Networks and Markov Chains: Modeling And Performance Evaluation with Computer Science Applications. New York: Wiley-Interscience, 1998. 726 p.
16. Bidabad B., Bidabad B. Complex Probability and Markov Stochastic Process // Proceeding of the 1st Iranian Statistics Conference (Isfahan, Iran, 26–28 May 1992). Isfahan: Isfahan University of Technology Publ., 1992.
17. Карасева Е.А., Мартышкин А.И. Применение аппарата теории массового обслуживания для системного анализа многопроцессорных систем // Международный студенческий научный вестник. 2017. № 4-9. С. 1401–1404.
18. Тихоненко О.М. Модели массового обслуживания в информационных системах. Минск: Технопринт, 2003. 326 с.
19. Наумов В.А., Самуйлов К.Е. Условия мультипликативности стационарного распределения вероятностей марковских ресурсных систем массового обслуживания с потерями // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2019. № 46. С.64–72. DOI:10.17223/19988605/46/8
20. Тихоненко О.М. Модели массового обслуживания информационных системах. Минск: УП «Технопринт», 2003.
21. Neuts M.F. A versatile Markovian arrival process // Journal of Applied Probability. 1979. Vol. 16. Iss. 4. PP. 764–779. DOI:10.2307/3213143
22. Кениг Д., Штойян Д. Методы теории массового обслуживания. Пер. с нем. М.: Радио и связь, 1981. 128 с.

* * *

The Orbital Channel Resource Control on Non-Markov Priority Systems of Mass Service Basis. Part 2. Dispatch Method

A. Kovalsky¹, G. Mitryaev¹, A. Pitrin¹

¹Military space academy of A.F. Mozhaysky,
St. Petersburg, 197198, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-54-62

Received 6th October 2021

Revised 8th November 2021

Accepted 12th November 2021

For citation: Kovalsky A., Mitryaev G., Pitrin A. The Orbital Channel Resource Control on Non-Markov Priority Systems of Mass Service Basis. Part 2. Dispatch Method. *Proc. of Telecom. Universities. Proc. of Telecom. Universities*. 2021;7(4):54–62. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-54-62

Abstract: *The article develops a methodology for scheduling an orbital channel resource with operational priority assignment based on the calculation of the parameters of a non-Markov service model with a limited residence time of a request in the system, which differs from known methods in that it takes into account the priority of various network subscribers, taking into account the high dynamics of their movement and the average waiting time in the service system with priority in the allocation of the orbital channel resource of the satellite command-relay system. The analysis of the influence of service quality indicators of information data flows is carried out. It is shown that the developed method of priority scheduling makes it possible to meet the requirements for the quality of service. A complex of experimental studies was carried out, which showed the possibility of ensuring the required level of stability with the deterioration in difficult conditions of radio electronic equipment, which made it possible to formulate practical proposals for improving the complex of coordination and distribution of resources of in the satellite command relay system.*

Keywords: *satellite command relay system, priority dispatching, orbital channel resource, priority service.*

References

1. Kovalsky A., Mitryaev G., Pitrin A. The Orbital Channel Resource Control on Non-Markov Priority Systems of Mass Service Basis. Part 1. Operational Distribution Model. *Proc. of Telecom. Universities*. 2021;7(3): 38–46. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-38-46
2. Vladimirov V.I. *Information Bases of Radio Suppression of Lines of a Radio Communication in Dynamics of Information Conflict*. Voronezh: VAIU; 2003. 139 p. (in Russ.)
3. Makarenko S.I. A Research of Influence of Deliberate Noises on Opportunities for Relaying of the Message and Figures of Merit of Service of the Data Link Layer of the OSI Model for the Communication System with Accidental Multiple Access of Subscribers. *Informatsionnyye tekhnologii modelirovaniya i upravleniya*. 2010;6(65):807–815. (in Russ.)
4. Kamnev V.E., Cherkasov V.V., Chechin G.V. *Satellite Communication Networks*. Moscow: Alpina Publisher Publ.; 2004. 536 p. (in Russ.)
5. Kosyakov E.N., Mitryaev G.A. The Method of Priority Dispatching of Orbital Channel Resource on the Basis of Non-Markov Priority Queuing Systems. *Izvestiya Instituta inzhenernoy fiziki*. 2018;4:43–49. (in Russ.)
6. Zhukov S., Kovalsky A., Mitryaev G., Kvasov M. Operational Distribution of the Radio Resource of Satellite Communication System for the Purpose of Ensuring Management of Spacecrafts. *Trudy Nauchno-issledovatel'skogo instituta radio*. 2017;2:29–36. (in Russ.)
7. Zinnurov S., Kovalsky A., Mitryaev G. Task's Solution of Satellite Communication System's Optimal Radio Resource Planning for the Sessions of Space Appliance's Orbital Group Managing. *Proc. of Telecom. Universities*. 2018;4(1):67–74. (in Russ.) DOI:10.31854/1813-324x-2018-1-67-74
8. Novikov E.A., Kovalsky A.A., Mitryaev G.A. An Algorithm and a Technique of Operational Planning and Distribution of a Radio Resource of the Satellite Communication System for the Organization of Steady Management of Orbital Grouping of Spacecrafts. *Proceedings of the Mozhaisky Military Space Academy*. 2019;3(666):68–76. (in Russ.)
9. Tsvetkov K.Yu., Kosyakov E.N., Novikov E.A., Pavlov A.R., Zinnurov S.Kh. *Optimization of the Distribution Parameters of the Channel Resource of the Relay Satellite When Organizing Low-Channel Networks for the Transmission of Self-Similar Traffic*. Patent RF, no. 2015615146, 05.08.2015.
10. Mikhaylov R.L., Makarenko S.I. Estimating Communication Network Stability Under the Conditions of Destabilizing Factors Affecting It. *Radio and telecommunication systems*. 2013;4:69–79. (in Russ.)
11. Abramov P.B. *Markov Models of Non-Markov Processes*. Voronezh: Publishing and printing center "Nauchnaya kniga"; 2015. 204 p. (in Russ.)
12. Ryzhikov Yu.I., Ulanov A.V. A Use of Hyperexponential Distribution in Non-Markovian Queuing Systems Analyses. *Tomsk State University Journal of Control and Computer Science*. 2016;3(36):60–65. (in Russ.)
13. Romanenko V.A. *Queuing Systems and Networks*. Samara: Samara University Publ.; 2021. (in Russ.)
14. Petrović G., Petrović N., Marinković Z. Application of the Markov theory to queuing networks. *Facta Universitatis, Series: Mechanical Engineering*. 2008;6(1):45–56.
15. Bolch G., Greiner S., de Meer H., Trivedi K.S. *Queueing Networks and Markov Chains: Modeling And Performance Evaluation with Computer Science Applications*. New York: Wiley-Interscience; 1998. 726 p.
16. Bidabad B., Bidabad B. Complex Probability and Markov Stochastic Process. *Proceeding of the 1st Iranian Statistics Conference 26–28 May 1992, Isfahan, Iran*. Isfahan: Isfahan University of Technology Publ.; 1992
17. Karaseva E.A., Martyshkin A.I. Application of the Apparatus of Queuing Theory for the System Analysis of Multiprocessor Systems. *Mezhdunarodnyy studencheskiy nauchnyy vestnik*. 2017;4-9:1401–1404. (in Russ.)
18. Tikhonenko O.M. *Models of Queuing in Information Systems*. Minsk: Technoprint Publ.; 2003. 326 p. (in Russ.)
19. Naumov V.A., Samouylov K.E. Conditions for the Product Form of the Stationary Probability Distribution of Markovian Resource Loss Systems. *Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie vychislitel'naya tekhnika i informatika*. 2019;46:64–72. (in Russ.) DOI:10.17223/19988605/46/8
20. Tikhonenko O.M. Models of mass service in information systems. Minsk: UP "Technoprint", 2003. (in Russ.)
21. Neuts M.F. A versatile Markovian arrival process. *Journal of Applied Probability*. 1979;16(4):764–779. DOI:10.2307/3213143
22. Koenig D., Stoyan D. *Methods of Queuing Theory*. Translated from German. Moscow: Radio i svyaz; 1981. 128 p. (in Russ.)

Сведения об авторах:

КОВАЛЬСКИЙ
Александр Александрович

кандидат технических наук, доцент, докторант военного института (научно-исследовательского) Военно-космической академии имени А.Ф. Можайского, vka@mil.ru
 <https://orcid.org/0000-0002-6878-5858>

МИТЯЕВ
Геннадий Андреевич

кандидат технических наук, начальник лаборатории военного института (научно-исследовательского) Военно-космической академии имени А.Ф. Можайского, vka@mil.ru
 <https://orcid.org/0000-0002-3840-8672>

ПИТРИН
Алексей Владимирович

адъюнкт военного института (научно-исследовательского) Военно-космической академии имени А.Ф. Можайского, vka@mil.ru
 <https://orcid.org/0000-0002-4662-9790>

Модель функционирования сети связи, построенной на основе радиорелейных станций с адаптивной модуляцией и коммутацией пакетов

С.М. Одоевский¹, В.О. Ключников¹, И.В. Степанец²

¹Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация

²Дойче Телеком,
Санкт-Петербург, 199034, Российская Федерация

*Адрес для переписки: KlyuchnikovVO@yandex.ru

Информация о статье

Поступила в редакцию 18.10.2021

Поступила после рецензирования 15.11.2021

Принята к публикации 18.11.2021

Ссылка для цитирования: Одоевский С.М., Ключников В.О., Степанец И.В. Модель функционирования сети связи, построенной на основе радиорелейных станций с адаптивной модуляцией и коммутацией пакетов // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 63–76. DOI:10.31854/1813-324X-2021-7-4-63-76

Аннотация: Статья посвящена описанию модели функционирования сети связи, построенной на основе радиорелейных станций с адаптивной модуляцией и коммутацией пакетов. Представлены математические выражения, позволяющие рассчитывать частные показатели устойчивости и пропускной способности радиорелейных интервалов, линий и направлений связи, а также обобщенные показатели качества сети связи в целом с учетом особенностей функционирования радиорелейных станций с адаптивной модуляцией и коммутацией пакетов в условиях замираний радиоволн на отдельных радиорелейных интервалах.

Ключевые слова: радиорелейная связь, адаптивная модуляция, коммутация пакетов, моделирование сетей связи.

Введение

Радиорелейная связь – вид наземной радиосвязи, основанной на многократной ретрансляции радиосигналов [1]. В настоящее время она считается надежной высокоскоростной (широкополосной) разновидностью беспроводной связи, являющейся удобной альтернативой проводной связи в сетях доступа и в транспортных сетях, особенно, когда прокладка медных или волоконно-оптических кабелей невозможна, затруднена или требует слишком много времени. Однако устойчивость радиорелейной связи ограничена влиянием среды распространения радиоволн на радиорелейных интервалах (РР-интервалах) радиорелейных линий (РР-линий) и внешних помех на входе приемников радиорелейных станций (РР-станций).

В обычных условиях при правильном планировании и эксплуатации РР-линий влияние внешних помех удастся практически исключить за счет использования направленных антенн и частотно-территориального разноса РР-станций с возмож-

ными источниками внешних помех. Остаточные неустранимые помехи (от близких передатчиков соседних РР-станций или других стволов собственной станции) проявляются в виде деградации чувствительности, для снижения (компенсации) которой используются специальные методы обработки сигналов, учитываемые при расчете РР-линий с целью прогноза их устойчивости, прежде всего, по отношению к замираниям радиоволн [2].

В целом расчет устойчивости сетей связи, построенных на основе РР-станций, в соответствии с [3] сводится к расчету устойчивости отдельных направлений связи, образуемых одной или несколькими (резервирующими друг друга) РР-линиями, состоящими из множества отдельных РР-интервалов. При этом основную сложность расчетов составляют расчеты устойчивости РР-интервалов, которые обычно выполняются в соответствии с апробированными отечественными (например, [2, 4]) и/или международными (например, [5]) рекомендациями (методиками).

Все отмеченные выше методики расчета устойчивости РР-линий и направлений связи основаны на математических моделях функционирования РР-интервалов с постоянной скоростью передачи, определяемой выбранным режимом работы модема. Однако современные РР-станции поддерживают режимы работы с адаптивной модуляцией и коммутацией пакетов (АМКП), которые предполагают адаптивное изменение скорости передачи при текущем изменении уровня сигнала и/или помех [6, 7]. Общепринятых математических моделей функционирования сетей связи, построенных на основе РР-станций с АМКП, а также соответствующих методик расчета их устойчивости, в настоящее время не существует [8]. В данной статье описывается предлагаемая математическая модель функционирования такой сети связи, которая может служить основой для дальнейшей разработки методик расчета РР-интервалов, РР-линий, направлений и сетей связи, построенных на основе РР-станций с АМКП.

Постановка задачи

В известных методиках расчета устойчивости РР-линий (в частности, [2, 4, 5]) предполагается, что РР-станции на всех РР-интервалах работают с постоянной скоростью передачи, определяемой выбранным режимом работы модема. При этом в качестве показателя неустойчивости P_n используется предположение, что вероятность ошибки превысит некоторую допустимую величину $P_{\text{ош.тр}}$. Данный показатель на практике (в ходе эксплуатации РР-интервалов и РР-линий) соответствует доле времени, когда нарушаются требования к вероятности ошибки. Принято различать (по-разному рассчитывать) и по-разному называть показатели, характеризующие неустойчивость из-за ухудшения качества связи ниже допустимой величины на коротких и продолжительных отрезках времени. Так, быстрые замирания на отрезках времени менее 10 с принято оценивать показателем качества по ошибкам или коэффициентом сильно пораженных секунд SESR (*аббр. от англ., Severely Errored Second Ratio*), а медленные замирания длительностью больше 10 с – коэффициентом неготовности [2].

Согласно указанным методикам, при расчете показателя неустойчивости P_n величина $P_{\text{ош.тр}}$ непосредственно не применяется, а задается соответствующая величина требуемого отношения сигнал/шум $h^2_{\text{тр}}$, при которой используемый в РР-станции модем на установленной (требуемой) скорости передачи $C_{\text{тр}}$ обеспечивает вероятность ошибки $P_{\text{ош}}(C_{\text{тр}})$ не более допустимой величины $P_{\text{ош.тр}}$.

При известной мощности шума $P_{\text{ш}}$, которая при отсутствии внешних помех соответствует собственному шуму приемника (при необходимости учета внешних помех их мощность добавляют к

ней, получая некоторую эквивалентную мощность шума) в полосе пропускания, соответствующей режиму работы модема, требуемое отношение сигнал/шум $h^2_{\text{тр}}$ пересчитывается в величину чувствительности $P_{\text{с.тр}} = P_{\text{ш}} \cdot h^2_{\text{тр}}$, равную минимально необходимой мощности сигнала на входе приемника, при которой обеспечивается допустимая вероятность ошибки $P_{\text{ош.тр}}$. Далее на основании рассчитанной по модели распространения радиоволн для конкретного РР-интервала медианной мощности сигнала P_c вычисляется запас на замирания $Z = P_c / P_{\text{с.тр}}$, который затем по известным статистическим зависимостям (аналитическим или графическим) пересчитывается в искомый показатель неустойчивости $P_n(Z)$.

Как следует из вышесказанного, традиционные методики расчета позволяют оценивать устойчивость РР-интервалов $P_n(C_{\text{тр}}) = P_n(Z(C_{\text{тр}}))$ после расчета запаса на замирания $Z(C_{\text{тр}})$ только при заданной постоянной скорости передачи $C_{\text{тр}}$. При пересчете найденных показателей неустойчивости отдельных РР-интервалов в показатели неустойчивости РР-линий обычно скорость передачи не упоминается, так как она в общем случае может быть разной на разных интервалах, в частности, между разными узловыми РР-станциями, ответвляющими часть каналов. Но очевидно, что неустойчивость РР-линии будет соответствовать неустойчивости сквозного цифрового канала с максимальной скоростью не выше минимальной скорости $C_{\text{тр}}$ по всем РР-интервалам.

Аналогично, при расчете неустойчивости отдельных направлений связи в общей сети связи [3], включающих несколько маршрутов прохождения сквозных каналов по участкам разных РР-линий, подразумевается, что каждый из резервных маршрутов обеспечивает скорость передачи в сквозном канале не ниже требуемой величины $C_{\text{тр}}$. В разных направлениях одной сети связи могут задаваться и оцениваться по устойчивости сквозные каналы с разными скоростями передачи. Но обобщенные показатели устойчивости сети в целом в [3] не рассматриваются.

Заметим, что показатели своевременности доставки информации (в виде любых блоков данных, в частности, пакетов) в традиционных методиках расчета РР-интервалов и РР-линий не затрагиваются, так как при использовании в них временного разделения каналов с постоянными значениями скоростей передачи пакеты данных не буферизируются и задержка составляет от нескольких тактов до цикла группового сигнала, что намного меньше длительности передачи одного пакета. В то же время нормы на показатели задержки в пакетных сетях существуют [9], но контролируются они между устройствами коммутации пакетов за пределами традиционных РР-линий, построенных на обычных РР-станциях, предоставляющих внешним устрой-

ствам коммутации пакетов сквозные каналы с постоянной скоростью передачи.

С появлением РР-станций с АМКП, которые могут динамически изменять скорость передачи и включают в своем составе устройства коммутации пакетов, возникает проблема определения показателей устойчивости РР-интервалов, РР-линий, направлений и сетей связи, построенных на основе таких РР-станций, а также проблема оценки дополнительных показателей пропускной способности и своевременности, которые до появления таких РР-станций при расчете РР-интервалов и РР-линий не регламентировались.

Для решения указанной проблемы необходимо разработать математическую модель функционирования сети связи, построенной на основе РР-станций с АМКП, которая позволит на основании заданных параметров РР-станций с АМКП $m \in M$ и заданных параметров дестабилизирующих факторов (Д-факторов) $u \in U$ рассчитывать различные частные (ЧПК) и обобщенные (ОПК) показатели качества РР-интервалов, РР-линий, направлений и сетей связи $Q(m, u)$, а также оценивать их (делать выводы о пригодности отдельных участков и сети в целом), сравнивая с требуемыми значениями данных показателей $Q_{тр}$. В обобщенном виде разработанная модель представлена на рисунке 1, где в символическом виде изображена иерархическая декомпозиция сети связи, построенной на основе РР-станций с АМКП, на вложенные направления связи, РР-линии и РР-интервалы, построенные на основе РР-станций с АМКП, функционирующих в условиях дестабилизирующих факторов, а также соответствующая последовательная взаимосвязь ЧПК РР-интервалов, РР-линий, направлений связи

и ОПК сети связи. В составе учитываемых параметров РР-станций и дестабилизирующих факторов выделены постоянные (const) и варьируемые (var) параметры, первые из которых в процессе функционирования сети не изменяются (задаются численно), а вторые изменяются случайным образом (касается дестабилизирующих факторов, описываемых соответствующими функциями распределения вероятностей) или в результате адаптации (касается РР-станций, описываемых соответствующими алгоритмами адаптации, реагирующими на текущие изменения дестабилизирующих факторов).

Стрелки в блоке с ЧПК и ОПК (см. рисунок 1) указывают причинно-следственные связи одних показателей с другими при прямом расчете (сплошные стрелки), который актуален при решении задач анализа (выбранных параметров РР-станций), и при обратном расчете (пунктирные стрелки), который актуален при решении задач синтеза (необходимых параметров РР-станций) или нормировки требований более крупных частей сети к их составным более мелким частям (например, при их нормировке касательно РР-интервалов на основании требований к РР-линиям, что бывает необходимо для оценки пригодности отдельных РР-интервалов без расчета показателей качества всей РР-линии).

Разработанная модель функционирования сети связи, построенной на основе РР-станций с АМКП, для решения указанных задач анализа и синтеза предоставляет необходимые математические зависимости, которые рассматриваются далее последовательно в виде моделей функционирования РР-интервалов, РР-линий, направлений связи и сети связи.

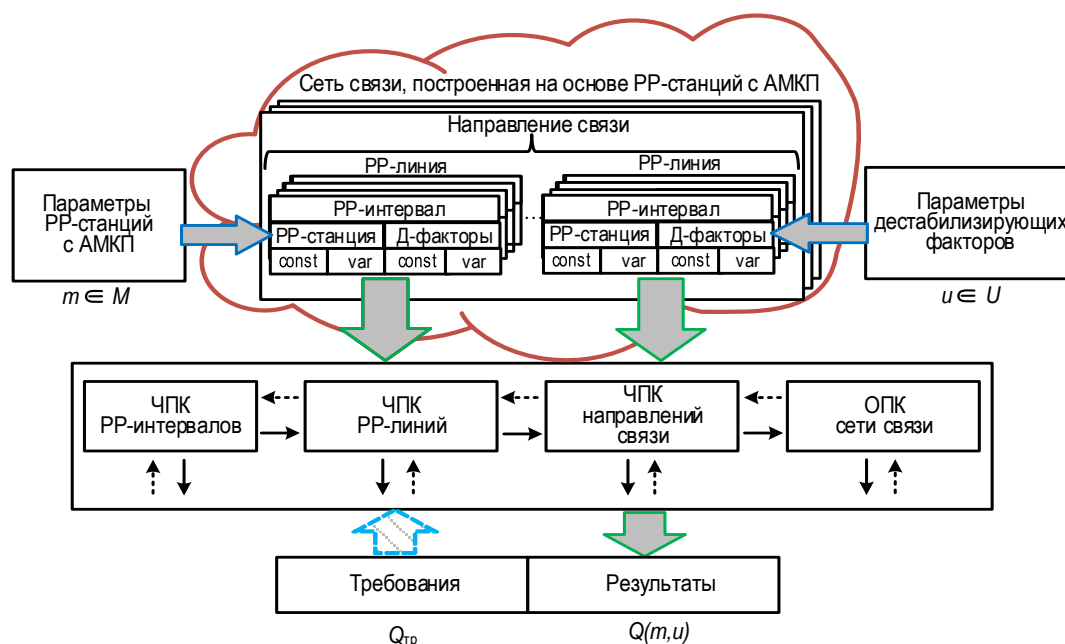


Рис. 1. Обобщенная модель функционирования сети связи, построенной на основе РР-станций с АМКП

Fig. 1. Common Functioning Model of Network of Microwave Link Stations with Adaptive Modulation and Packet Switching

Модель функционирования радиорелейного интервала

Минимальными участками сети связи, построенной на основе РР-станций с АМКП, характеристики которых влияют на характеристики всех более крупных участков, являются радиорелейные интервалы, включающие две РР-станции и среду распространения радиоволн между ними (рисунок 2).

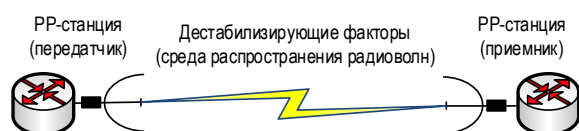


Рис. 2. Элементы модели функционирования РР-интервала, построенного на основе РР-станций с АМКП

Fig. 2. Elements of the Functional Model of Microwave Link Interval Supplied with Microwave Link Stations with Adaptive Modulation and Packet Switching

На рисунке 2 выделены элементы, участвующие в передаче информации на РР-интервале в одну сторону: от передатчика левой РР-станции к приемнику правой РР-станции. При использовании одинаковых параметров РР-станций с обеих сторон РР-интервала с учетом дуальности среды распространения радиоволн полученные результаты расчетов в одну сторону используются и в качестве результатов расчета в обратную сторону. В противном случае (если есть отличия параметров РР-станций) расчеты повторяются аналогичным образом для обратного направления.

Математическая модель функционирования РР-интервала представляет собой набор формул, связывающих параметры РР-станций $\mathbf{m}$ и дестабилизирующих факторов $\mathbf{u}$ с ЧПК РР-интервала $Q(\mathbf{m}, \mathbf{u})$ с учетом особенностей используемых режимов работы РР-станций с АМКП. Основной отличительной особенностью таких РР-станций является поддержка множества градаций скорости передачи $\mathbf{C} = \{C_1, \dots, C_n\}$ с соответствующими градациями чувствительности $\mathbf{P}_{\text{стр}} = \{P_{\text{стр},1}, \dots, P_{\text{стр},n}\}$, $\{\mathbf{C}, \mathbf{P}_{\text{стр}}\} \in \mathbf{m}$. В дальнейшем будем полагать, что все градации скорости и чувствительности упорядочены по возрастанию, т. е. $C_1 < C_2 < \dots < C_n$ и $P_{\text{стр},1} < P_{\text{стр},2} < \dots < P_{\text{стр},n}$.

После вычисления по известным методикам [2–5] медианного уровня сигнала P_c на входе приемника РР-станции с учетом известных для данного РР-интервала или вычисленных долговременных (усредненных) параметров $\mathbf{u}$ среды распространения радиоволн в роли дестабилизирующих факторов для каждой градации скорости передачи C_i , $i = \overline{1, n}$, можно вычислить запас уровня сигнала на замирания $Z_i = P_c / P_{\text{стр},i}$. Для дальнейших расчетов вместо значений запаса уровня удобнее использовать обратную величину – допустимый коэффициент ослабления сигнала $V_i = 1/Z_i$, значения которого так же, как и соответствующие градации

скорости C_i и чувствительности $P_{\text{стр},i}$, оказываются упорядоченными по возрастанию: $V_1 < V_2 < \dots < V_n$.

Случайная составляющая дестабилизирующих факторов $\mathbf{u}$, характеризующая замирания уровня сигнала, в общем случае задается некоторой функцией распределения $F(V) = \Pr(v_t < V)$ дополнительного ослабления радиоволн v_t , из-за которого уменьшается текущий уровень сигнала $P_{c,t} = P_c \cdot v_t$. Зная данную функцию распределения, можно для каждой градации скорости C_i определить коэффициент неустойчивости РР-интервала $P_{n,i} = F(V_i)$.

Сравнивая рассчитанные значения коэффициентов неустойчивости $P_{n,i}$ для каждой градации скорости C_i с требуемым значением $P_{n,\text{тр}} \in Q_{\text{тр}}$ для РР-интервала, можно определить максимальную скорость, при которой выполняются требования к устойчивости РР-интервала:

$$C_{\max} = \max_{i=\overline{1, n}} C_i | P_{n,i} \leq P_{n,\text{тр}}. \quad (1)$$

Величина $C_{\max}$ является новым ЧПК, характерным для РР-интервалов, построенных на основе РР-станций с АМКП, расчет которого известными методиками [2–5] не регламентируется, хотя и основан, как следует из представленного выше описания модели функционирования РР-интервала, именно на них. Расчет данного дополнительного показателя уже реализован во многих специальных программах проектирования РР-линий, в частности, в [8], для обоснования выбора максимальной постоянной скорости передачи на РР-интервале для обычных цифровых каналов. Но он не затрагивает в явном виде режима динамического адаптивного изменения скорости передачи на РР-интервале при пакетной передаче данных.

Математические модели радиоканалов с адаптивным изменением скорости встречались в научной литературе уже давно [10–12]. В основном они опирались на статистику замираний в диапазоне коротких волн и изменение скорости передачи путем изменения длительности (влияющей на изменение ширины спектра) простых одномерных двухпозиционных символов с амплитудной, частотной или фазовой манипуляцией. С появлением сотовой связи в диапазоне ультракоротких волн появились модели адаптивных радиолоний, в которых изменение скорости происходит путем изменения позиционности сигналов и кодовой скорости при сохранении постоянной ширины спектра [13–14]. Близость используемых алгоритмов адаптивной модуляции в сотовой и современной радиорелейной связи позволяет использовать их в составе модели функционирования РР-интервала, построенного на основе РР-станций с АМКП.

В общем случае адаптивное изменение скорости (путем изменения модуляции) происходит в некоторые дискретные моменты времени с интервалом Δt , кратном циклу группового сигнала (обыч-

но единицы – десятки миллисекунд). При выборе на очередном отрезке времени $(t, t + \Delta t)$ некоторой градации скорости C_i , реальная скорость C_t , в зависимости от текущего дополнительного ослабления v_t на данном отрезке времени, будет иметь величину:

$$C_t = \begin{cases} C_i, & v_t \geq V_i \\ 0, & v_t < V_i \end{cases} \quad (2)$$

В случае точного предсказания величины ослабления v_t на данном отрезке времени, очевидно, наилучшим выбором, максимизирующим текущую (а следовательно, и среднюю скорость за длительное время $T \gg \Delta t$ – см. далее), будет выбор градации скорости C_{i^*} , где:

$$i^* = \arg \max_{i=1,n} C_i | v_t \geq V_i. \quad (3)$$

Однако из-за погрешности измерений и задержки наблюдений, как минимум на величину Δt , абсолютно точно предсказать величину v_t по результатам наблюдений до момента $t - \Delta t$ невозможно. Как показано в [10], в случае использования непрерывного множества градаций скорости (при изменении скорости путем изменения длительности символов – это возможно) при любой дисперсии ошибки прогноза ожидаемая величина скорости C_{i^*} будет достигаться лишь с вероятностью 50 %, т. е. итоговая средняя скорость будет в два раза меньше. В [11, 12] показано, что для обеспечения более высокой (вплоть до требуемой) устойчивости и, соответственно, более высокой итоговой скорости, необходимо выбирать очередную ее градацию с некоторым дополнительным запасом по чувствительности ΔZ , величина которого зависит от функции распределения и степени корреляции замираний на интервале Δt .

При использовании дискретных градаций скорости $\{C_i\}_n$ с достаточно большим отличием соседних градаций чувствительности $\{P_{с.тр.i}\}_n$ погрешности прогнозирования замираний сказываются не так сильно. Кроме того, интервал корреляции даже быстрых интерференционных замираний на РР-интервале обычно довольно большой (десятые доли – единицы секунд), а медленных рефракционных замираний или замираний из-за осадков еще больше (десятки секунд – минуты и даже часы). На рисунке 3 представлены графики зависимости коэффициента корреляции замираний от интервала времени между моментами измерений, полученные на основании обработки статистических данных об уровне принимаемого сигнала на РР-интервале длиной 3,5 км на частоте 80 ГГц.

Из графика на рисунке 3 видно, что коэффициент корреляции очень медленно убывает с увеличением интервала времени между измерениями. При сдвиге на минимальный интервал времени 10 мин коэффициент корреляции оказался равен 0,93. Следует ожидать, что на интервале времени,

равном циклу адаптации по скорости Δt , составляющем доли секунд, коэффициент корреляции будет очень близок к 1. Таким образом, погрешностью предсказания уровня замираний на отрезке времени цикла управления скоростью передачи на РР-интервале можно пренебречь.

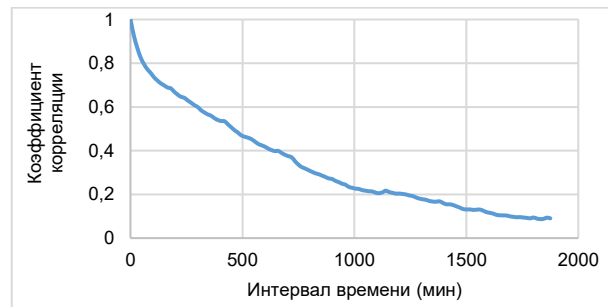


Рис. 3. Зависимость коэффициента корреляции замираний от интервала времени между моментами измерений

Fig. 3. Fading Correlation Coefficient Dependent on Different Time Intervals between the Measurements

С учетом (2), зная функцию распределения $F(V) = \Pr(v_t < V)$ дополнительного ослабления v_t , можно рассчитать среднюю скорость $C_{ср}$ передачи на РР-интервале за длительное время $T \gg \Delta t$ следующим образом:

$$C_{ср} = \sum_{i=1}^n C_i (F(V_{i+1}) - F(V_i)) = \sum_{i=1}^n C_i (P_{n,i+1} - P_{n,i}), \quad (4)$$

где $F(V_{n+1}) = P_{n,n+1} = 1$.

При отсутствии ошибок управления коэффициент неустойчивости РР-интервала в режиме пакетной передачи данных со средней скоростью (4) определяется вероятностью ослаблений, меньше допустимой величины V_1 для самой маленькой скорости C_1 , т. е. равен $P_{n,1}$.

Как следует из характеристик современных РР-станций с АМКП [6, 7], они могут по-разному обслуживать разный трафик, который можно условно разделить на две группы:

- 1) постоянный или непрерывный трафик (с требуемой постоянной скоростью $C'_t = \text{const}$);
- 2) переменный или прерывистый трафик (с допустимой переменной скоростью $C''_t = \text{var}$).

К первому типу трафика относится передача речи и видео в реальном времени (*rt* – аббр. от *англ. real time*) с жесткими требованиями к задержке, а ко второму – передача прочих данных, нетребовательных к задержке (*nrt* – аббр. от *англ. not real time*).

Обычно первый тип трафика является (и называется) приоритетным, а второй неприоритетным. При этом именно по устойчивости РР-интервала при передаче первого типа трафика с заданной скоростью $C'_{тр}$ делается вывод о пригодности интервала, т. е. РР-интервал считается пригодным, если $P_n(C'_{тр}) < P_{n,тр}$.

При использовании на РР-интервале РР-станций с АМКП эквивалентный вывод о пригодности можно сделать на основании сравнения величины $C_{\max}(P_{n,тр})$, рассчитанной по формуле (1), с $C'_{тр}$, т. е. РР-интервал считается пригодным, если $C_{\max}(P_{n,тр}) \geq C'_{тр}$. Если при этом оказывается, что $C_{j-1} \leq C'_{тр} < C_j$, где $1 < j \leq n$, то избыточные градации скорости $\{C_j, \dots, C_n\}$ можно использовать для передачи неприоритетного трафика с максимальной средней скоростью:

$$C''_{ср} = \sum_{i=j}^n (C_i - C'_{тр}) \cdot (P_{n,i+1} - P_{n,i}), \quad (5)$$

где $P_{n,n+1} = 1$.

При этом коэффициент неустойчивости РР-интервала $P_n(C''_{ср})$ при обслуживании неприоритетного пакетного трафика со средней скоростью $C''_{ср}$ (5) определяется вероятностью ослаблений, меньше допустимой величины V_j для градации скорости C_j , т. е. $P_n(C''_{ср}) = P_{n,j}$.

В связи с обслуживанием приоритетного трафика с заданной скоростью передачи практически с прежними (до появления РР-станций с АМКП) минимальными задержками на РР-интервале, можно ограничиться для данного трафика ЧПК РР-интервала в виде рассчитанной величины коэффициента неустойчивости $P_n(C'_{тр})$. Для неприоритетного трафика, кроме коэффициента неустойчивости $P_n(C''_{ср})$ (который, очевидно, в общем случае отличается от коэффициента неустойчивости для приоритетного трафика $P_n(C'_{тр}) < P_n(C''_{ср})$), к ЧПК РР-интервала следует отнести величину максимальной доступной средней скорости $C''_{ср}$. При этом, если коэффициент неустойчивости $P_n(C''_{ср})$ еще можно (для оценки пригодности РР-интервала) сопоставить с требуемой величиной $P_{n,тр}$, то о достаточности рассчитанной величины средней скорости $C''_{ср}$ ничего однозначно сказать нельзя, поскольку требования к ней для отдельных РР-интервалов не предъявляются.

В то же время для пакетных сетей, как уже отмечалось ранее, существуют нормы на допустимые задержки, которые можно пересчитать, исходя из требований к максимальной допустимой задержке передачи пакетов через сеть между граничными устройствами коммутации пакетов [9]. Среднюю задержку пакетного неприоритетного трафика $\tau_{ср}$ на РР-интервале, построенном на основе РР-станций с АМКП, можно примерно оценить, исходя из рассчитанной величины средней скорости $C''_{ср}$ при известной средней длине (объеме) L протокольных блоков данных (в частном случае, пакетов) с помощью следующей простой формулы:

$$\tau_{ср} = L/C''_{ср}. \quad (6)$$

Однако данная формула является достаточно точной только при малой дисперсии случайных

колебаний скорости. Более точное значение средней задержки можно вычислить на основании известного распределения замираний и связанного с ним (в следствие адаптации) распределения градаций скорости:

$$\tau_{ср} = L \sum_{i=j}^n (P_{n,i+1} - P_{n,i}) / (C_i - C'_{тр}). \quad (7)$$

Следует отметить, что средняя задержка, рассчитанная по формулам (6) или (7), фактически является средним временем обслуживания пакетов на РР-интервале и не зависит от интенсивности трафика на входе РР-интервала. Реальная задержка пакетов на РР-интервале будет дополнительно включать время ожидания начала обслуживания пакетов в очереди, которое существенно зависит от интенсивности и других характеристик потока данных на входе РР-интервала. В предлагаемой модели функционирования РР-интервала реальный трафик не учитывается, но данная модель может быть использована для оценки показателей качества обслуживания конкретного пакетного трафика с заданными параметрами входного потока.

Таким образом, с помощью описанной выше математической модели функционирования РР-интервала, построенного на основе РР-станций с АМКП, можно рассчитать такие ЧПК РР-интервала, как коэффициент неустойчивости приоритетного $P_n(C'_{тр})$ и неприоритетного пакетного трафика $P_n(C''_{ср})$, максимальная средняя скорость $C''_{ср}$ и средняя задержка $\tau_{ср}$ неприоритетного пакетного трафика. Причем последние три показателя являются новыми и актуальными именно для РР-интервала, построенного на основе РР-станций с АМКП. Данные ЧПК РР-интервала используются самостоятельно (если целью расчетов является анализ характеристик только РР-интервала) или в качестве исходных данных для расчетов ЧПК РР-линий, направлений связи и сетей связи, построенных на основе РР-станций с АМКП.

Модель функционирования радиорелейной линии

Согласно классическому определению радиорелейной связи, приведенному в начале статьи, одной из ее отличительных особенностей является многократная ретрансляция радиосигналов. Структурно это выражается в том, что рассмотренные выше РР-интервалы являются лишь звеньями цепи, именуемой РР-линией, с ретрансляцией на промежуточных РР-станциях. Ретрансляция в РР-линиях на стыках между соседними РР-интервалами в общем случае может осуществляться довольно большим количеством способов – начиная от пассивной ретрансляции на несущей частоте в промежуточной РР-станции, состоящей из двух антенн (или специального переотражателя радиоволн), которая

практически не вносит задержку, до ретрансляции с предварительным разуплотнением каналов для ответвления части из них на узловых РР-станциях, что уже вносит задержку, малозаметную при временном уплотнении/разделении каналов, но более существенную при использовании технологий коммутации пакетов, реализуемых в современных РР-линиях на узловых РР-станциях с АМКП (рисунок 4).

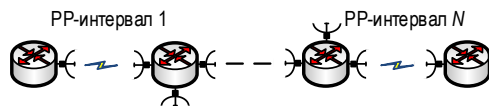


Рис. 4. Элементы модели функционирования РР-линии, построенной на основе РР-станций с АМКП

Fig. 4. Elements of the functional Model of Microwave Link Line Supplied with Microwave Link Stations with Adaptive Modulation and Packet Switching

Как и в предыдущем случае для РР-интервалов, расчеты для РР-линий выполняются в предположении, что передача данных осуществляется в одну сторону (по рисунку слева направо). При использовании симметричных РР-интервалов это неважно, и полученные результаты расчетов в одну сторону используются в качестве результатов расчета в обратную сторону. В противном случае (если есть отличия в ЧПК РР-интервалов в разные стороны) расчеты повторяются аналогичным образом для обратного направления.

Последовательный характер обработки данных на множестве РР-интервалов одной РР-линии предопределяет вид ЧПК РР-линии как некоторую аддитивную или мультипликативную свертку ЧПК РР-интервалов. Основной такой сверткой, регламентированной известными методиками расчета РР-линий, является расчет коэффициента готовности РР-линии путем перемножения коэффициентов готовности РР-интервалов (что предполагает независимость отказов и замираний на разных РР-интервалах). Указанный расчет эквивалентен следующей формуле расчета коэффициента неустойчивости РР-линии $P_{н.ррл}$ на основании рассчитанных коэффициентов неустойчивости РР-интервалов $P_{н.ррл.i}$, $i = \overline{1, N}$:

$$P_{н.ррл} = 1 - \prod_{i=1}^N (1 - P_{н.ррл.i}) \approx \sum_{i=1}^N P_{н.ррл.i} \quad (8)$$

Приближенное равенство справа в формуле (8) справедливо при очень маленьких значениях $P_{н.ррл.i} \ll 1/N$, $\forall i = \overline{1, N}$, что на практике обычно выполняется с большим запасом.

В РР-линии, построенной на основе РР-станций с АМКП, по формуле (8) можно вычислять показатели неустойчивости отдельно для приоритетного $P'_{н.ррл}$ и непериприоритетного $P''_{н.ррл}$ трафика на основании рассчитанных показателей неустойчивости $P'_{н.ррл.i}$ и $P''_{н.ррл.i}$, $i = \overline{1, N}$, для данных типов трафика на РР-интервалах.

Дополнительным ЧПК РР-линии, характеризующим ее максимальную пропускную способность, может служить величина максимальной сквозной скорости передачи $C_{\max.ррл}$ с заданной устойчивостью, которую можно рассчитать на основании рассчитанных по формуле (1) значений максимальной скорости $C_{\max.ррл.i}$, $i = \overline{1, N}$, на отдельных интервалах:

$$C_{\max.ррл} = \min_{i=\overline{1, N}} C_{\max.ррл.i} \quad (9)$$

Величина $C_{\max.ррл}$ (9) фактически характеризует максимальную пропускную способность РР-линии для приоритетного трафика $C'_{\max.ррл}$, поскольку предполагает выполнение требований по устойчивости и пренебрежимо малую задержку.

Аналогичным образом по формуле (9), подставляя в правую часть рассчитанные по формуле (5) значения максимальной средней скорости непериприоритетного трафика $C''_{ср.ррл.i}$ на отдельных интервалах $i = \overline{1, N}$, можно рассчитать и максимальную пропускную способность РР-линии для непериприоритетного пакетного трафика $C''_{ср.ррл}$. Для данного типа трафика дополнительным ЧПК является суммарная задержка в РР-линии $\tau_{ср.ррл}$, которую можно рассчитать на основании рассчитанных по формулам (6) или (7) задержек на отдельных интервалах $\tau_{ср.ррл.i}$, $i = \overline{1, N}$:

$$\tau_{ср.ррл} = \sum_{i=1}^N \tau_{ср.ррл.i} \quad (10)$$

По аналогии с замечанием, приведенным выше по поводу формул (6) и (7) расчета $\tau_{ср}$ на РР-интервале, следует отметить, что суммарная средняя задержка, рассчитанная по формуле (10), характеризует суммарное время обслуживания пакетов в РР-линии без учета времени ожидания на входе каждого очередного РР-интервала. Но если время ожидания, с учетом характеристик входного и, возможно, дополнительного (добавляемого на узловых РР-станциях) трафика будет рассчитано с помощью соответствующих математических моделей систем массового обслуживания, то оно может быть учтено в качестве дополнительных составляемых в формуле (10).

Таким образом, с помощью описанной выше математической модели функционирования РР-линии, построенной на основе РР-станций с АМКП, можно рассчитать такие ЧПК РР-линии, как коэффициент неустойчивости для приоритетного $P'_{н.ррл}$ и непериприоритетного $P''_{н.ррл}$ трафика, пропускная способность для приоритетного $C'_{\max.ррл}$ и непериприоритетного $C''_{ср.ррл}$ трафика, а также средняя задержка $\tau_{ср.ррл}$ для непериприоритетного пакетного трафика. Причем последние четыре показателя являются новыми и актуальными именно для РР-линий, построенных на основе РР-станций с АМКП. Данные ЧПК РР-линий используются самостоятельно (если целью расчетов является анализ ха-

рактических только РР-линий) или в качестве исходных данных для расчетов ЧПК направлений связи и сетей связи, построенных на основе РР-станций с АМКП.

Модель функционирования направления связи

Расчет характеристик направлений связи, образуемых между граничными устройствами коммутации (ГУК) с помощью множества маршрутов, проходящих обычно через разные участки не только разных РР-линий, но и разных кабельных линий связи, является не характерным для традиционного моделирования систем радиорелейной связи. Однако включение в состав РР-станций устройств коммутации пакетов, с которыми активно взаимодействует каналообразующая аппаратура с адаптивной модуляцией, динамически изменяющая скорость передачи на РР-интервалах, обуславливает научный и практический интерес к рассмотрению вопросов влияния характеристик РР-станций с АМКП не только на ЧПК РР-интервалов и РР-линий, но и на ЧПК направлений связи.

На рисунке 5 приведен пример элементов модели функционирования направления связи, построенного на основе РР-станций с АМКП, образующих несколько маршрутов (проходящих по разным РР-линиям) между двумя граничными устройствами коммутации ГУК₁ и ГУК₂.

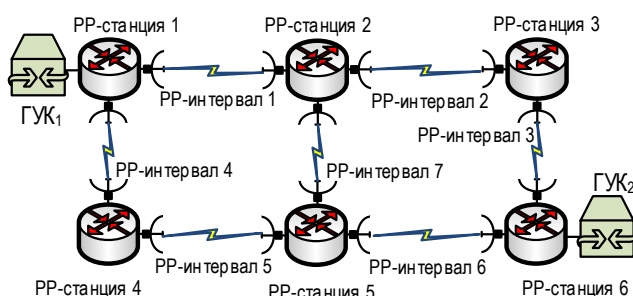


Рис. 5. Элементы модели функционирования направления связи, построенного на основе РР-станций с АМКП

Fig. 5. Elements of the Functional Model of Network Directions Supplied with Microwave Link Stations with Adaptive Modulation and Packet Switching

Выделение нескольких маршрутов (РР-линий) в одном направлении связи используется для решения двух задач: для повышения устойчивости и/или для повышения пропускной способности направления связи. Формально данные задачи могут решаться независимо, однако если оговорить, для каналов с какой пропускной способностью нужно повысить устойчивость или какую устойчивость нужно обеспечить для каналов с максимальной пропускной способностью, то оказывается, что данные задачи тесно взаимосвязаны. Если все маршруты использовать для обеспечения максимальной пропускной способности, то устойчивость направления связи будет определяться устойчивостью самой неустойчивой РР-

линии. Если же все маршруты использовать для повышения устойчивости, то пропускная способность направления связи будет определяться радиорелейной линией с самой маленькой пропускной способностью.

С другой стороны, указанное выше противоречие между устойчивостью и пропускной способностью направления связи очень напоминает противоречие между устойчивостью и скоростью передачи на РР-интервалах. И там, и там при увеличении скорости (пропускной способности) падает устойчивость, и наоборот – при снижении скорости устойчивость повышается. Отсюда следует, что при образовании направлений связи, построенных на основе РР-станций с АМКП, можно за счет изменения маршрутов в устройствах коммутации пакетов, входящих в узловые РР-станции, согласованно с адаптивным изменением скорости передачи на РР-интервалах различных маршрутов адаптивно перераспределять и тем самым максимизировать общую пропускную способность направления связи с контролируемой устойчивостью.

В целом такая процедура динамического изменения маршрутов в сетях связи, построенных на основе РР-станций с АМКП, потребует доработки системы управления всей сетью, и пока не известны (в деталях) примеры реализации таких систем. Но спрос на них есть и даже есть реклама готовых предложений [7] на основе РР-станций с АМКП в миллиметровом диапазоне волн, в котором замирания из-за осадков бывают очень длительными (о чем уже шла речь ранее), но локальными, что позволяет быстро восстанавливать или даже не прерывать связь за счет использования обходных маршрутов по участкам разных РР-линий, не подверженным одновременным замираниям.

Предлагаемая математическая модель функционирования направления связи, построенного на основе РР-станций с АМКП, базируется на методике оценки связности двухполюсного графа методом перебора простых цепей (МППЦ). Данная методика рекомендована в ГОСТ Р 53111-2008 [3], но полностью там не представлена. В приложении Б к данному ГОСТу лишь приводится общий вид формулы расчета вероятности связности p_{ij} заданной пары вершин (i, j) графа как вероятности исправного состояния хотя бы одного пути (маршрута) $\mu_{ij}^{(l)}$ из всех возможных маршрутов между этими вершинами μ_{ij} :

$$p_{ij} = E \left\{ p_{ij}^{\max} = 1 - \prod_{\forall \mu_{ij}^{(l)} \in \mu_{ij}} (1 - p_{ij}^{(l)}) \right\}, \quad (11)$$

где $p_{ij}^{(l)}$ – вероятность связности l -го маршрута $\mu_{ij}^{(l)}$, определяемая как совместная вероятность ис-

правного состояния всех ребер и вершин a , образующих этот маршрут l :

$$p_{i,j}^{(l)} = \prod_{\forall a \in \mu_{i,j}^{(l)}} p_a, \quad (12)$$

где p_a – коэффициент готовности a -го элемента последовательности ребер и вершин, принадлежащих пути $\mu_{i,j}^{(l)}$.

В части, касающейся ребер, коэффициентам готовности p_a в рассматриваемом случае направления связи, построенного на основе РР-станций с АМКП, соответствуют значения коэффициентов готовности (устойчивости) РР-интервалов, равные $(1 - P_n)$, где P_n – коэффициент неустойчивости РР-интервала, метод расчета которого был описан ранее в модели функционирования РР-интервала. В качестве коэффициентов готовности вершин можно принять коэффициенты готовности, определяемые технической надежностью РР-станций, учет которой, в частности, регламентирован в методике расчета цифровых радиорелейных линий, представленной в ГОСТ Р 53363-2009 [4].

Проблемой расчетов по формуле (11), взятой из [3], является нераскрытый математический смысл символа E перед фигурными скобками, который лишь указывает на использование в процессе расчетов по формуле, приведенной внутри скобок, так называемого поглощения, т. е. замены показателей степени больше единицы, появляющихся после раскрытия скобок у некоторых слагаемых, на единицу, что позволит исключить события многократного учета коэффициента готовности одного ребра или одной вершины. На рисунке 5 такими элементами, входящими в несколько маршрутов (в несколько РР-линий), являются РР-станции с номерами 1, 2, 5, 6 и РР-интервал 7.

Полное математическое описание МППЦ есть в [15]. Пример реализации МППЦ с подробным алгоритмическим описанием приведен в [16]. Особенностью программной реализации МППЦ, описанной в [16], является предварительный отбор всех кондиционных (подходящих) маршрутов с заданной пропускной способностью, что позволяет его использовать для расчета коэффициентов неустойчивости направлений связи, построенных на основе РР-станций с АМКП, как для приоритетного трафика $P'_{n,nc}$ с заданной скоростью передачи C'_{tr} , резервирующего для себя такую пропускную способность $C'_{tr,nc}$ во всех или в выбранной части маршрутов (РР-линий), так и для неприоритетного трафика, использующего всю оставшуюся пропускную способность C''_{nc} .

Для расчета пропускной способности C''_{nc} можно использовать известные методы решения задачи о максимальном потоке между заданными вершинами графа, например, метод расстановки пометок (алгоритм Форда – Фалкерсона), описанный в [17].

По аналогии с расчетом максимальной пропускной способности РР-линий (9) с заданной устойчивостью, для направления связи можно определить маршрут с максимальной пропускной способностью для приоритетного трафика $C'_{max,nc}$ с заданной устойчивостью. Если окажется, что $C'_{max,nc} \geq C'_{tr,nc}$, то для приоритетного трафика не потребуются резервирование, и всю оставшуюся пропускную способность C''_{nc} всех маршрутов можно использовать для неприоритетного трафика.

Величина средней задержки $t_{ср,nc}$ в направлении связи для неприоритетного трафика без учета характеристик входного трафика является неоднозначной, так как она в общем случае будет зависеть от выбираемого маршрута из множества всех маршрутов, доступных в направлении связи для неприоритетного трафика и от пропускной способности входящих в этот маршрут РР-интервалов, влияющих на задержки на каждом из них, которые учитываются в качестве слагаемых в формуле (10) при расчете суммарной задержки в РР-линии.

В качестве однозначного ЧПК, характеризующего задержку в направлении связи, можно использовать величину минимальной задержки $t_{min,nc}$ по всем маршрутам, которую можно определить известными методами поиска кратчайших маршрутов [17] или путем простого перебора уже отобранных кондиционных маршрутов.

При наличии исходных данных о характеристиках входного потока и его распределении между разными маршрутами можно будет рассчитать не минимальную, а реальную среднюю задержку $t_{ср,nc}$, которую можно минимизировать путем решения совместной задачи распределения пропускной способности и потоков данных между разными маршрутами [18].

Таким образом, с помощью описанной выше математической модели функционирования направления связи, построенного на основе РР-станций с АМКП, можно рассчитать такие ЧПК направления связи, как коэффициент неустойчивости направления связи для приоритетного $P'_{n,nc}(C'_{tr})$ и неприоритетного $P''_{n,nc}$ трафика, максимальная пропускная способность $C'_{max,nc}$ отдельного маршрута для приоритетного трафика с допустимой неустойчивостью, а также пропускная способность C''_{nc} и минимальная задержка в направлении связи $t_{nc,min}$ для неприоритетного пакетного трафика.

Все эти показатели являются новыми и актуальными для направлений связи, построенных на основе РР-станций с АМКП. Данные ЧПК направлений связи используются самостоятельно (если целью расчетов является анализ характеристик направлений связи) или в качестве исходных данных для последующего расчета ОПК сети связи, построенной на основе РР-станций с АМКП.

Модель функционирования сети связи

Расчет характеристик сети связи, включающей множество разнообразного каналаобразующего и коммутационного оборудования, используемого для формирования и обслуживания множества различных направлений связи, предоставляющих множество телекоммуникационных услуг, еще менее характерен для традиционного моделирования систем радиорелейной связи, чем расчет характеристик отдельных направлений связи. Но если для построения отдельных направлений связи, расчет ЧПК которых был рассмотрен выше, могут использоваться РР-станции с АМКП, то напрашивается вывод о возможности обобщения результатов расчета ЧПК всех направлений связи в виде некоторых обобщенных показателей качества (ОПК) всей сети связи, построенной на основе РР-станций с АМКП.

На рисунке 6 приведен пример элементов модели функционирования сети связи, построенной на основе РР-станций с АМКП, образующих по несколько маршрутов (РР-линий) во всех направлениях связи между четырьмя граничными устройствами коммутации ГУК₁, ГУК₂, ГУК₃, ГУК₄.

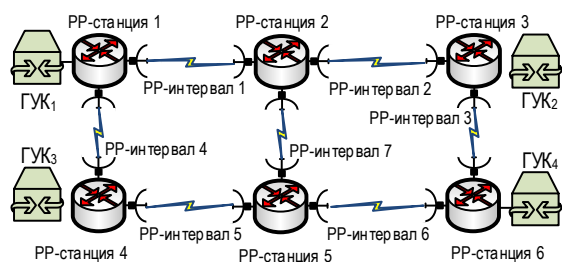


Рис. 6. Элементы модели функционирования сети связи, построенной на основе РР-станций с АМКП

Fig. 6. Elements of the Functional Model of Communication Network Supplied with Microwave Link Stations with Adaptive Modulation and Packet Switching

Обобщенная оценка показателей качества всех направлений связи, использующих общие сетевые ресурсы, является классической многокритериальной задачей, не имеющей однозначного решения без дополнительных уточнений. Указанные уточнения касаются в первую очередь степени известности на этапе проектирования требований к сети в части касающейся обслуживаемого трафика в различных направлениях связи.

Неопределенность (неполнота) указанных требований при необходимости получения конкретных гарантированных результатов принято учитывать расчетами на наихудший случай, результаты которых характеризуют вполне определенные предельные возможности сети. Так, при отсутствии исходных данных о потребностях отдельных направлений связи в пропускной способности, устойчивости и допустимых задержках в качестве ОПК сети связи можно использовать следующие граничные оценки на основе ЧПК отдельных направлений связи:

– гарантируемый (минимальный) коэффициент неустойчивости $P'_{н.с.с}$ сети связи при передаче приоритетного трафика в любом направлении связи с заданной скоростью $C'_{тр}$:

$$P'_{н.с.с}(C'_{тр}) = \max_{k=1,K} P'_{н.с.с}(C'_{тр}); \quad (13)$$

– гарантируемая (максимальная) пропускная способность сети связи для приоритетного трафика $C'_{max.с.с}$ в любом направлении связи с допустимой неустойчивостью:

$$C'_{max.с.с} = \min_{k=1,K} C'_{max.с.с,k}, \quad (14)$$

где K – количество направлений в сети связи (например, на рисунке 6 количество дуплексных направлений связи между всеми парами ГУК $K = 6$, а однонаправленных $K = 12$);

– гарантируемая (максимальная) пропускная способность сети связи для неприоритетного трафика $C''_{max.с.с}$ в любом направлении связи:

$$C''_{max.с.с} = \min_{k=1,K} C''_{н.с.с,k}; \quad (15)$$

– гарантируемая (минимальная) задержка $\tau_{min.с.с}$ в сети связи при передаче неприоритетного трафика в любом направлении связи:

$$\tau_{min.с.с} = \max_{k=1,K} \tau_{min.с.с,k}. \quad (16)$$

Указанные выше ОПК сети связи в виде граничных оценок возможностей сети позволяют, при появлении информации о конкретных требованиях обслуживаемого трафика в отдельных направлениях связи, сразу делать выводы (без дополнительных расчетов) о потенциальных возможностях их выполнения в данной сети. Однако приведенные выше граничные оценки предполагают использование всех сетевых ресурсов в интересах хотя и любого, но лишь одного направления связи.

Другим вариантом граничной оценки обобщенных показателей качества сети связи является расчет предельных возможностей сети при использовании сетевых ресурсов в интересах всех направлений связи одновременно. Одним из таких известных ОПК сети связи является обобщенный показатель устойчивости, вычисляемый как вероятность связности сети, под которой понимается вероятность наличия хотя бы одного исправного маршрута во всех направлениях связи. Относительно сети связи, построенной на основе РР-станций с АМКП, как уже отмечалось ранее, под исправным маршрутом следует понимать маршрут с пропускной способностью не менее требуемой. Эквивалентным показателем неустойчивости $P'_{н.с.с}$ сети связи для приоритетного трафика при этом является вероятность отсутствия маршрутов с требуемой пропускной способностью $C'_{тр}$ хотя бы в одном направлении связи. Рассчитать данный показатель можно одним из методов анализа структурной надежности многополюсных сетей связи, приведенных в [15].

Другим известным ОПК сети связи является обобщенный показатель суммарной пропускной способности сети $C_{\text{сум.сс}}$, который может быть рассчитан как для приоритетного $C'_{\text{сум.сс}}$, так и для неаприоритетного трафика $C''_{\text{сум.сс}}$ (на основании пропускных способностей отдельных РР-интервалов $C'_{\text{мах.рри}}$ и $C''_{\text{ср.рри}}$), вычисляемый как пропускная способность эквивалентного направления связи, образованного объединением входов всех направлений связи на одном фиктивном узле, а выходов – на другом фиктивном узле.

Расчет приведенных выше ОПК $P'_{\text{н.сс}}$ и $C_{\text{сум.сс}}$ известными методами для больших сетей является сложной переборной задачей, которая для очень больших сетей является неразрешимой. В то же время эти ОПК не позволяют судить о распределении устойчивости и пропускной способности между отдельными направлениями связи.

Первый обобщенный показатель $P'_{\text{н.сс}}$ говорит только о гарантированной минимальной устойчивости в любом направлении, но в отдельных направлениях устойчивость может быть гораздо выше этой величины $P'_{\text{н.сс}}$, которая сама по себе может превышать требуемое значение. Обе ситуации свидетельствуют об избыточном расходе ресурсов сети, что является характерным для подобных граничных оценок в условиях отсутствия информации о конкретных требованиях к устойчивости в отдельных направлениях связи.

Второй показатель $C_{\text{сум.сс}}$ говорит лишь о максимальной гарантированной суммарной пропускной способности сети по всем направлениям связи, но в конкретных направлениях связи может оказаться пропускная способность совершенно разная как выше, так и ниже требуемой, что также, как и в предыдущем случае, является следствием отсутствия учета реальных потребностей отдельных направлений связи в пропускной способности.

Если будут известны потребности отдельных направлений связи в пропускной способности $C_{\text{тр.к}}$, $k = \overline{1, K}$, то в качестве ОПК сети можно использовать обобщенный показатель $P_{\text{сс}}$ степени выполнения требований к пропускной способности в каждом направлении $C_k/C_{\text{тр.к}}$, где C_k – рассчитанные значения пропускной способности, усредненный по всем направлениям с весовыми коэффициентами, равными доле их потребностей $C_{\text{тр.к}}/C_{\text{тр.с}}$ в суммарной требуемой пропускной способности $C_{\text{тр.с}}$:

$$P_{\text{сс}} = \frac{\sum_k C_{\text{тр.к}} \cdot (C_k/C_{\text{тр.к}})}{\sum_k C_{\text{тр.к}}} = \frac{\sum_k C_k}{C_{\text{тр.с}}}. \quad (17)$$

Величина C_k представляет собой обеспеченную или реализованную пропускную способность сети в k -м направлении и зависит от распределения пропускной способности всех сетевых элементов между проходящими через них маршрутами во всех направлениях связи. На это распределение

влияют настройки маршрутов в устройствах коммутации РР-станций с АМКП, которые можно сравнивать по обобщенному показателю $P_{\text{сс}}$ (17) и оптимизировать по критерию максимума его величины. При этом требования по устойчивости в каждом направлении будут выполняться, если контролировать их выполнение при выделении указанных пропускных способностей $\{C_k\}_k$ в каждом направлении на каждом входящем в них РР-интервале, что позволяет обеспечивать адаптивную модуляцию, как было показано ранее в модели функционирования РР-интервала.

С другой стороны, заметим, что формально показатель устойчивости направления связи также характеризует степень выполнения требований к пропускной способности, но не как долю общей пропускной способности сети (что можно назвать функциональной устойчивостью [16]), а как долю времени, в течение которого эти требования выполняются. Поэтому можно включить эти показатели, именуемые показателями структурной устойчивости (поскольку рассчитываются на основе структуры сетевого графа) в качестве дополнительных коэффициентов в числителе формулы (17) и получить обобщенный показатель одновременно структурной и функциональной устойчивости сети [16]:

$$P_{\text{сс}} = \frac{\sum_k C_k \cdot (1 - P_{\text{н.к}})}{C_{\text{тр.с}}}. \quad (18)$$

При этом по-прежнему сохраняется возможность обеспечения требуемой устойчивости в каждом отдельном направлении при выделении пропускных способностей $\{C_k\}_k$.

Недостатком ОПК сети связи (18) является отсутствие учета разной важности отдельных направлений, которая может быть известна при анализе сетей связи, построенных на основе РР-станций с АМКП. Одним из популярных методов учета разной важности при аддитивной свертке частных показателей, подобной (18), является добавление весовых коэффициентов $\{\beta_k\}_k$ [19], величина которых задается пропорционально важности отдельных направлений:

$$P_{\text{сс}} = \frac{\sum_k \beta_k \cdot C_k \cdot (1 - P_{\text{н.к}})}{C_{\text{тр.с}}}, \quad (19)$$

$$\beta_k \geq 0 | \forall k = \overline{1, K}, \quad \sum_k \beta_k = 1.$$

Следует отметить, что в приведенных выше вариантах свертки ЧПК направлений связи в ОПК сети связи (17–19) под индексами $k = \overline{1, K}$ можно понимать не номера направлений связи, а условные сквозные номера виртуальных каналов во всех направлениях связи, что позволит учесть распределение сетевых ресурсов не только между направлениями связи в целом, но и между отдельными виртуальными каналами, различаемыми в устройствах коммутации РР-станций с АМКП.

Введенные в ОПК (19) весовые коэффициенты важности разных виртуальных каналов для максимизации данного ОПК можно учесть при распределении пропускной способности доступных каналов и поступающих потоков данных в каждом отдельном устройстве коммутации, что позволяет делать современные сетевые механизмы, например, механизмы взвешенных очередей [20].

Известно [10], что весовая свертка частных показателей (19) может привести к увеличению ОПК не только за счет лучших ЧПК более важных слагаемых, но и за счет большого количества менее важных слагаемых в ущерб более важным ЧПК. Поэтому представляет интерес учета в ОПК сети связи также других вариантов свертки с учетом разной важности отдельных ЧПК, чувствительных, в частности, к результатам действия сетевых механизмов приоритетного обслуживания, обеспечивающих распределение сетевых ресурсов не пропорционально весовым коэффициентам, а в порядке убывания важности (приоритета).

В качестве такого ОПК в [16] предложено использовать особую свертку частных показателей качества отдельных виртуальных каналов с учетом их относительной важности, влияющей на распределение сетевых ресурсов. Внешне данная свертка напоминает обычную аддитивную свертку (18), но сложение ЧПК при этом выполняется не в произвольном, а в строгом порядке убывания важности ЧПК. Разумеется, если бы все ЧПК были вычислены заранее, т. е. до вычисления ОПК по формуле (18), то от перестановки слагаемых сумма бы не поменялась. Но сложение ЧПК в данном случае предлагается выполнять последовательно с одновременными промежуточными вычислениями очередных ЧПК с учетом промежуточной оптимизации выделяемых ресурсов с учетом их части, уже затраченной на образование уже учтенных виртуальных каналов более высокого приоритета:

$$P_{cc} = \frac{\sum_k C_k(\{C_r\}_{k-1}) \cdot (1 - P_{n,k}(\{C_r\}_{k-1}))}{C_{тр,\Sigma}}, \quad (20)$$

где $\{C_r\}_{k-1} = \{C_1, C_2, \dots, C_{k-1}\}$ – множество сетевых ресурсов (обозначенных значениями предоставленной скорости передачи), выделенных для $k-1$ виртуальных каналов, упорядоченных в порядке убывания приоритета; $C_k(\{C_r\}_{k-1})$, $P_{n,k}(\{C_r\}_{k-1})$ – значения скорости передачи и коэффициента неустойчивости k -го виртуального канала, рассчи-

танные с учетом затраченных сетевых ресурсов для предыдущих $r = 1, k - 1$ виртуальных каналов.

Таким образом, с помощью описанной выше математической модели функционирования сети связи, построенной на основе РР-станций с АМКП, можно рассчитать как классические ОПК сети связи, характеризующие предельные возможности сети по устойчивости $P_{n,min,cc}$, пропускной способности $C_{max,cc}$ и задержкам $t_{min,cc}$ в любом отдельном направлении связи, так и интегральные сетевые показатели общесетевой устойчивости $P_{n,cc}$ и пропускной способности $C_{sum,cc}$ во всех направлениях связи. Кроме того, предложены варианты расчета ОПК сети связи P_{cc} , позволяющие учитывать индивидуальные требования к пропускной способности и устойчивости отдельных направлений связи с детализацией до требований отдельных виртуальных каналов одновременно с учетом используемых в устройствах коммутации РР-станций с АМКП сетевых механизмов, обеспечивающих распределение сетевых ресурсов с учетом указанных требований и относительной важности (приоритета) каждого виртуального канала.

Заключение

Существующие методики расчета устойчивости радиорелейных линий и образуемых на их основе направлений связи в различных транспортных сетях и сетях доступа базируются на математических моделях функционирования РР-интервалов с постоянной скоростью передачи. Однако современные РР-станции поддерживают режимы работы с адаптивной модуляцией и коммутацией пакетов, которые позволяют изменять скорость передачи, адаптируясь к текущим изменениям уровня сигнала из-за замираний. Общепринятых математических моделей функционирования сетей связи, построенных на основе РР-станций с АМКП, а также соответствующих методик расчета их устойчивости в настоящее время не существует.

В статье описана предлагаемая математическая модель функционирования такой сети связи, которая может служить основой для дальнейшей разработки методик расчета и оптимизации радиорелейных интервалов, радиорелейных линий, направлений и сетей связи, построенных на основе радиорелейных станций с адаптивной модуляцией и коммутацией пакетов.

Список используемых источников

1. Справочник по радиорелейной связи. Под ред. С.В. Бородача. М.: Радио и связь, 1981. 416 с.
2. Методика расчета трасс цифровых РРЛ прямой видимости в диапазоне частот 2-20 ГГц. М.: Инженерный центр, 1998. 245 с.
3. ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. М.: Стандартинформ, 2009. 16 с.
4. ГОСТ Р 53363-2009 Цифровые радиорелейные линии. Показатели качества. Методы расчета. М.: Стандартинформ, 2009. 68 с.

5. Рекомендация МСЭ-R P.530-17 (12/2017) Данные о распространении радиоволн и методы прогнозирования, требующиеся для проектирования наземных систем прямой видимости.
6. Кирик Ю.М., Петренко А.А. Радиорелейное оборудование с пакетной технологией передачи данных // Т-Comm: Телекоммуникации и транспорт. 2010. Т. 4. № 7. С. 86–88.
7. Брусиловский Л.И. Радиорелейные системы: настоящее и будущее // XII Международный IT-форум с участием стран БРИКС и ШОС (Югра, 2021). URL: https://itforum.admhmao.ru/upload/iblock/b2d/Radioreleynye-sistemy-svyazi-RF-nastoyashchee-i-budushchee_Brusilovskiy-L.I..pdf (дата обращения 10.10.2021)
8. Одоевский С.М., Степанец В.А. Проектирование РРЛ: программный комплекс ONEPLAN RPLS // Первая миля. 2016. № 61. С. 18–23.
9. Рекомендация МСЭ-T Y.1541 (02/2006) Требования к сетевым показателям качества для служб, основанных на протоколе IP.
10. Каневский З.М., Дорман М.И., Токарев Б.В., Крестинин В.В. Передача информации с обратной связью. М.: Связь, 1976. 349 с.
11. Постюшков В.П., Серебряков Ю.М. Пахомов И.С. Управление параметрами сигналов в радиопереносных линиях. Л.: ВАС, 1980. 51 с.
12. Онышко А.Г., Постюшков В.П., Чухванцев В.Я. Оптимальное управление энергетическими ресурсами в одноинтервальных радиопереносных линиях. Л.: ВАС. 1984. 48 с.
13. Hanzo L., Webb W. T., Keller T. Single-and Multi-carrier Quadrature Amplitude Modulation: Principles and Applications for Personal Communications, WATM and Broadcasting. Wiley, 2000. 762 p.
14. Alouini M.S., Goldsmith A.J. Adaptive Modulation over Nakagami Fading Channels // Wireless Personal Communications. 2000. Vol. 13. PP. 119–143. DOI:10.1023/A:1008979107539
15. Филин Б.П. Методы анализа структурной надежности сетей связи. М.: Радио и связь. 1987. 205 с.
16. Одоевский С.М., Лебедев П.В. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности. 2021. № 1. С. 152–189. DOI:10.24411/2410-9916-2021-10107
17. Филлипс Д., Гарсия-Диас А. Методы анализа сетей. М.: Мир. 1984. 496 с.
18. Одоевский С., Григорчук А., Яговитов Д., Ясинский С. Обобщенная методика оптимизации совместного управления трафиком и пропускной способностью мультисервисной сети связи // Информация и космос. 2021. № 2. С. 37–44.
19. Ланнэ А.А., Улахович Д.А. Многокритериальная оптимизация Л.: ВАС, 1984. 94 с.
20. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2019. 992 с.

* * *

Functional Model of Communication Network of Microwave Link Stations with Adaptive Modulation and Package Switching

S. Odоеvsky¹, V. Kluychnikov¹, I. Stepanets²

¹Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

²Deutsche Telekom,
St. Petersburg, 199034, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-63-76

Received 18th October 2021

Revised 15th November 2021

Accepted 18th November 2021

For citation: Odоеvsky S., Kluychnikov V., Stepanets I. Functional Model of Communication Network of Microwave Link Stations with Adaptive Modulation and Package Switching. *Proc. of Telecom. Universities*. 2021;7(4):63–76. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-63-76

Abstract: The article describes the model of the communication network functioning, which consist of microwave link stations with adaptive modulation and packet switching. Mathematical expressions are presented, which allow to calculate particular indicators of stability and throughput of microwave link intervals, lines and communication

directions, as well as generalized quality indicators of the communication network as a whole, taking into account the peculiarities of the functioning of microwave link stations with adaptive modulation and packet switching under the fading conditions at separate microwave link intervals.

Keywords: microwave link communication, adaptive modulation, packet switching, modeling of communication networks.

References

1. *Handbook on Radio Relay Communication*. Ed. S.V. Borodich. Moscow: Radio i sviaz Publ.; 1981. 416 p. (in Russ.)
2. *Methodology for Calculating Lines of Line-of-Sight Digital Radio Relay Lines in the Frequency Range 2–20 GHz*. Moscow: Inzhenernyi tsentr Publ.; 1998. 245 p. (in Russ.)
3. GOST R 53111-2008 *Stability of functioning of the public communications network. Requirements and check methods*. Moscow: Standartinform Publ.; 2009. 16 p. (in Russ.)
4. GOST R 53363-2009 *Digital radio-relay links. Quality parameters. Calculation methods*. Moscow: Standartinform Publ.; 2009. 68 p. (in Russ.)
5. Rec. ITU-R P.530 (12/2017) Propagation data and prediction methods required for the design of terrestrial line-of-sight systems.
6. Kirik Yu.M., Petrenko A.A. Radio Relay Equipment with Packet Data Transmission Technology. *T-Comm*. 2010;4(7): 86–88. (in Russ.)
7. Brusilovsky L.I. Radio Relay Systems: Present and Future. *Proceedings of the XII International IT Forum with the participation of the BRICS and SCO countries, Ugra, 2021*. Available from: <https://itforum.admhmao.ru/upload/iblock/b2d/Radioreleynye-sistemy-svyazi-RF-nastoyashchee-i-budushchee-Brusilovskiy-LI.pdf> [Accessed 10th October 2021]
8. Odoevsky S., Stepanets V. Designing Microwave Links, ONEPLAN RPLS Software. *Last Mile*. 2016;61:18–23. (in Russ.)
9. Rec. ITU-T Y.1541 (02/2006) Network performance objectives for IP-based services.
10. Kanevsky Z.M., Dorman M.I., Tokarev B.V., Kretinin V.V. *Information Transfer with Feedback*. Moscow: Sviaz Publ.; 1976. 349 p. (in Russ.)
11. Postyushkov V.P., Serebryakov Yu.M., Pakhomov I.S. *Control of Parameters of Signals in Radio Lines*. Leningrad: Military Academy of Communications Publ.; 1980. 51p. (in Russ.)
12. Onyshko A.G., Postyushkov V.P., Chukhvantsev V.Ya. *Optimal Management of Energy Resources in Single-Interval Radio Lines*. Leningrad: Military Academy of Communications Publ.; 1984. 48 p. (in Russ.)
13. Hanzo L., Webb W. T., Keller T. *Single-and Multi-carrier Quadrature Amplitude Modulation: Principles and Applications for Personal Communications, WATM and Broadcasting*. Wiley; 2000. 762 p.
14. Alouini M.S., Goldsmith A.J. Adaptive Modulation over Nakagami Fading Channels. *Wireless Personal Communications*. 2000;13:119–143. DOI:10.1023/A:1008979107539
15. Filin B.P. *Methods for Analyzing the Structural Reliability of Communication Networks*. Moscow: Radio i sviaz Publ.; 1987. 205 p. (in Russ.)
16. Odoevsky S.M., Lebedev P.V. Method for estimating the stability of a system of technological management for a special purpose infocommunication network with a defined topological and functional structures. *Systems of Control, Communication and Security*. 2021;1:152–189. (in Russ.) DOI:10.24411/2410-9916-2021-10107.
17. Phillips D., Garcia-Diaz A. *Network Analysis Methods*. Moscow: Mir Publ.; 1984. 496 p. (in Russ.)
18. Odoevsky S.M., Grigorchuk A.N., Yagovitev D.S., Yasinsky S.A. General Optimization Method and the Algorithm for of the Mutual Traffic and Bandwith Management of a Multiservice Communication Network. *Information and Space*. 2021;2: 37–44. (in Russ.)
19. Lanne A.A., Ulakhovich D.A. *Multi-Criterial Optimization*. Leningrad: Military Academy of Communications Publ.; 1984. 94 p. (in Russ.)
20. Olifer V., Olifer N. *Computer Networks. Principles, Technologies, Protocols*. St. Petersburg: Piter; 2019. 992 p. (in Russ.)

Сведения об авторах:

**ОДОЕВСКИЙ
Сергей Михайлович**

доктор технических наук, профессор, профессор кафедры «Сетей связи и систем коммутации» Военной академии связи имени Маршала Советского Союза С. М. Буденного», odse2017@mail.ru
 <https://orcid.org/0000-0003-3616-507X>

**КЛЮЧНИКОВ
Виктор Олегович**

адъюнкт кафедры «Сетей связи и систем коммутации» Военной академии связи имени Маршала Советского Союза С. М. Буденного», KlyuchnikovVO@yandex.ru
 <https://orcid.org/0000-0001-8812-9236>

**СТЕПАНЕЦ
Ирина Валерьевна**

эксперт ключевых проектов отдела планирования интегрированного доступа Дойче Телеком, stepanets.irina@gmail.com
 <https://orcid.org/0000-0003-1167-1590>

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

**2.3.1 – Системный анализ,
управление и обработка
информации**

**2.3.6 – Методы и системы защиты
информации, информационная
безопасность**

Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 2. Оценка прототипа

А.В. Власенко¹, М.В. Евсюков¹, М.М. Путятю¹*, А.С. Макарян¹

¹Кубанский государственный технологический университет,
Краснодар, 350072, Российская Федерация

*Адрес для переписки: putyato.m@gmail.com

Информация о статье

Поступила в редакцию 16.05.2021

Поступила после рецензирования 15.11.2021

Принята к публикации 30.11.2021

Ссылка для цитирования: Власенко А.В., Евсюков М.В., Путятю М.М., Макарян А.С. Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 2. Оценка прототипа // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 78–84. DOI:10.31854/1813-324X-2021-7-4-78-84

Аннотация: В заключительной части цикла статей, посвященного разработке системы поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей, произведено обоснование и оценка эффективности предложенной методики выбора оптимальной реализации постквантового криптографического алгоритма. Показана экономическая целесообразность предложенного подхода и продемонстрировано его положительное влияние на качество функционирования подсистемы криптографической защиты информации. Проведено сравнение эффективности разработанного прототипа системы поддержки принятия решений с существующими программными продуктами, направленными на поддержку принятия решений в области информационной безопасности. Выполнена проверка согласованности результатов работы прототипа системы поддержки принятия решений с выводами аналитических исследований в области постквантовой криптографии.

Ключевые слова: квантовый компьютер, информационная безопасность, постквантовая криптография, механизм инкапсуляции ключей, принятие решений, оценка эффективности, веб-приложение.

Введение

В настоящее время усилия ведущих мировых исследовательских институтов и крупнейших технических корпораций направлены на изучение квантовых вычислений и создание полноценного квантового компьютера, способного решать прикладные задачи. Ожидается, что вычислительные возможности квантового компьютера позволят совершить прорыв в изучении искусственного интеллекта, физике, химии и многих других областях науки [1]. Тем не менее, с точки зрения информационной безопасности, важнейшей особенностью квантового компьютера является его исключительная эффективность как инструмента криптоанализа современных криптографических алгоритмов с открытым ключом, которая обусловлена квантовым алгоритмом Шора, разработанным в

1994 г. Данный алгоритм позволяет с полиномиальной сложностью решать задачи факторизации и дискретного логарифмирования (в том числе в группе точек эллиптической кривой) [2], на субэкспоненциальной сложности которых основана надежность современных асимметричных криптографических алгоритмов [3].

Таким образом, квантовый компьютер делает небезопасными все широко применяемые сегодня криптосистемы с открытым ключом. Данный факт поставил перед научным сообществом задачу поиска новых, постквантовых асимметричных криптографических алгоритмов, способных противостоять квантовому криптоанализу. В результате такие алгоритмы были разработаны и следующим шагом на пути внедрения постквантовой криптографии стал процесс принятия соответствующих стандартов. Данный процесс был инициирован

NIST и проводится в форме открытого для заявок и комментариев конкурса [4].

В момент написания данной статьи проходит 3-й этап конкурса, к началу которого был определен перечень алгоритмов-фаворитов, которые в наибольшей мере отвечают требованиям, предъявляемым к постквантовому стандарту [5].

По сравнению с такими классическими асимметричными алгоритмами как, например, RSA или ElGamal, постквантовые криптосистемы характеризуются использованием сложных и ресурсоемких математических структур. Вследствие этого постквантовые алгоритмы уступают классическим при сравнении по различным метрикам производительности. Данный факт усложняет процесс внедрения новых алгоритмов, поскольку существенное повышение нагрузки на защищаемые информационные системы крайне нежелательно.

На конкурсе NIST представлено широкое разнообразие конкурирующих подходов к обеспечению безопасности. Конструкция и характеристики постквантовых алгоритмов существенно отличаются от заявки к заявке, что не позволяет выделить среди них безусловно лучшее решение, являющееся оптимальным для всех возможных сценариев применения [6].

Более того, каждый из заявленных алгоритмов имеет несколько различных реализаций, каждая из которых нацелена на определенный сценарий применения и задает собственный баланс между метриками безопасности и производительности.

Перечисленные выше особенности текущего состояния постквантовой криптографии делают актуальной задачу выбора оптимальной реализации постквантового криптографического алгоритма для защиты конкретной информационной системы. Данный тезис подтверждается отчетами NIST, в которых подчеркивается полезность дифференцированного подхода к выбору используемой криптосистемы. В зависимости от особенностей защищаемого канала связи, предпочтительным может быть применение алгоритма, отличного от того, который закреплен в стандарте [4].

Оценивается, что полноценный квантовый компьютер будет создан в течение ближайших 10 лет. За это время необходимо успеть не только принять постквантовые стандарты, но и внедрить новые алгоритмы в практическое использование. Например, внедрение симметричного алгоритма AES заняло более 5 лет, однако переход на новые асимметричные алгоритмы, электронные подписи и механизмы инкапсуляции ключей обещает быть более сложной задачей. В то же время, важно учитывать, что квантовый компьютер уже сейчас представляет угрозу для критически важной информации. Это связано с тем, что злоумышленник имеет возможность записать интересующие его данные и

дешифровать их после появления полноценного квантового компьютера.

В связи с этим, задача внедрения постквантовых криптографических алгоритмов станет актуальной в ближайшем будущем. Именно поэтому цель предыдущей части цикла статей состояла в том, чтобы предложить алгоритм автоматизированного выбора оптимальной для конкретной информационной системы реализации постквантового криптографического алгоритма и разработать прототип системы поддержки принятия решений (СППР), использование которой позволило бы упростить внедрение постквантовых средств криптографической защиты информации в работу организации [7].

В результате, в предыдущей статье цикла был произведен выбор алгоритмов принятия решения для разрабатываемой системы, а также выполнена адаптация метода последовательных уступок в соответствии с особенностями рассматриваемой задачи. В качестве частных критериев для метода последовательных уступок предложено использовать метрики канала связи, которые затем выражены через характеристики методов инкапсуляции ключей. Сформирована база данных характеристик существующих реализаций механизмов инкапсуляции ключей. Выполнена практическая реализация прототипа поддержки принятия решения в форме веб-приложения [7].

Однако конкурентоспособность предложенного подхода требует обоснования. Для этого требуется провести оценку эффективности разработанной СППР с учетом существующих аналитических исследований в области постквантовой криптографии.

Для оценки эффективности предложенного подхода предполагается использовать следующие критерии:

- экономическая эффективность;
- повышение качества работы защищаемого сервиса;
- эффективность по сравнению с аналогичными системами;
- согласованность предлагаемых решений с результатами аналитических исследований в области постквантовой криптографии.

Экономическая эффективность

Предложенное решение позволяет оптимизировать сроки исполнения задач, связанных с разработкой программного продукта, использующего реализации криптографических алгоритмов, или сроки создания комплексной системы защиты информации для конкретного объекта информатизации.

В свою очередь, это приводит к следующим позитивным последствиям:

- получение конкурентного преимущества от максимально быстрого выпуска продукта, что позволяет избежать потери доли рынка из-за более

раннего выпуска аналогичного продукта конкурентами;

- более ранний выпуск продукта позволяет избежать упущенной за время простоя (невозможности выполнения критических функций) выгоды;
- снижение вероятности нарушения сроков выполнения проекта и, следовательно, потери доверия со стороны заказчиков;
- своевременное достижение целей позволяет избежать нарушения сроков выполнения зависимых задач.

С точки зрения бизнеса, более быстрый выпуск продукта позволяет уменьшить такие показатели эффективности как «Time to Market» и «Cost of Delay» [8]. Концепция показателя «Cost of Delay» проиллюстрирована на рисунке 1.

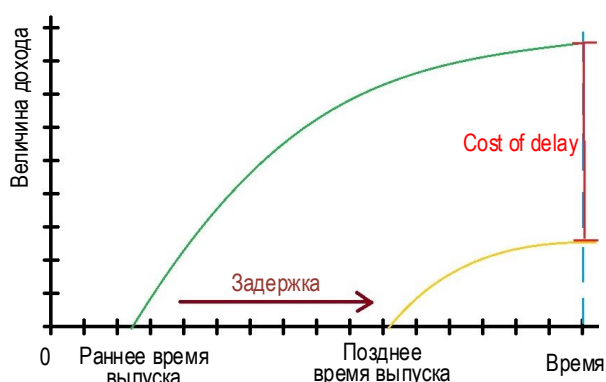


Рис. 1. Иллюстрация концепции показателя «Cost of Delay»

Fig. 1. Illustration of the "Cost of delay" Metric Concept

Однако коммерческая выгода от использования предложенной СППР не исчерпывается оптимизацией сроков исполнения задач. Другая важная составляющая экономического эффекта – экономия времени специалистов, задействованных в проектировании системы, использующей реализации постквантовых криптографических алгоритмов.

Задача разработанного прототипа СППР – предложить оптимальную реализацию постквантового механизма инкапсуляции ключей для использования в информационной системе, обладающей указанными пользователем набором характеристик. Таким образом, с экономической точки зрения, эффективность разработанной программы можно выразить как экономию ресурсов и времени специалистов, которое расходуется на принятие решения при неавтоматизированном выборе реализации постквантового алгоритма.

Для того, чтобы сделать обоснованный выбор, специалистам необходимо детально изучить свойства и особенности каждой реализации алгоритма и принять решение о том, какая из них наиболее полно соответствует требованиям системы. Однако разработанное приложение использует указываемые пользователем характеристики защищаемой системы для того, чтобы предложить оптимальную реализацию постквантового алгорит-

ма, что существенно снижает издержки на принятие решения.

Реализованный в прошлой части цикла статей подход к решению задачи выбора оптимального средства защиты заключается в формализованном представлении характеристик криптографических алгоритмов и свойств защищаемых разновидностей информационных систем. Далее эти сведения используются для того, чтобы для указанной информационной системы предложить рейтинг оптимальных реализаций постквантовых механизмов инкапсуляции ключей [7].

Таким образом, можно сказать, что работа специалистов, занимающихся развитием конкретной информационной системы, направленная на анализ реализаций постквантовых алгоритмов, заменяется работой создателей СППР, направленной на имплементацию алгоритма принятия решений и настройку параметров системы. Преимущество такого подхода заключается в том, что СППР разрабатывается в форме веб-приложения, что позволяет многократно использовать ее неограниченно большому кругу пользователей. Кроме того, при изменении предметной области, а именно набора алгоритмов или характеристик реализаций, параметры системы могут быть актуализированы.

Повышение качества работы защищаемого сервиса

Обязательность внедрения постквантовой криптографии обусловлена необходимостью поддержания безопасности информационных систем на должном уровне после появления угрозы нового поколения – квантового компьютера. Для достижения этой цели неизбежен переход к использованию более сложных и ресурсоемких алгоритмов, ввиду чего становится актуальной задача сохранения производительности работы сервисов на максимально возможном уровне.

Неоптимальный, с точки зрения производительности, выбор криптографического алгоритма способен привести к возникновению следующих нежелательных технических проблем в работе сервиса:

- чрезмерное расходование вычислительных ресурсов вплоть до прихода сервиса в состояние «отказ в обслуживании»;
- повышение частоты сбоев из-за повышенной нагрузки, т. е. уменьшение средней доступности;
- увеличение времени отклика сервиса;
- уменьшение полезной пропускной способности (увеличение количества служебного трафика).

Перечисленные выше проблемы, в свою очередь, способны привести к следующим последствиям для владельца сервиса:

- потеря пользователей;
- необходимость материальных затрат на увеличение доступной вычислительной мощности;

- наступление последствий нарушения штатного режима работы объектов критической информационной инфраструктуры;
- нарушение утвержденного соглашения об уровне услуг.

Например, для провайдеров информационных услуг критически важно поддержание показателей уровня обслуживания (SLI, аббр. от англ. Service Level Indicator) в соответствии с обозначенным целевым уровнем обслуживания (SLO, аббр. от англ. Service Level Objectives) [9]. Обычно допускается, что реальные SLI могут отклоняться от SLO не более, чем на некоторую допустимую величину (от англ. Error Budget). Выход данных показателей за установленный предел может привести к нарушению критических функций бизнеса, потере клиентов и утрате конкурентного преимущества. Также это способно повлечь за собой нарушение договорных обязательств перед клиентами, а именно соглашения об уровне оказываемых услуг (SLA, аббр. от англ. Service Level Agreement) и, следовательно, юридические последствия и штрафы.

Таким образом, правильный выбор криптографического алгоритма способен упростить переход на постквантовую криптографию, минимизировать риски, избежать лишних материальных затрат и обеспечить максимально качественный пользовательский опыт. Дополнительным преимуществом оптимизации использования располагаемых вычислительных ресурсов компании является минимизация расходов на модернизацию информационной системы, потребность в которой может возникнуть в результате перехода на новые криптографические алгоритмы.

Эффективность по сравнению с аналогичными системами

Проблема выбора набора средств защиты информации, соответствующего требованиям конкретного объекта информатизации и обеспечивающего достаточную защиту, в условиях ограниченности ресурсов – важная задача в сфере информационной безопасности, которая является предметом большого числа исследований. Например, в [10] на основе модели целочисленного программирования разрабатывается прототип инструмента поддержки принятия решения, нацеленный на оптимизацию портфеля средств управления безопасностью организации, в который входят элементы управления оборудованием, ПО, политиками, процедурами и учебными мероприятиями. В [11] разрабатывается компьютерная СППР, а также ее методическое обеспечение выбора вариантов систем информационной безопасности коммерческих организаций на основе предложенных критериев (и шкал их измерений), не сводимых к одному критерию. При этом, в качестве теоретической базы используются исследования ра-

боты ведущих отечественных и зарубежных специалистов в области многокритериального принятия решений. В [12] с целью повышения эффективности системы обеспечения информационной безопасности разрабатываются механизмы интеллектуализации процессов защиты информации. В качестве теоретического базиса выступают методы системного анализа, математического моделирования, нечеткой логики и теории принятия решений.

Как было показано ранее, проблема выбора оптимального средства защиты особенно актуальна для постквантовой криптографии, но на данный момент отсутствуют программные средства, осуществляющие поддержку решения данной задачи. К настоящему моменту созданы программные библиотеки, предлагающие разработчикам ПО широкое разнообразие реализаций постквантовых криптографических алгоритмов, например, OpenSSL [13]. Однако пользователю зачастую неясно, какая конкретная реализация способна наилучшим образом удовлетворить его требования. Таким образом, присутствует потребность в дополнении имеющегося разнообразия криптосистем руководством или информационным ресурсом, облегчающим выбор наиболее подходящего.

В контексте сравнения с другими системами поддержки принятия решений в области информационной безопасности разработанный подход обладает следующими преимуществами:

- ориентированность на задачу (пользователю достаточно указать характеристики системы и целевой уровень защиты, чтобы получить рейтинг наиболее подходящих реализаций);
- возможность актуализации сведений о реализациях постквантовых алгоритмов с учетом актуальных исследований;
- легкость «доставки» веб-приложения до пользователей;
- интерактивность;
- фокус на решении конкретной задачи.

Согласованность предлагаемых решений с результатами аналитических исследований

Важнейшим критерием корректности работы любой СППР является согласованность с результатами актуальных исследований в соответствующей предметной области. Сравнительный анализ результатов работы СППР и результатов аналитических исследований в сфере постквантовой криптографии [14–18] представлена в таблице 1. Здесь видно, что наиболее оптимальные для конкретных сценариев применения, согласно аналитических исследований, постквантовые механизмы инкапсуляции ключей находятся на первых местах в рейтинге, составленном СППР. Это свидетельствует о том, что результаты работы СППР согласуются с выводами аналитических исследований в области постквантовой криптографии.

ТАБЛИЦА 1. Сравнительный анализ результатов работы СППР и результатов аналитических исследований

TABLE 1. Comparative Analysis of the Results of the Work of the Decision Support System and the Results of Analytical Studies in the Field

Способ управления ключами	Характеристики				Уровень безопасности	Лучший алгоритм на основе исследований	Место в рейтинге составленном СППР
	клиента		сервера				
	Тип	Канал связи	Тип	Количество подключений			
Эфемерный	Ноутбук	Узкий	ПК	Высокое	AES-512	NTRU	1
Эфемерный	ПК	Узкий	Промышленный	Среднее	AES-128	SIKE	2
Эфемерный	Смартфон	Узкий	Микрокомпьютер	Среднее	AES-128	Round5	1
Повторная отправка	Смартфон	Средний	ПК	Высокое	AES-256	Saber	1
Кеширование на стороне клиента	ПК	Широкий	Промышленный	Низкое	AES-256	FrodoKEM	2

Также из таблицы 1 видно, что лучший, согласно исследованиям, алгоритм не всегда находится на первом месте. Это связано с тем, что, как было обозначено в предыдущей части цикла статей, разрабатываемая СППР способна учесть только формализуемые параметры криптосистем, в частности, их количественные метрики, связанные с безопасностью и производительностью. В то же время, в аналитических исследованиях принимаются во внимание более тонкие особенности каждого алгоритма, которые не всегда возможно учесть при автоматизированном принятии решения.

Именно поэтому пользователю системы предлагается не единственный «лучший» алгоритм, а рейтинг альтернатив, составленный по убыванию характеристик алгоритмов, связанных с безопасностью и производительностью. Информация о неформализованных свойствах алгоритмов представляется в форме справочной информации [7].

Заключение

Предложенный в [7] подход продемонстрировал свою эффективность в обеспечении информационной поддержки задачи внедрения постквантовых средств криптографической защиты в рамках организации, которая является одной из наиболее актуальных проблем современной информационной безопасности.

К недостаткам представленного подхода можно отнести необходимость корректной настройки параметров системы экспертами, а также потребность в постоянной актуализации сведений о реализациях криптографических алгоритмов. Также, в работе системы используется ряд допущений, в частности, все многообразие реальных вычислительных машин представлено набором абстрактных устройств. Кроме того, при составлении рейтинга альтернатив принимаются во внимание только формализованные характеристики алгоритмов.

Список используемых источников

1. Гринштейн Д., Зайонц А. Квантовый вызов. Современные исследования оснований квантовой механики. М.: Изд-во Интеллект, 2012. 432 с.
2. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Scientific and Statistical Computing. 1997. Vol. 26. Iss. 5. PP. 1484–1509. DOI:10.1137/S0097539795293172
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Изд-во Триумф, 2002. 815 с.
4. NIST Report. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2016. 25 p.
5. Alagic G., Alperin-Sheriff J., Apon D., et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2020. 39 p.
6. Alagic G., Alperin-Sheriff J., Apon D., et al. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2019. 27 p.
7. Власенко А.В., Евсюков М.В., Путятю М.М., Макарян А.С. Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 1. Алгоритм принятия решений // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 70–79. DOI:10.31854/1813-324X-2020-6-4-70-79
8. Larson E., Gray C. Project Management: The Managerial Process. NY: McGraw-Hill Education, 2017. 688 p.
9. Wetzstein B., Karastoyanova D., Leymann F. Towards Management of SLA-Aware Business Processes Based on Key Performance Indicators // Proceedings of the 9th Workshop on Business Process Modeling Development and Support (BPMDS'08 Montpellier, France, 16–17 June 2008). URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.623.3105&rep=rep1&type=pdf> (дата обращения 14.05.2021)
10. Almeida L., Respicio A. Decision support for selecting information security controls // Journal of Decision Systems. 2018. Vol. 27. No. S1. PP. 173–180. DOI:10.1080/12460125.2018.1468177
11. Рагозин Ю.Н. Система поддержки принятия управленческих решений при выборе вариантов информационной безопасности. М.: ГОУ МГИУ, 2011. 23 с.

12. Рахимов Е.А. Модели и методы поддержки принятия решений в интеллектуальной системе защиты информации. Уфа: УГАТУ, 2006. 21 с.
13. OpenSSL. Cryptography and SSL/TLS Toolkit. URL: <https://www.openssl.org> (дата обращения 14.11.2021)
14. Луценко М.С., Киян А.С., Кузнецова Т.Ю., Кузнецов А.А. Анализ и сравнительные исследования кодовых схем инкапсуляции ключей, представленные на конкурсе NIST PQC // Всеукраинский межведомственный научно-технический сборник «Радиотехника». 2018. № 193. URL: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_193_8.pdf (дата обращения 14.11.2021)
15. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking? // The 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019), Chongqing, China, 8–10 May 2019. URL: <https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf> (дата обращения 03.11.2020)
16. Baan H., Bhattacharya S., Fluhrer S., et al. Round5: KEM and PKE based on (Ring) Learning with Rounding // Round 5. URL: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions> (дата обращения 14.11.2021)
17. Власенко А.В., Евсюков М.В., Путятю М.М., Макарян А.С. Исследование реализации механизмов инкапсуляции ключей постквантовых криптографических методов // Прикаспийский журнал: управление и высокие технологии. 2019. № 4. С. 121–127. DOI:10.21672/2074-1707.2019.48.4.121-127
18. Nist software performance tests // SAFECrypto. URL: <https://www.safecrypto.eu/pqclounge> (дата обращения 14.11.2021)

* * *

Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 2. Prototype Evaluation

A. Vlasenko¹, M. Evsyukov¹, M. Putyato¹, A. Makaryan¹

¹Kuban State Technological University,
Krasnodar, 350072, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-78-84

Received 16th May 2021

Revised 15th November 2021

Accepted 30th November 2021

For citation: Vlasenko A., Evsyukov M., Putyato M., Makaryan A. Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 2. Prototype Evaluation. *Proc. of Telecom. Universities*. 2021;7(4): 78–84. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-78-84

Abstract: *This is the final part of the series of articles devoted to the development of a decision support system for choosing the optimal post-quantum key encapsulation mechanism. Efficiency of the methodology proposed for choosing the optimal implementation of the post-quantum cryptographic algorithm is evaluated and substantiated. The economic feasibility of approach is shown and its positive impact on the quality of the cryptographic information protection subsystem is demonstrated. Efficiency comparison of the prototype of the decision support system with existing software products aimed at supporting decision-making in the field of information security is carried out. The consistency of prototype's recommendations with the conclusions of analytical studies in the field of post-quantum cryptography is checked.*

Keywords: *quantum computer, information security, postquantum cryptography, key encapsulation mechanism, decision making, efficiency estimation, web-application.*

References

1. Grinshteyn D., Zayonz A. *Quantum Challenge. Modern Research of Quantum Mechanic's Basics*. Moscow: Intellect Publ.; 2012. 432 p. (in Russ.)
2. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Scientific and Statistical Computing*. 1997;5(26):1484–1509. DOI:10.1137/S0097539795293172
3. Schneier B. *Applied Cryptography. Protocols, Algorithms, and Source Code*. Moscow: Triumph Publ.; 2002. 815 p. (in Russ.)

4. NIST Report. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2016. 25 p.
5. Alagic G., Alperin-Sheriff J., Apon D. et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2020. 39 p.
6. Alagic G., Alperin-Sheriff J., Apon D. et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2019. 27 p.
7. Vlasenko A., Evsyukov M., Putyato M., Makaryan A. Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 1. Decision Making Algorithm. *Proc. of Telecom. Universities*. 2020;6(4):70–79. (in Russ.) DOI:10.31854/1813-324X-2020-6-4-70-79
8. Larson E., Gray C. *Project Management: The Managerial Process*. NY: McGraw-Hill Education; 2017. 688 p.
9. Wetzstein B., Karastoyanova D., Leymann F. Towards Management of SLA-Aware Business Processes Based on Key Performance Indicators. *Proceedings of the 9th Workshop on Business Process Modeling Development and Support, BPMDS'08, 16–17 June 2008, Montpellier, France*. Available from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.623.3105&rep=rep1&type=pdf> [Accessed 14 May 2021]
10. Almeida L., Respicio A. Decision support for selecting information security controls. *Journal of Decision Systems*. 2018;27(S1):173–180. DOI:10.1080/12460125.2018.1468177
11. Ragozin Y. *Management Decision Support System for Choosing Information Security Options*. Moscow: Moscow State Industrial University Publ.; 2011. 23 p. (in Russ.)
12. Rahimov E. *Models and Methods of Decision Support in an Intelligent Information Security System*. Ufa: Ufa State Aviation Technical University Publ.; 2006. 21 p. (in Russ.)
13. OpenSSL. Cryptography and SSL/TLS Toolkit. Available from: <https://www.openssl.org/> [Accessed 14th November 2021]
14. Lucenko M.S., Kiyani A.S., Kuznetsova T.U., Kuznetsov A.A. Analysis and Comparative Studies of Key Encapsulation Code Schemes Presented at the NIST PQC Competition. *All-Ukrainian Interdepartmental Scientific and Technical Collection "Radio-tekhnika"*. 2018;193. (in Russ.) Available from: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_193_8.pdf [Accessed 14th November 2021]
15. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking? // The 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019), Chongqing, China, 8–10 May 2019. URL: <https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf> [Accessed 3rd November 2020]
16. Baan H., Bhattacharya S., Fluhrer S. et al. Round5: KEM and PKE based on (Ring) Learning with Rounding // Round 5. Available from: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions> [Accessed 14th November 2021]
17. Vlasenko A.V., Evsyukov M.V., Putyato M.M., Makaryan A.S. Research of Key Encapsulation Mechanisms Based on Postquantum Cryptographic Algorithms. *Caspian journal: Management and High Technologies*. 2019;4(48):121–127. (in Russ.) DOI:10.21672/2074-1707.2019.48.4.121-127
18. Nist software performance tests. SAFECrypto. Available from: <https://www.safecrypto.eu/pqclounge> [Accessed 14th November 2021]

Сведения об авторах:

ВЛАСЕНКО
Александра Владимировна

кандидат технических наук, профессор, заведующая кафедрой «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, alex.vlasenko@list.ru
 <https://orcid.org/0000-0002-4134-4980>

ЕВСЮКОВ
Михаил Витальевич

аспирант кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, michael.evsyukov@gmail.com

ПУТЯТО
Михаил Михайлович

кандидат технических наук, доцент, доцент кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, putyato.m@gmail.com
 <https://orcid.org/0000-0001-9974-7144>

МАКАРЯН
Александр Самвелович

кандидат технических наук, доцент, доцент кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, msanya@yandex.ru
 <https://orcid.org/0000-0002-1801-6137>

Метод оценки устойчивости информационного направления, функционирующего на ресурсах сети связи с отказами

С.А. Иванов¹^{*}

¹Военная академия связи им. С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация

^{*}Адрес для переписки: sa-ivanov@inbox.ru

Информация о статье

Поступила в редакцию 19.10.2021

Поступила после рецензирования 14.11.2021

Принята к публикации 19.11.2021

Ссылка для цитирования: Иванов С.А. Метод оценки устойчивости информационного направления, функционирующего на ресурсах сети связи с отказами // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 85–94. DOI:10.31854/1813-324X-2021-7-4-85-94

Аннотация: В статье представлены основные направления качественной и количественной оценки устойчивости в области инфокоммуникаций, показаны различия в подходах к определению устойчивости. Предложен метод, отличающийся от известных обоснованным применением положений теории случайных импульсных потоков. Обобщенный импульсный поток описывает устойчивость передачи данных в информационном направлении. Метод оценки позволяет учитывать как состояния элементов составного канала, представленные импульсными потоками отказов и восстановлений, так и переходные процессы и подпроцессы информационного обмена (передачи по линии связи, коммутации, хранения в памяти, деструктивных воздействий и др.), представленные отдельными импульсными потоками. Вариативность состава импульсных потоков позволяет повышать точность и достоверность оценки.

Ключевые слова: устойчивость, информационное направление, сеть связи с отказами, импульсный поток.

Важным аспектом при эксплуатации инфокоммуникационных систем является обеспечение процессов передачи данных с требуемым качеством в обслуживаемых информационных направлениях. Элементы сетей связи, задействованные при построении маршрутов информационных направлений, могут быть подвержены внутренним и внешним деструктивным воздействиям непреднамеренного и преднамеренного характера. Наиболее емким интегральным свойством, отражающим реакцию системы на воздействие деструктивных факторов, является ее устойчивость. Обеспечение функционирования информационных направлений с заданными требованиями обуславливает необходимость поддержания показателей их устойчивости в заданном диапазоне значений, что требует достоверной оценки ее показателей.

Теория устойчивости в области инфотелекоммуникаций и ее количественной оценки развивается в ряде направлений, основными из которых являются: надежность и живучесть; структурная устойчивость; функциональная динамическая устойчивость.

К направлению надежности и живучести информационно-телекоммуникационных систем (ИТКС) относятся работы Б.Я. Дудника, В.Ф. Овчаренко [1], Б.П. Филина [2], Е.В. Гречишникова, А.С. Белова, А.В. Скубьева [3], К.А. Батенкова [4], В.Г. Иванова [5].

К направлению структурной устойчивости ИТКС относятся работы А.А. Привалова [6], Е.Е. Исакова [7], Ю.Ю. Громова [8], В.К. Попкова [9], J. Park [10], W. Jansen [11], N. Bartol [12].

К направлению функциональной динамической устойчивости ИТКС относятся работы Ю.И. Стародубцева [13], А.Н. Буренина, К.Е. Легкова [14], С.И. Макаренко [15, 16], М.А. Коцыняк, А.И. Осадчего [17], О.С. Лауты [17, 18], I. Linkov [10, 19, 20] P. Bocchini, [21], A. Ganin [20], D. Bodeau [22], И.В. Котенко, И.Б. Саенко [18], А.Е. Кучерявого [23].

Следует отметить, что в работах разных научных школ используются различные определения устойчивости, например:

– устойчивость как способность системы связи выполнять свои функции в условиях воздействия на ее элементы различных видов дестабилизирующих факторов [1, 2, 4–9, 14–16];

– устойчивость как состояние любых свойств системы, характеризующее вероятность нахождения их показателей в заданный период времени в пределах, обеспечивающих требуемый режим функционирования элементов системы и системы в целом [3, 13];

– устойчивость как способность системы планировать и подготавливаться к реагированию, компенсации и восстановлению после деструктивных воздействий и адаптироваться к новым условиям [10–12];

– устойчивость как способность предвидеть, продолжать действовать, корректно преодолевать трудности, восстанавливаться и развиваться с целью успешной адаптации к угрозам [22];

– оценка устойчивости основана на критических функциях и особенностях внешних воздействий на элементы сети [10, 19–21];

– рассматривается устойчивость с акцентом на информационно-технические воздействия [17, 18].

В части работ сохраняется подход, ориентированный на оценку и обеспечение устойчивости аналоговых сетей. В других работах разрабатываются методы и способы обеспечения киберустойчивости без учета, или с ограниченным учетом, ее взаимовлияний с другими свойствами. В третьей группе работ подходы к обеспечению устойчивости основаны на управлении другими свойствами, и, как правило, одним. Особенно необходимо отметить тот факт, что данные труды, опираясь на различные определения устойчивости в качестве основного ресурса сетей связи приняли пропускную способность линий связи.

Основные идеи методов и способов оценки устойчивости [1–25] базируются на классических теоремах сложения и умножения теории вероятностей, при этом вероятности функционирования элементов сети не учитывают распределение времени интервалов отказов во времени: значения коэффициентов готовности (исправного действия) принимаются на длительном временном интервале, исходя из надежных характеристик оборудования, а внешние деструктивные воздействия учтены загруженными коэффициентами, исходя из эмпирических результатов, что снижает достоверность оценки. Кроме того, такая оценка не учитывает время, необходимое для переключения информационных направлений с одного маршрута на другой при неисправности первого.

Таким образом, существует задача разработки методического инструмента для решения класса задач по оценке устойчивости протекающих в информационно-коммуникационных системах процессов, который позволит учитывать динамику деструктивных воздействий на сетевые элементы на протяжении интервалов любой продолжительности T , а также время δ , необходимое для переключения информационных направлений с одного маршрута на другой.

Результатом решения этой задачи стал метод оценки устойчивости информационного направления, представленный в статье. Данный метод основан на реализации положений теорий графов, случайных импульсных потоков, случайных процессов, комбинаторики, дифференциального и интегрального исчисления.

Постановка задачи

Пусть заданы:

– сеть связи (рисунок 1), описываемая графом G , состоящим из элементов k (узлов связи g и линий связи c);

– узлы подключения корреспондентов информационного направления I и требования к процессу передачи данных в нем (пропускной способности $C_{тр}$ и времени передачи $t_{тр}$);

– поток воздействий на каждый k -й элемент сети связи, описываемый плотностью вероятности пауз между импульсами воздействий $\omega_k(u)$;

– подсистемы восстановления элементов сети, описываемые плотностью вероятности времени восстановления элементов $\omega_k(t_b)$.

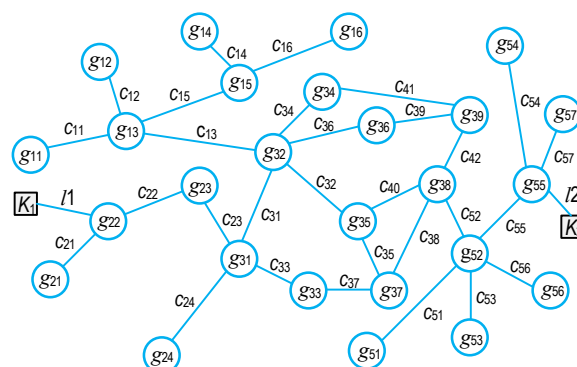


Рис. 1. Пример графа G сети связи, с подключенными посредством линий доступа $I1$ и $I2$, корреспонденты $K1$ и $K2$, между которыми сформировано информационное направление I_{12}

Fig. 1. An Example of a Graph G of a Communication Network with Connected Via Access Lines $I1$ and $I2$, Correspondents $K1$ and $K2$ between which an Information Direction is Formed I_{12}

Распределения $\omega_k(u)$ и $\omega_k(t_b)$ позволяют однозначно определить математическое ожидание соответствующих показателей и среднюю частоту потока отказов [26].

Для обеспечения функционирования информационного направления используются элементы сети, через которые могут проходить маршруты передачи данных (рисунок 2). На основе этих элементов формируется сеть информационного направления, описываемая графом G_I . На основе сети с графом G_I может быть построено M маршрутов, каждый из которых отличается хотя бы одним элементом. Каждый m -й маршрут формирует составной канал в информационном направлении I , включающий простые каналы (в данном случае понятия простой канал и линия связи c – тождественны), скоммутированные на узлах связи g (рисунок 3).

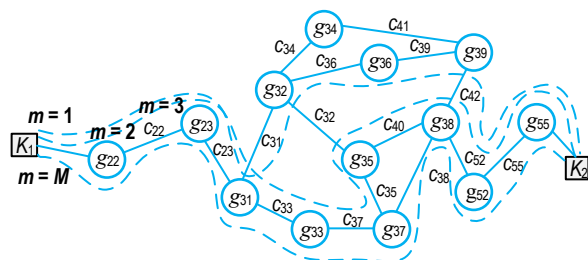


Рис. 2. Пример графа G_1 сети связи информационного направления I_{12}

Fig. 2. An Example of a Graph G_1 of a Communication Network of Information Direction I_{12}

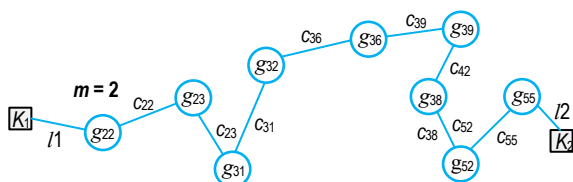


Рис. 3. Пример графа маршрута ($m = 2$) информационного направления I_{12}

Fig. 3. An Example of a Route Graph ($m = 2$) of Information Direction I_{12}

Цель метода: оценить вероятность функционирования информационного направления в сети связи с отказами описываемой графом G_I и образующей M маршрутов передачи данных в информационном направлении, для переключения между которыми необходимо время не более δ .

Суть метода заключается в поиске между корреспондентами информационного направления в любой момент времени хотя бы одного составного канала в сети, характеристики которого удовлетворяют требованиям информационного обмена, при этом интервалы работоспособности составных каналов должны пересекаться на время не меньше, чем необходимо для переключения потока данных между ними. Т. е. определяется, с какой вероятностью в случайный момент времени ζ будет существовать укороченный на δ временной интервал τ работоспособности хотя бы одного маршрута $P(\tau \geq \delta)$.

Обоснование применения теории случайных импульсных потоков

Примем *допущение* о том, что любой элемент сети связи в исправном состоянии удовлетворяет требованиям обмена данными в информационном направлении. Тогда процесс функционирования элемента с точки зрения обеспечения информационного обмена можно рассматривать в виде потока прямоугольных импульсов $X_k(t)$, который описывает элемент в двух состояниях $\xi_k \in \{0,1\}$. Значение $\xi_k = 0$ будем ставить в соответствие неработоспособному состоянию элемента в течение времени восстановления t_b , а значение $\xi_k = 1$ – работоспособному в течение времени его исправной работы τ .

В соответствии с принципами системного анализа и синтеза [27], подобные состояния $\xi_m \in \{0,1\}$ будут определять функционирование маршрутов информационного направления (их потоки прямоугольных импульсов $X_m(t)$), входящих в сеть информационного направления и самого информационного направления $\xi_I \in \{0,1\}$ (потока прямоугольных импульсов $X_I(t)$) (рисунк 4), где $\xi_I = 1$ соответствует состоянию, при котором требуемая для передачи данных в информационном направлении пропускная способность $C_{тр}$ не меньше пропускной способности динамического составного канала C .

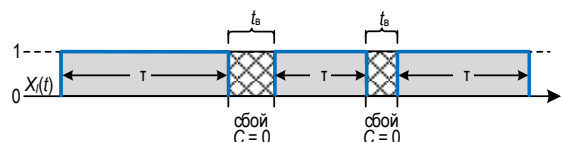


Рис. 4. Графическое отображение реализации процесса функционирования информационного направления I как случайного потока прямоугольных импульсов $X_I(t)$

Fig. 4. Graphic Display of the Implementation of the Process of Functioning of the Information Direction I as a Random Stream of Rectangular Pulses $X_I(t)$

Импульсный поток состояния элемента сети $X_k(t)$ *стационарен*: примем, что деструктивные воздействия на элементы сети связи носят случайный характер, т. е. вероятность отказа в случайно выбранном интервале $(\zeta, \zeta + \Delta t)$ не зависит от отказов на других интервалах.

Импульсный поток состояния элемента сети состоит из *взаимно неперекрывающихся* импульсов – элемент либо исправен, либо нет (отказ):

$$T_{zi} = t_{zi} - t_{zi-1} > \tau_i. \quad (1)$$

Импульсные потоки состояний элементов сети *независимы*: данное утверждение также основано на допущении о случайности деструктивных воздействий на элементы сети.

Импульсные потоки состояний маршрутов $X_m(t)$ информационного направления *независимы*: различные маршруты отличаются хотя бы одним элементом. Если формируемый импульсный поток маршрута отличается от потока другого маршрута хотя бы одним случайным составляющим потоком, то их импульсные потоки этих маршрутов независимы.

Представление процесса передачи данных в информационном направлении рядом *стационарных* и *независимых* импульсных потоков, каждый из которых удовлетворяет условию (1), дает основание для применения положений теории случайных импульсных потоков [28, 29].

Обобщенный показатель устойчивости информационного направления находится в условиях классической постановки теоремы о повторении опытов (схемы Бернулли) на общий случай [30].

Структура метода

Очевидно, что для выполнения требования к устойчивости P_y передачи с $t_{\text{тр}}$ данных в информационном направлении на интервале времени T должно выполняться условие:

$$P_{\xi_I=1} \geq P_y. \quad (2)$$

Вероятность $P_{\xi_I=1}$ в течение T будет определяться характеристиками элементов сети, на основе которых в множестве $\{M\}$ маршрутов формируются составные каналы в информационном направлении, характеристиками потоков воздействий на элементы сети, а также временем δ , необходимым для переключения информационного направления между маршрутами.

Отказ передачи данных в текущем маршруте информационного направления определяет необходимость переключения на другой, работоспособный маршрут. Сеть информационного направления с отказами, описываемая графом G_I , может функционировать с требуемой устойчивостью при условии наличия в любой момент интервала T работоспособного маршрута (составного канала) с вероятностью, удовлетворяющей условию (2). В результате переключения в I составных каналов по причине отказов в информационном направлении формируется *динамический составной канал*.

Метод оценки устойчивости информационного направления проводится в три этапа (рисунок 5).

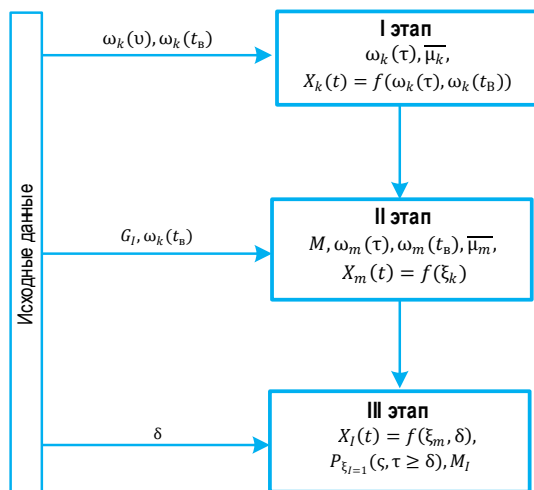


Рис. 5. Структура метода оценки устойчивости информационного направления

Fig. 5. Structure of the Stability Assessment Method Information Direction

На первом этапе оцениваются импульсные вероятностно-временные характеристики состояния $X_k(t) = f(\omega_k(\tau), \omega_k(t_B))$ всех элементов сети, описываемых графом G_I . На втором этапе оцениваются импульсные вероятностно-временные характеристики состояния $X_m(t) = f(\xi_k)$ каждого возможного маршрута (составного канала) информацион-

ного направления. Последовательность расположения элементов в маршруте предопределяет возможность существования импульса в потоке $\xi_m = 1$ только при существовании импульса в потоках каждого элемента составного канала $\xi_k = 1$. На третьем этапе оценивается импульсная вероятностно-временная характеристика состояния импульсного потока $X_I(t) = f(\xi_m, \delta)$, являющаяся обобщенной характеристикой его устойчивости.

Логическая параллельность функционирования маршрутов предопределяет возможность существования импульса в потоке информационного направления при существовании импульса хотя бы в одном (любом) потоке маршрутов $\forall \xi_m = 1$.

Описание метода

На **первом этапе** необходимо найти плотность вероятности длительности интервалов исправной работы (импульсов потока) элементов сети связи $\omega_k(\tau)$ и среднюю частоту следования интервалов исправной работы элементов сети связи $\overline{\mu}_k$. Имеющиеся характеристики элементов сети $\omega_k(v)$, $\omega_k(t_B)$, задействованных в обеспечении функционирования информационного направления, позволяют найти вышеуказанную плотность этих элементов.

Учитывая, что импульс воздействия входит в интервал неисправной работы элемента – времени его восстановления (рисунок 6), интервал его исправной работы можно найти из условия:

$$\tau = v - t_B. \quad (3)$$

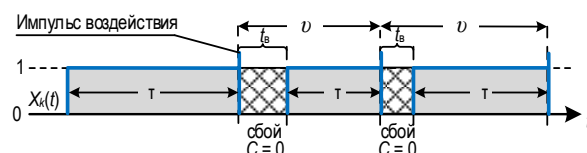


Рис. 6. Графическое отображение реализации процесса функционирования k -го элемента сети связи как случайного потока прямоугольных импульсов $X_k(t)$

Fig. 6. Graphic Display of the Implementation of the Process of Functioning of the k -th Element of the Communication Network as a Random Stream of Rectangular Pulses $X_k(t)$

С учетом независимости времени восстановления и интервалов между импульсами воздействия, нахождение закона распределения интервала исправной работы сводится к составлению композиции законов распределения v и t_B :

$$\begin{aligned} \omega_k(\tau) &= \int_0^{\infty} \omega_k(v) \omega_k(v - \tau) dv = \\ &= \int_0^{\infty} \omega_k(t_B) \omega_k(t_B + \tau) dv. \end{aligned} \quad (4)$$

Средняя частота следования интервалов исправной работы элементов сети находится по формуле:

$$\overline{\mu}_k = \frac{1}{\tau_k + t_{Bk}}, \quad (5)$$

где $\overline{\tau}_k$ и $\overline{t_{Bk}}$ – математическое ожидание интервала исправной работы и времени восстановления k -го элемента, соответственно, которые определяются выражениями [31]:

$$\overline{\tau}_k = \int_0^{\infty} \tau \cdot \omega_k(\tau) d\tau, \quad (6)$$

$$\overline{t_{Bk}} = \int_0^{\infty} t_B \cdot \omega_k(t_B) dt_B. \quad (7)$$

На **втором этапе** по установленному алгоритму (например, алгоритм поиска максимальных паросочетаний, алгоритм поиска кратчайших маршрутов [23, 32, 33]) и критериям определяются все возможные маршруты информационного направления, образующие соответствующие составные каналы передачи данных из K_m элементов сети. В предельном случае количество маршрутов соответствует всем возможным вариантам, отличающихся хотя бы одним элементом.

Каждый составной канал, в зависимости от комбинации простых каналов, имеет поток отказов (пауз, восстановлений) (рисунок 7), характеризующихся плотностью вероятности длительности интервалов исправной работы и восстановления.

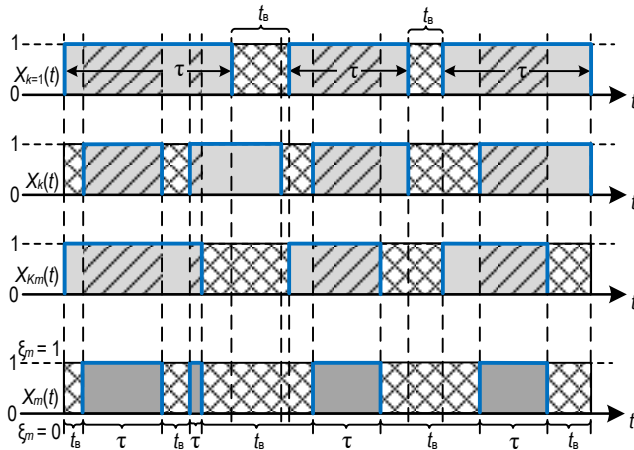


Рис. 7. Графическое отображение реализации процесса функционирования составного канала связи m -го маршрута как случайного потока прямоугольных импульсов $X_m(t)$, сформированного в результате последовательного объединения потоков прямоугольных импульсов элементов сети $X_k(t)$

Fig. 7. Graphic Display of the Implementation of the Process of Functioning of the Composite Communication Channel of the m -th Route as a Random Stream of Rectangular Impulses $X_m(t)$, Formed as a Result of Sequential Combination of Streams of Rectangular Pulses of Network Elements $X_k(t)$

На данном этапе необходимо для каждого маршрута найти, с какой вероятностью в случайный момент времени ζ будет существовать интервал его исправной работы – $P_m(\tau)$:

– плотность вероятности длительности интервалов исправной работы (импульсов потока) маршрутов информационного направления $\omega_m(\tau)$;

– плотность вероятности длительности времени восстановления (пауз потока) маршрутов информационного направления $\omega_m(t_B)$;

– среднюю частоту следования интервалов исправной работы маршрутов информационного направления $\overline{\mu}_m$.

Последовательность расположения элементов в маршруте предопределяет возможность существования импульса в его потоке только при существовании импульса в потоках каждого элемента составного канала.

В этом случае вероятность исправной работы маршрута будет определяться без учета δ выражением [28], которое по сути является формулой Бернулли, расширенной на общий случай решения задачи о повторении независимых испытаний [30]:

$$P_m(\tau) = P_{K_m, K_m}(\tau) = \frac{1}{K_m!} \frac{d^{K_m}}{d\lambda^{K_m}} \prod_{k=1}^{K_m} [Q_k(\tau) + \lambda \cdot P_k(\tau)]_{\lambda=0}, \quad (8)$$

где $P_k(\tau)$ и $Q_k(\tau)$ – вероятность существования и отсутствия импульса в потоке состояния k -го элемента сети, относящегося к m -му маршруту, которые находятся в соответствии с выражениями [28]:

$$P_k(\tau) = \overline{\mu}_k \int_0^{\infty} \tau \cdot \omega_k(\tau) d\tau, \quad (9)$$

$$Q_k(\tau) = \overline{\mu}_k \int_0^{\infty} t_B \cdot \omega_k(t_B) dt_B \quad (10)$$

и связаны между собой соотношением:

$$Q_k(\tau) = 1 - P_k(\tau). \quad (11)$$

Средняя частота следования импульсов совпадения маршрута определяется выражением [28]:

$$\overline{\mu}_m = \overline{\mu}_{K_m, K_m} = \frac{P_{K_m, K_m}(\tau)}{\tau_{K_m, K_m}}, \quad (12)$$

где τ_{K_m, K_m} определяется как:

$$\tau_{K_m, K_m} = \left(\sum_{k=1}^{K_m} \frac{1}{\tau_k} \right). \quad (13)$$

Распределение длительности интервалов исправной работы (импульсов потока) маршрутов определяется плотностью вероятности [28]:

$$\omega_m(\tau) = \omega_{K_m, K_m}(\tau) = \overline{\mu}_m \frac{d^2}{d\tau^2} P_m(\tau), \quad (14)$$

а распределение длительности времени восстановления (пауз потока) маршрутов (с учетом последовательной схемы подключения элементов) определяется плотностью вероятности [28]:

$$\omega_m(t_B) = \omega_{K_m, 1}(t_B) = \overline{\mu}_m \frac{d^2}{dt_B^2} P_m(t_B), \quad (15)$$

где

$$P_m(t_B) = P_{K_{m,1}}(t_B) = \frac{d}{d\lambda} \prod_{k=1}^{K_m} [P_k(\tau) + \lambda \cdot Q_k(\tau)]_{\lambda=0}. \quad (16)$$

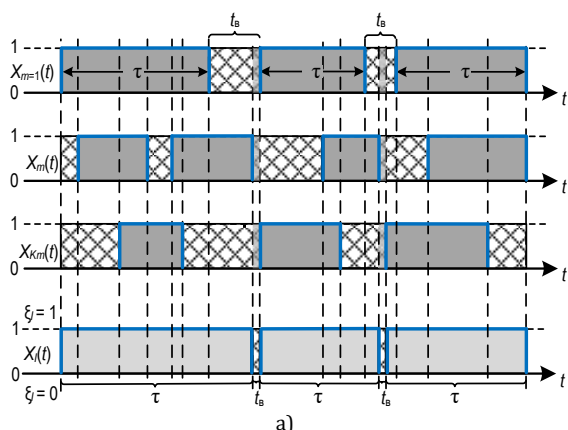
Третий этап. Рассмотрим оценку устойчивости в трех вариантах функционирования динамического составного канала: при мгновенном переключении между составными каналами, удовлетворяющими требованиям информационного направления (ИН); при переключении между составными каналами, удовлетворяющими требованиям ИН с учетом переходных процессов в ходе переключения; при переключении между составными каналами, каждый из которых по отдельности не удовлетворяет требованиям ИН с учетом переходных процессов в ходе переключения.

Оценка устойчивости при мгновенном переключении между составными каналами, удовлетворяющими требованиям ИН

При параллельном соединении M составных каналов (маршрутов) в информационное направление наличие импульса хотя бы в одном (любом) канале $\xi_m = 1$ будет соответствовать наличию импульса $\xi_I = 1$ в потоке динамического составного канала информационного направления (рисунок 8а).

В этом случае вероятность существования импульса в потоке состояния ИН будет определяться выражением:

$$P_{\xi_I=1} = P_{M,1}(\tau) = \frac{d}{d\lambda} \prod_{m=1}^M [Q_m(\tau) + \lambda \cdot P_m(\tau)]_{\lambda=0} \omega_m(t_B) = \omega_{K_{m,1}}(t_B) = \overline{\mu}_m \frac{d^2}{d\tau^2} P_m(t_B), \quad (17)$$



где $P_m(\tau)$ и $Q_m(\tau)$ – вероятность существования и отсутствия импульса в потоке состояния m -го маршрута ИН, которые по аналогии с (9) и (10) находятся в соответствии с выражениями:

$$P_m(\tau) = \overline{\mu}_m \int_0^\infty \tau \cdot \omega_m(\tau) d\tau, \quad (18)$$

$$Q_m(\tau) = \overline{\mu}_m \int_0^\infty t_B \cdot \omega_m(t_B) dt_B. \quad (19)$$

Оценка устойчивости при переключении между составными каналами, удовлетворяющими требованиям ИН с учетом переходных процессов в ходе переключения

Переключение информационного направления между маршрутами сопровождается переходными процессами, занимающими время не менее некоторого значения δ . Для учета этих процессов при оценке устойчивости направления, необходимо укорачивать на величину δ импульсы совпадения потоков состояния составных каналов (рисунок 8б).

Тогда выражение (17) примет вид:

$$P_{\xi_I=1} = P_{M,1}(\delta) = \frac{d}{d\lambda} \prod_{m=1}^M [Q_m(\delta) + \lambda \cdot P_m(\delta)]_{\lambda=0}, \quad (20)$$

где $P_m(\delta)$ и $Q_m(\delta)$ – вероятность существования и отсутствия укороченного на δ импульса в потоке состояния m -го маршрута информационного направления, которые по аналогии с (9) и (10) находятся в соответствии с выражениями:

$$P_m(\delta) = \overline{\mu}_m \int_0^\infty (\tau - \delta) \cdot \omega_m(\tau) d\tau, \quad (21)$$

$$Q_m(\delta) = \overline{\mu}_m \int_0^\infty (t_B - \delta) \cdot \omega_m(t_B) dt_B. \quad (22)$$

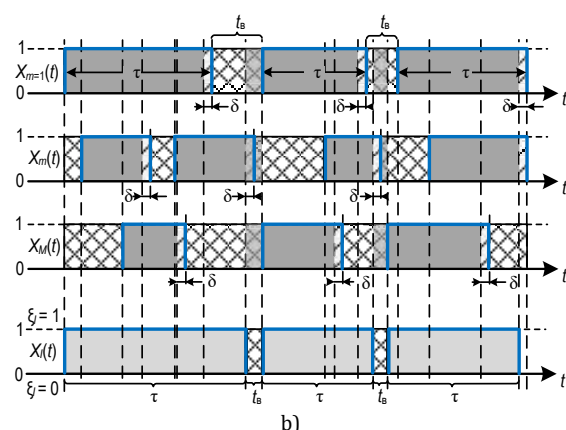


Рис. 8. Графическое отображение реализации функции состояний процесса передачи данных в информационном направлении $X_I(t)$, полученной в результате объединения параллельных потоков прямоугольных (полноразмерных) импульсов $X_m(t)$ (а) и импульсов, укороченных на δ (б), соответствующих состояниям процесса функционирования составных каналов M маршрутов

Fig. 8. Graphical Display of the Function's Implementation of the States of the Data Transfer Process in the Information Direction $X_I(t)$, Obtained as a Result of Combining Parallel Flows of Rectangular (Full-Size) Pulses $X_m(t)$ (a) and Pulses Shortened by δ (b), Corresponding to the States of the Process of Functioning of Composite Channels of M Routes

Оценка устойчивости при переключении между составными каналами, каждый из которых по отдельности не удовлетворяет требованиям ИН с учетом переходных процессов в ходе переключения

Представляя состояние составного канала m -го маршрута потоком импульсов $X_m(t)$ с амплитудой равной единице ($\xi_m = 1$), состояние ИН, включающего M маршрутов, можно представить суммой (рисунок 9):

$$X_I(t) = \sum_{m=1}^M X_m(t). \quad (23)$$

Тогда $X_I(t)$ может принимать целочисленные значения от 0 до M , что будет соответствовать событиям от полного отсутствия маршрута с заданными требованиями в информационном направлении до работоспособности любого из M маршрутов с заданными требованиями.

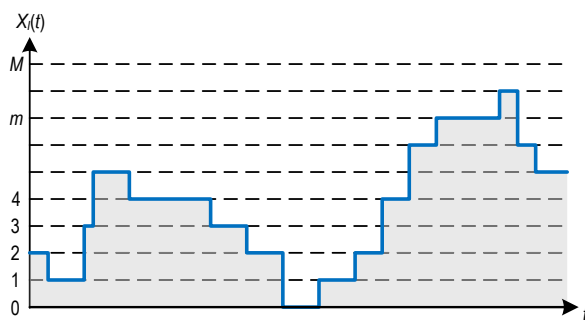


Рис. 9. Вариант функции $X_I(t)$ состояний процесса передачи данных в информационном направлении, включающем M маршрутов

Fig. 9. A Variant of the Function $X_I(t)$ of the States of the Data Transfer Process in the Information Direction, Including M Routes

По условиям задачи, для обеспечения функционирования ИН достаточно наличия импульса в любой момент времени в составном канале хотя бы в одного маршрута. При допущении того, что наличие импульса соответствует только части требуемой пропускной способности для передачи данных в ИН, необходимо оценить вероятность существования укороченного на δ импульса совпадения M_I маршрутов (рисунок 9):

$$M_I \geq \left\lceil \frac{C_{\text{тр}}}{C} \right\rceil, \quad (24)$$

где $M_I \in \mathbb{N}$.

Тогда выражение (17) примет вид:

$$P_{\xi_I=1} = P_{M, M_I}(\delta) = \frac{1}{M_I!} \frac{d^{M_I}}{d\lambda^{M_I}} \prod_{m=1}^M [Q_m(\delta) + \lambda \cdot P_m(\delta)]_{\lambda=0}. \quad (25)$$

Решение задачи обеспечения устойчивости обмена данных в ИН сводится к нахождению численными методами по выражению (25) необходимого количества маршрутов для выполнения условий (2) и (24).

Достоверность метода

По сравнению с традиционными методами, использующими средневзвешенную оценку (коэффициенты готовности и оперативной готовности), повышение достоверности и точности оценки устойчивости в разработанном методе обусловлено:

- учетом распределения времени отказов (состояния элемента по отношению к требованиям информационного обмена) каждого элемента сети на всем интервале оценки;
- учетом времени, необходимого для переключения между составными каналами различных маршрутов.

Кроме того, дополнительными импульсными потоками можно представлять задержки, вызываемые обработкой заголовков, очередями при отказах и перегрузках каналов, внешними и внутренними деструктивными воздействиями, линейным кодированием/декодированием и т. д. Такая возможность указывает на высокую чувствительность метода оценки устойчивости ИН к изменениям внутренних и внешних условий функционирования сети связи.

Достоверность представленного метода оценки подтверждается применением апробированных положений теорий графов, случайных импульсных потоков, случайных процессов, комбинаторики, дифференциального и интегрального исчисления.

Заключение

Метод оценки устойчивости направлен на определение в любой момент времени вероятности исправного функционирования ИН в зависимости от вероятностно-временных характеристик состояния элементов сети связи и характеристик подпроцессов информационного обмена.

Основным отличием метода от известных и его научной новизной является обоснованное применение положений теории случайных импульсных потоков, позволяющей совместно с традиционными методами, используемыми при оценке устойчивости, учитывать ключевые традиционные и дополнительные характеристики сети в условиях деструктивных воздействий.

Для повышения точности и достоверности оценки устойчивости метод позволяет представить подпроцессы информационного обмена (например, передачи по линии связи, коммутации, хранения в памяти) отдельными импульсными потоками. Представленный в статье результат учитывает время, необходимое для переключения составных каналов связи при управлении конфигурацией динамического составного канала ИН. Переключение составных каналов также можно представить отдельным импульсным потоком.

Вариативность состава импульсных потоков, включенных в общий поток, описывающий устойчивость передачи данных в ИН, позволяет повышать точность и достоверность оценки, масштабировать при этом перечень учитываемых показателей, выявлять пути повышения устойчивости информационного обмена.

Практическое применение представленного метода оценки требует дальнейшей проработки:

- порядка адаптации метода к внутренним и внешним условиям функционирования объекта оценки;
- порядка получения данных о внутренних параметрах сети связи;
- оптимизации периодичности контроля параметров сети связи;
- мониторинга состояния кабельной инфраструктуры в условиях внешних физических деструктивных воздействий.

Список используемых источников

1. Дудник Б.Я., Овчаренко В.Ф., Орлов В.К. и др. Надежность и живучесть систем связи. М.: Радио и связь, 1984. 216 с.
2. Филин Б.П. Методы анализа структурной надежности сетей связи. М.: Радио и связь, 1988. 208 с.
3. Гречишников Е.В., Белов А.С., Скубьев А.В. Способ обеспечения живучести сети связи в зоне обслуживания подвижных абонентов // Телекоммуникации. 2016. № 7. С. 13–18.
4. Батенков К.А. Устойчивость сетей связи: учебное пособие. Орел: Академия ФСО России, 2016. 278 с.
5. Иванов В.Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи. СПб.: СПбПУ, 2018. 214 с.
6. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб.: ВМА, 2000. 240 с.
7. Исаков Е.Е. Устойчивость военной связи в условиях информационного противоборства. СПб.: Изд-во Политехнического университета, 2009. 400 с.
8. Громов Ю.Ю., Драчев В.О., Набатов К.А., Иванова О.Г. Синтез и анализ живучести сетевых систем. М.: Изд-во Машиностроение-1, 2007. 152 с.
9. Попков В.К. Математические модели связности. Новосибирск: ИВМиМГ СО РАН, 2006. 490 с.
10. Park J., Seager T.P., Rao P.S.C., Convertino M., Linkov I. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems // Risk Analysis. 2013. Vol. 33. Iss. 3. PP. 356–367. DOI:10.1111/j.1539-6924.2012.01885.x
11. Jansen W. Directions in Security Metrics Research. National Institute of Standards and Technology, 2009. URL: <http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf> (дата обращения 23.11.2021)
12. Bartol N., Bates B., Goertzel K.M., Winograd T. Measuring Cyber Security and Information Assurance: A State-of-the-Art Report. Herndon: Information Assurance Technology Analysis Center, 2009.
13. Стародубцев Ю.И., Иванов С.А., Закалкин П.В. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации в интересах органов государственной власти и военного управления // Военная мысль. 2021. № 4. С. 39–49.
14. Буренин А.Н., Легков К.Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения управления. М.: Медиа паблишер, 2015. 348 с.
15. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. СПб.: Научное издание, 2020. 337 с.
16. Макаренко С.И. Усовершенствование функций маршрутизации и сигнализации протокола PNNI с целью повышения устойчивости сети связи // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 45–59. DOI:10.31854/1813-324X-2020-6-2-45-59
17. Коцыняк М.А., Осадчий А.И., Коцыняк М.М., Лаута О.С., Дементьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2015. 126 с.
18. Kotenko I., Saenko I., Lauta O. Modeling the Impact of Cyber Attacks // In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Cham: Springer, 2019. PP. 135–169. DOI:10.1007/978-3-319-77492-3_7
19. Linkov I., Eisenberg D.A., Plourde K., Seager T.P., Allen J., Kott A. Resilience metrics for cyber systems // Environment Systems & Decisions. 2012. Iss. 33. PP. 471–476. DOI:10.1007/s10669-013-9485-y
20. Ganin A.A., Massaro E., Gutfraun A., Steen N., Keisler J.M., Kott A., et al. Operational resilience: Concepts, design and analysis // Scientific Reports. 2016. Iss. 6. DOI:10.1038/srep19540
21. Bocchini P., Frangopol D.M., Ummenhofer T., Zinke T. Resilience and Sustainability of Civil Infrastructure: Toward a Unified Approach // Journal of Infrastructure Systems. 2014. Vol. 20. Iss. 2.
22. Bodeau D., Graubart R., Heinbockel W., Laderman E. Cyber Resiliency Engineering Aid – The Updated Cyber Resilience Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. Bedford: MITRE Corporation, 2015. URL: <https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf> (дата обращения 23.11.2021)
23. Кучерявый А.Е., Махмуд О.А., Парамонов А.И. Метод маршрутизации трафика в сети Интернета Вещей на основе минимума вероятности коллизий // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 37–44. DOI:10.31854/1813-324X-2019-5-3-37-44
24. ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. М.: Стандартинформ, 2009. 16 с.

25. Казаченко Ю.М., Патрина Н.С. Методическое обеспечение устойчивого функционирования сетей связи в условиях ЧС // Т-Сот: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 26–30.
26. Вадзинский Р.Н. Справочник по вероятностным распределениям. СПб.: Наука, 2001. 295 с.
27. Попов А.А., Телушкин С.Н., Бушуев С.Н. Основы общей теории систем. Часть I. СПб.: ВАС, 1992. 248 с.
28. Седякин Н.М. Элементы теории случайных импульсных потоков. М.: Советское радио, 1965. 261 с.
29. Смагин В.А. Вероятностные модели сложных систем. СПб.: ВКА им. А.Ф. Можайского, 2004. 171 с.
30. Венцель Е.С. Теория вероятностей. М.: Государственное издание физико-математической литературы, 1962. 564 с.
31. Половко А.М., Гуров С.В. Основы теории надежности. СПб.: БХВ-Петербург, 2006. 704 с.
32. Харари Ф. Теория графов. Пер. с англ. М.: ЛЕНАНД, 2018. 304 с.
33. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2020. 1008 с.

* * *

Method for Assessing the Sustainability of the Information Direction, Functioning on the Resources of the Communication Network with Failures

S. Ivanov¹ 

¹Military Academy of Communications,
St. Petersburg, 194064, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-85-94

Received 19th October 2021

Revised 14th November 2021

Accepted 19th November 2021

For citation: Ivanov S. Method for Assessing the Sustainability of the Information Direction, Functioning on the Resources of the Communication Network with Failures. *Proc. of Telecom. Universities*. 2021;7(4):85–94. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-85-94

Abstract: *The article presents the main directions of the qualitative and quantitative assessment of sustainability in the field of infocommunications, shows the differences in approaches to the definition of sustainability. A method is proposed that differs from the known well-grounded application of the provisions of the theory of random impulse flows. The generalized impulse flow describes the robustness of data transmission in the information direction. The estimation method allows one to take into account both the states of the elements of a composite channel, represented by impulse flows of failures and restorations, and transient processes and sub-processes of information exchange (transmission over a communication line, switching, storage in memory, destructive influences, etc.), represented by separate impulse streams. The variability of the composition of the impulse streams makes it possible to increase the accuracy and reliability of the assessment.*

Keywords: *stability, information direction, communication network with failures, impulse flow.*

References

1. Dudnik B.Ya., Ovcharenko V.F., Orlov V.K., et al. *Reliability and Survivability of Communication Systems*. Moscow: Radio i sviaz Publ.; 1984. 216 p. (in Russ.)
2. Filin B.P. *Methods for Analyzing the Structural Reliability of Communication Networks*. Moscow: Radio i sviaz Publ.; 1988. 208 p. (in Russ.)
3. Grechishnikov E.V., Belov A.S., Skubiyev A.V. Survivability Support Method of Telecommunication Network in Service Area of Mobile Users. *Telekommunikatsii (Telecommunications)*. 2016;7:13–18. (in Russ.)
4. Batenkov K.A. *Stability of Communication Networks*. Orel: Russian Federation Security Guard Service Federal Academy Publ.; 2016. 278 p. (in Russ.)
5. Ivanov V.G. *Model of the Technical Basis of a Special-Purpose Control System in a Single Information Space Based on the Converged Infrastructure of the Communication System*. St. Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2018. 214 p. (in Russ.)

6. Privalov A.A. *The Method of Topological Transformation of Stochastic Networks and its Use for the Analysis of Communication Systems of the Navy*. St. Petersburg: S. M. Kirov Military Medical Academy Publ.; 2000. 240 p. (in Russ.)
7. Isakov E.E. *Stability of Military Communications in the Context of Information Confrontation*. St. Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2009. 400 p. (in Russ.)
8. Gromov Yu.Yu., Drachev V.O., Nabatov K.A., Ivanova O.G. *Synthesis and Analysis of the Survivability of Network Systems*. Moscow: Mashinostroenie-1 Publ.; 2007. p. 152 (in Russ.)
9. Popkov V.K. *Mathematical Models of Connectivity*. Novosibirsk: Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch of the Russian Academy of Sciences Publ.; 2006. 490 p. (in Russ.)
10. Park J., Seager T.P., Rao P.S.C., Convertino M., Linkov I. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis*. 2013;33(3):356–367. DOI:10.1111/j.1539-6924.2012.01885.x
11. Jansen W. *Directions in Security Metrics Research*. National Institute of Standards and Technology; 2009. Available from: <http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf> [Accessed 23rd November 2021]
12. Bartol N., Bates B., Goertzel K.M., Winograd T. *Measuring Cyber Security and Information Assurance: A State-of-the-Art Report*. Herndon: Information Assurance Technology Analysis Center; 2009.
13. Starodubtsev Y., Ivanov S., Zakalkin P. Conceptual Trends in Solving the Issue of Stability for the Uniform Network of Electrocommunications in the Russian Federation. *Voennaya mysl*. 2021;4:39–49. (in Russ.)
14. Burenin A.N., Legkov K.E. *Modern Infocommunication Systems and Special Purpose Networks. The Basics of Building Management*. Moscow: Media Publ.; 2015. 348 p. (in Russ.)
15. Makarenko S.I. *Communication System Models under the Conditions of Deliberate Destabilizing Influences and Reconnaissance*. St. Petersburg: Naukoemkie tekhnologii Publ.; 2020. 337 p. (in Russ.)
16. Makarenko S. Improved Routing and Signaling Functions of PNNI Protocol for High Network Stability. *Proc. of Telecom. Universities*. 2020;6(2):45–59. (in Russ.) DOI:10.31854/1813-324X-2020-6-2-45-59
17. Kotsynyak M.A., Osadchiy A.I., Kotsynyak M.M., Lauta O.S., Dementyev V.E., Vasyukov D.Yu. Ensuring the Stability of Information and Telecommunication Systems in the Context of Information Confrontation. St. Petersburg: Central Research Institute of Communications Publ.; 2015. 126 p. (in Russ.)
18. Kotenko I., Saenko I., Lauta O. Modeling the Impact of Cyber Attacks. In: Kott A., Linkov I. (eds) *Cyber Resilience of Systems and Networks*. Cham: Springer; 2019. p.135–169. DOI:10.1007/978-3-319-77492-3_7
19. Linkov I., Eisenberg D.A., Plourde K., Seager T.P., Allen J., Kott A. Resilience metrics for cyber systems. *Environment Systems & Decisions*. 2012;33:471–476. DOI:10.1007/s10669-013-9485-y
20. Ganin A.A., Massaro E., Gutfrain A., Steen N., Keisler J.M., Kott A., et al. Operational resilience: Concepts, design and analysis. *Scientific Reports*. 2016;6. DOI:10.1038/srep19540
21. Bocchini P., Frangopol D.M., Ummenhofer T., Zinke T. Resilience and Sustainability of Civil Infrastructure: Toward a Unified Approach. *Journal of Infrastructure Systems*. 2014;20(2).
22. Bodeau D., Graubart R., Heinbockel W., Laderman E. *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. Bedford: MITRE Corporation; 2015. Available from: <https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf> [Accessed 23rd November 2021]
23. Koucheryavy A., Mahmood O.A., Paramonov A. Traffic Routing Method for the Internet of Things Based on the Minimum of Collisions Probability. *Proc. of Telecom. Universities*. 2019;5(3):37–44. (in Russ.) DOI:10.31854/1813-324X-2019-5-3-37-44
24. GOST P 53111-2008. *Stability of functioning of the public communications network. Requirements and check methods*. Moscow: Standartinform Publ.; 2009. 16 p. (in Russ.)
25. Kozachenko Yu.M., Patrino N.S. Methodological support of sustainable operation of communication networks in emergency situations. *T-Comm*. 2017;11(9):26–30. (in Russ.)
26. Vadzinsky R.N. *Probability Distributions Handbook*. St. Petersburg: Nauka Publ.; 2001. 295 p. (in Russ.)
27. Popov A.A., Telushkin S.N., Bushuev S.N. *Foundations of General Systems Theory. Part I*. St. Petersburg: Military Academy of Communications Publ.; 1992. 248 p. (in Russ.)
28. Sedyakin N.M. *Elements of the Theory of Random Impulse Flows*. Moscow: Sovetskoe radio Publ.; 1965. 261 p. (in Russ.)
29. Smagin V.A. *Probabilistic Models of Complex Systems*. St. Petersburg: Mozhaisky Military Space Academy Publ.; 2004. 171 p. (in Russ.)
30. Wenzel E.S. *Probability Theory*. Moscow: Gosudarstvennoe izdanie fiziko-matematicheskoi literatury Publ.; 1962. 564 p. (in Russ.)
31. Polovko A.M., Gurov S.V. *Fundamentals of the Theory of Reliability*. St. Petersburg: BKHV-Peterburg Publ.; 2006. 704 p. (in Russ.)
32. Harari F. *Graph Theory*. Translated from English. Moscow: LENAND Publ.; 2018. 304 p. (in Russ.)
33. Olifer V., Olifer N. *Computer Networks. Principles, Technologies, Protocols*. St. Petersburg: Piter Publ.; 2020. 1008 p. (in Russ.)

Сведения об авторе:

ИВАНОВ
Сергей Александрович

кандидат технических наук, докторант Военной академии связи имени Маршала Советского Союза С. М. Буденного, sa-ivanov@inbox.ru
 <https://orcid.org/0000-0002-0528-276X>

Концепция генетической декомпиляции машинного кода телекоммуникационных устройств

К.Е. Израйлов^{1, 2} 

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,

Санкт-Петербург, 193232, Российская Федерация

²Санкт-Петербургский федеральный исследовательский центр Российской академии наук,

Санкт-Петербург, 199178, Российская Федерация

*Адрес для переписки: konstantin.izrailov@mail.ru

Информация о статье

Поступила в редакцию 01.12.2021

Поступила после рецензирования 20.12.2021

Принята к публикации 21.12.2021

Ссылка для цитирования: Израйлов К.Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 95–109. DOI:10.31854/1813-324X-2021-7-4-95-109

Аннотация: Восстановление корректного исходного кода из машинного в интересах поиска и нейтрализации уязвимостей является актуальнейшей проблемой для области телекоммуникационного оборудования. Применимые для этого техники декомпиляции потенциально достигли своего эволюционного предела. Как результат, требуются новые концепции, способные осуществить качественный скачок в разрешении проблемы. Исходя из этого, в работе предлагается концепция генетической декомпиляции, представляющая собой решение задачи многопараметрической оптимизации в виде итерационного приближения экземпляров исходного кода к «истинному», компилируемому в заданный машинный. Осуществляется проверка данной концепции путем проведения серии экспериментов с разработанным программным прототипом на базовом примере машинного кода. Результаты экспериментов доказывают обоснованность предлагаемой концепции, предполагая тем самым новые инновационные направления обеспечения информационной безопасности в данной предметной области.

Ключевые слова: информационная безопасность, телекоммуникационное оборудование, машинный код, уязвимость, реверс-инжиниринг, декомпиляция, искусственный интеллект, генетический алгоритм, концепция

ВВЕДЕНИЕ

Проблема безопасности телекоммуникационного оборудования актуализировалась в тот же момент, когда для передачи информации стало использоваться программное обеспечение. Причина такой связи заключается в наличии уязвимостей в программном коде, используемом для обработки передаваемых данных. При этом, источник появления уязвимости может быть как случайным (например, ошибка программиста), так и злонамеренным (например, «backdoor»). Вследствие чего телекоммуникационные устройства будут функционировать отличным от изначально задуманного образом, приводя тем самым к классической триаде нарушений информационной безопасности передаваемых данных: конфиденциальности, целостности и доступности. Одним из основных подходов противодействия этому является непосредственный поиск и нейтрализация уязвимостей в программном коде.

Безопасность программного кода

Способы поиска могут носить различный характер, зависящий, в том числе, от точки возникновения уязвимости в программном коде. Например, ее появление при создании архитектуры, реализации алгоритмов или непосредственном переводе кода в бинарное (выполняемое) представление потребует качественно отличных друг от друга способов, имеющих различную эффективность (как совокупность доли выявленных уязвимостей, скорости выявления и затраченных ресурсов). Однако в современных реалиях, когда телекоммуникационное оборудование разрабатывается крупными транснациональными корпорациями, его исходный код (далее – ИК) из соображений «ноу-хау» не предоставляется, а в наличии имеется лишь машинный код (далее – МК). Работа с последним существенно снижает количество применимых способов поиска уязвимостей, основной

причиной чего является практическая невозможность (или по крайней мере, высокая трудоемкость) анализа кода вручную экспертом. Автоматический же поиск [1–3], как правило, позволяет выявлять низкоуровневые уязвимости, затрагивая лишь нижние структурные уровни программы (отдельные выражения, доступ к данным и т. п.) и пропуская наиболее критичные – алгоритмические, архитектурные и концептуальные.

Для расширения использования всего «пула» способов поиска уязвимостей применяется так называемая техника «декомпиляции» (или «реверс-инжиниринга программного кода»), которая и определяет предметную область исследования, изложенного в текущей статье. Суть техники заключается в переводе программного кода из низкоуровневого представления, адаптированного для выполнения автоматом, в высокоуровневое, подходящее для работы с ним человеком [4]. Так, современные декомпиляторы (программные средства, реализующие технику декомпиляции) позволяют преобразовывать МК в некоторый псевдоисходный, из которого гипотетически и был получен данный МК. Стоит отметить, что в полном смысле задача декомпиляции считается нерешаемой, поскольку при компиляции (процессе трансформации ИК в МК) часть метainформации теряется (комментарии, имена переменных, точный вид алгоритмов подпрограмм, архитектура программных модулей и т. п.) и, как следствие, не может быть восстановлена.

Научное противоречие

Несмотря на значительные успехи в исследовании и разработке декомпиляторов, предметная область содержит следующее научное противоречие в виде противопоставления – потребность *vs* возможность.

Потребность. С одной стороны, экспертам для поиска и нейтрализации уязвимостей требуется способ получения ИК, компилируемого в требуемый МК; при этом способ должен быть инвариантным относительно типа процессора выполнения. Первая часть потребности вытекает из того, что, как правило, уязвимость закладывается вручную в момент создания ИК (хотя и может делать небезопасным более высокоуровневые представления программы, такие, как его архитектура или концептуальная модель) [5]. Следовательно, анализ кода, близкого к такому исходному, не только даст эксперту больше информации для поиска уязвимостей, но и позволит ему произвести необходимую модификацию кода, приводящую после компиляции к безопасному МК. Причина второй части потребности заключается в том, что, исходя из огромного количества существующих и постоянно создаваемых процессорных архитектур, адаптация способов декомпиляции под новые процессоры будет не успевать за действиями злоумышленников, эксплуатирующих уязвимости.

Это, в частности, обосновывается общей сложностью решения задачи декомпиляции, что требует огромных ресурсо-временных затрат на разработку программных средств.

Возможность. С другой стороны, существующие декомпиляторы (а также идеи, модели и алгоритмы, лежащие в их основе) предназначены для преобразования МК в ИК, который лишь отражает данный МК, а не стремится соответствовать изначально ИК; при этом, возникновение задачи поиска уязвимостей в МК для нового (например, менее популярного или только что созданного) процессора требует разработки декомпилятора «с нуля». Первая часть возможности вытекает из общего подхода к декомпиляции, когда правила преобразования машинных инструкций в конструкции ИК создаются вручную или полуавтоматически с привлечением ограниченного количества высококвалифицированных экспертов. Причина второй части заключается в том, что каждый такой декомпилятор предназначен для восстановления ИК для одного типа машинных инструкций или их близкого набора.

Разрешение противоречия

Разрешение противоречия возможно лишь гипотетически, поскольку существующие подходы лишь улучшают давно применяемые решения, не предполагая какого-либо качественного (т. е. прорывного) скачка. Таким образом, любые исследования, направленные на создание новых подходов в технике декомпиляции, являются безусловно актуальными.

Исследование в данной статье как раз и направлено на проверку авторской концепции декомпиляции, основанной на качественно новых принципах. Естественно, предлагаемый далее подход проверялся на разработанном прототипе декомпилятора для достаточно простых примеров МК; тем не менее, цель статьи заключается именно в проверке самой концепции; такой процесс доказательства имеет более широко известное название, как – PoC (аббр. от. англ. Proof of Concept). Естественно, описание полноценного решения не предполагается в данной статье, поскольку имеет существенную сложность для реализации. Однако его получение в будущем позволит практически полностью «свести на нет» указанное противоречие предметной области, разрешив тем самым проблему *гарантированной декомпиляции МК для любого типа процессора выполнения*, которая насчитывает уже несколько десятилетий.

ЭВОЛЮЦИЯ ТЕХНИКИ ДЕКОМПИЛЯЦИИ

Прежде чем описать предлагаемый программный прототип и провести с его помощью проверку концепции, рассмотрим общие этапы эволюции техник декомпиляции, которая послужила предпосылкой для возникновения новой концепции декомпиляции.

Первый этап

На первом этапе решение задачи преобразования МК в ИК производилось экспертами вручную – как ментально, так и с текстово-графическим отображением логики программы в виде блок-схем. Недостатками такого подхода были низкая скорость работы, высочайшие затраты ресурсов (в основном, человеческих) и как результат, большое количество ошибок.

Второй этап

На втором этапе, возникшем вследствие повышения производительности программно-аппаратного обеспечения, стали разрабатываться алгоритмы автоматического преобразования как отдельных блоков машинных инструкций, так и целых их структур, включая даже типы переменных [6]. В этот момент стали появляться первые программные реализации декомпиляторов. Однако, несмотря на существенно выросшую скорость применения способов (до нескольких секунд или минут), при снижении требований к экспертам, анализирующим получаемый ИК, существенного роста эффективности не произошло. Причина этого заключается в том, что разработка самих программных решений оказалась крайне сложной задачей. Также, поскольку алгоритмы преобразования МК в ИК создавались вручную, то росли и ошибки декомпиляции; или же процесс восстановления работал некорректно для непредвиденных входных данных.

Третий этап

На текущий момент, с точки зрения автора, идет третий этап развития техники декомпиляции, который ознаменован повсеместным внедрением искусственного интеллекта. Суть его применения к текущей задаче может заключаться в избавлении человека от необходимости создания всех правил преобразования МК в ИК вручную [7]. При этом, участие человека все равно будет требоваться – для обучения таких интеллектуальных систем или постобработки их результатов. И несмотря на большой потенциал в интеллектуализации подходов [8], суть остается та же – в конечном итоге необходимо создание правил, которые как требуют участия эксперта [9], так и не стремятся получить начальный ИК. При этом процесс обучения и доработки необходимо производить для каждого нового процессора выполнения заново.

Четвертый этап...?

Исходя из общей тенденции этапов эволюции техник декомпиляции, можно спрогнозировать постепенное и вынужденное сокращение участия человека в процессе, полностью отдавая выполнение процесса на откуп автомату (за счет продолжающегося роста аппаратных мощностей современной техники, включая появление суперкомпьютеров,

облачных сервисов, распараллеливание вычислений и т. п.). Как результат, должны появиться способы декомпиляции, позволяющие не только снизить потребность в экспертном мнении, но и даже полностью отказаться от него. Именно такая авторская концепция, а также ее подтверждение, и будет продемонстрирована далее.

ГЕНЕТИЧЕСКИЙ АЛГОРИТМ

Идея качественно нового подхода в декомпиляции была описана автором ранее в работе [10]. Суть ее сводится к тому, что не МК преобразуется в ИК, а производится постепенный (многошаговый) поиск ИК, компилируемого в требуемый МК, или максимально близкий к нему. Таким образом, решается задача многопараметрической оптимизации, для чего предлагается использовать генетический алгоритм [11] – аналог происходящих механизмов эволюции в живой природе, хорошо себя зарекомендовавший для подобного рода задач. Суть алгоритма заключается в итеративном подстраивании популяции особей к среде существования путем их мутации, скрещивания и селекции. Принципы работы алгоритма хорошо известны и не требуют дополнительного объяснения. Способ же на базе данного алгоритма назван автором, как «генетическая декомпиляция», что полностью отражает его суть. Стоит отметить, что перенесение особенностей функционирования живой природы в сферу информационных технологий набирает все большую популярность, обосновывая тем самым эффективность такого рода подходов [12].

Разрешение противоречия

Рассмотрим, как повлияет доведение идеи генетической декомпиляции для полноценной реализации на разрешение обозначенного противоречия, и связанную с ним научную проблему.

Во-первых, в результате применения такого способа будет получаться ИК, который гарантированно компилируется в МК – сглаживание частного противоречия между первыми частями потребности и возможности. Во-вторых, реализация декомпиляторов будет практически не зависеть от типа процессора выполнения, поскольку работа генетического алгоритма не предполагает сильной зависимости от особенностей языка исходного кода и набора машинных инструкций – сглаживание частного противоречия между вторыми частями потребности и возможности.

Следовательно, доведение текущего исследования до практической реализации позволит полностью разрешить указанные противоречия и следующую из него проблему. И даже лишь именно этот умозаключительный факт может служить сильнейшей научной мотивацией для проведения текущего исследования.

Принцип работы

Стоит отметить, что принцип работы генетической декомпиляции противоположен классической, поскольку производится попытка компиляции различных экземпляров ИК в МК, а не наоборот. Таким образом, данный способ имеет качественное отличие от существующих.

Адаптация к предметной области

Произведем адаптацию классических генетических алгоритмов к задаче декомпиляции путем сопоставления основных терминов первого с сущностями второй: под особью понимается экземпляр ИК; хромосома особи – текст ИК; ген хромосомы – отдельная конструкция текста (в простейшем случае – символ); популяция – множество сгенерированных экземпляров ИК; поколение (или эпоха) – количество генерации экземпляров ИК из предыдущих (0-е поколение может быть сформировано случайным образом); селекция – отбор части экземпляров, компилируемый ИК которых наиболее близок к заданному декомпилируемому МК; мутация – случайное изменение конструкций ИК; скрещивание – составление нового ИК из двух имеющихся.

Наиболее интересным с научной и сложным с практической точки зрения сущностью является функция приспособляемости (иногда еще называемая фитнес-функцией от англ. Fitness), которая показывает, насколько МК, скомпилированный из экземпляра ИК после N -поколений, близок к заданному. Также, поскольку преобразование между текстовым ассемблерным кодом (далее – АК) и бинарным МК считается практически тождественным, функция приспособляемости может работать только с текстовым представлением инструкций.

Фактически, суть генетического алгоритма сводится к оптимизации функции приспособляемости путем подбора ее параметров – генов особи, что тождественно поиску такого ИК, который в точности бы компилировался в заданный МК. Следовательно, результатом решения задачи оптимизации как раз и будет осуществление генетической декомпиляции. При этом, как хорошо видно, в сопоставленных сущностях отсутствует явная привязка как к языку программирования ИК, так и к типу процессора инструкций МК. Единственная зависимость имеется в процессе компиляции, что полностью нейтрализуется использованием соответствующего компилятора, представляющего собой внешнее по отношению к способу программное средство. Таким образом, аналогом выживания особей во враждебной среде для предметной области будет постепенная подстройка «размножающихся» и компилируемых экземпляров ИК к тому (а точнее, одному из набора), который в точности соответствует или максимально близок к заданному МК.

АРХИТЕКТУРА ПРОТОТИПА

Предложенная концепция ранее проверялась с помощью мысленного эксперимента, описанного автором в работе [10], что конечно же, не является достаточным для ее подтверждения. Поэтому был разработан прототип генетического декомпилятора (далее – Прототип), описание которого приводится ниже. Прототип предназначен для восстановления ИК на языке C, обработка которого с помощью утилиты компиляции «cl.exe» из состава *Microsoft Visual Studio Community 2019* дает заданный АК (прямой аналог бинарного МК) для 64-битной версии архитектуры x86. Указанные характеристики не являются существенным ограничением, поскольку в теории может использоваться практически любой язык программирования и набор инструкций процессора (в том числе и для виртуальной машины) – это повлияет лишь на выбор компилятора.

Инструменты разработки

Для создания Прототипа использовалась среда разработки *Microsoft Visual Studio Community 2019*, в состав которой входит язык программирования C# и программная платформа .Net Framework версии 4.7.2. Для реализации генетического алгоритма использовалась библиотека *Genetic* версии 2.2.5 из состава открытой программной платформы *AForge.NET*.

Структурно-функциональная архитектура

Опишем строение Прототипа с помощью структурно-функциональной архитектуры – в виде структуры его модулей и их функциональных связей (рисунок 1).

Архитектура состоит из следующих модулей (см. рисунок 1), функциональные связи которых отражены направленными стрелками и не требуют дополнительных пояснений:

- 1) модуль запуска, ответственный за начало работы Прототипа, инициализацию структур и т. д.;
- 2) модуль завершения, ответственный за конец работы, деинициализацию структур и т. д.;
- 3) модуль ядра генетического алгоритма, являющийся упомянутой библиотекой *Genetic* из состава *AForge.NET*, реализующей основную логику эволюции экземпляров ИК;
- 4) модуль параметров алгоритма, содержащий настройки генетического алгоритма (например, частоту мутации и скрещивания);
- 5) модуль обработки эпохи, обеспечивающий получение нового поколения экземпляров ИК;
- 6) модуль мутации, осуществляющий мутацию экземпляра ИК путем случайного изменения его конструкций;
- 7) модуль скрещивания, осуществляющий скрещивание двух экземпляров ИК путем выбора случайным образом из их гена конструкций языка для формирования нового экземпляра;

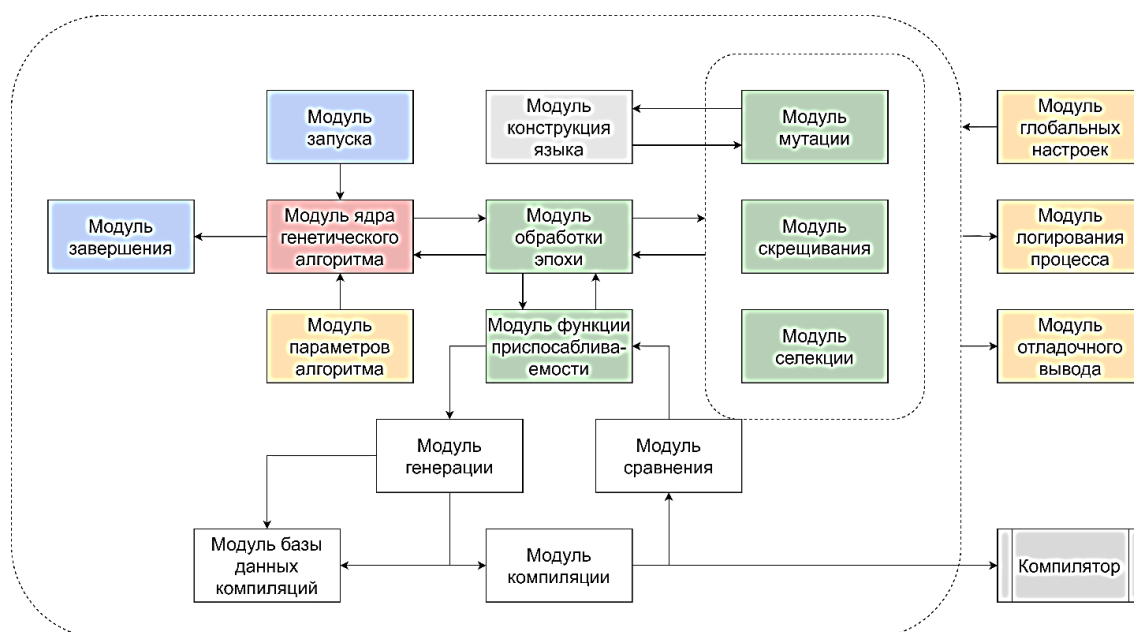


Рис. 1. Структурно-функциональный слой архитектуры прототипа генетического декомпилятора

Fig. 1. Structural and Functional Layer of the Genetic Decompiler Prototype Architecture

8) модуль селекции, осуществляющий выбор наиболее приспособленных экземпляров ИК, т. е. таких, АК которых наиболее близок к заданному;

9) модуль конструкция языка (программирования), содержащий одноименный набор для ИК (т. е. генов), на основании которых происходит мутация;

10) модуль функции приспособляемости, возвращающей численный показатель близости АК к заданному;

11) модуль генерации, создающий ИК экземпляра в текстовом виде, готовом для компиляции;

12) модуль базы данных компиляций, носящий оптимизационное назначение и хранящий все полученные ранее результаты компиляции ИК; таким образом, если некоторый ИК уже был скомпилирован ранее, то значение приспособляемости для его АК может быть получено из базы данных без запуска ресурсоемкой внешней утилиты;

13) модуль компиляции, запускающий внешнюю утилиту компиляции для получения АК из сгенерированного ИК;

14) модуль сравнения, оценивающий, насколько два АК близки друг к другу (способ сравнения учитывает то, что один из вариантов АК должен в процессе генетической декомпиляции приближаться к другому, заданному);

15) модуль глобальных настроек, содержащий настройки, используемые всеми другими модулями (например, уровень детализации логирования процесса или флаги отладочного вывода);

16) модуль логирования процесса, отображающий весь процесс эволюции поколений экземпляров ИК;

17) модуль отладочного вывода, отображающий информацию об ИК и АК экземпляров; наличие мо-

дуля обусловлено сложностью понимания и прогнозирования поведения генетического алгоритма, для чего требуется детализация его работы;

18) компилятор, являющийся внешним программным средством преобразования ИК на конкретном языке программирования в АК, набор инструкций которого полностью совпадает с инструкциями в заданном АК.

Отметим, что элемент архитектуры Компилятор в строгом смысле не является полноценным модулем, поскольку представляет собой полностью обособленное программное средство вне Прототипа. Однако его рассмотрение, как набора интерфейсов работы с файловой системой для компиляции ИК и чтения из файла содержимого его АК, может интерпретироваться как модульная часть Прототипа.

Принцип работы

Опишем достаточно общий алгоритм работы Прототипа. После запуска программы и инициализации параметров генетического алгоритма начинается итеративная генерация поколений экземпляров ИК. В процессе такой эволюции с некоторой частотой (заданной параметрами) в ИК экземпляров происходят мутации путем случайного изменения нескольких их конструкций. Затем часть экземпляров скрещивается, формируя таким образом новый экземпляр, ИК которого получен из случайного набора двух родительских. После этого происходит вычисление приспособляемости всех имеющихся экземпляров (часть из которых получена из предыдущего поколения и осталась неизменной, часть подверглась мутации, а часть появилась в результате скрещивания). Экземпляры с наилуч-

шей приспособляемостью отбираются для следующего поколения – т. е. осуществляется селекция; остальные же считаются «не выжившими» и отбрасываются. Как было указано выше, наиболее сложным элементом такой схемы является функция приспособляемости, поэтому ее алгоритм будет описан далее более детально.

Функция приспособляемости

Разработка корректной функции приспособляемости, используемой в работе генетического алгоритма, хоть и является сложной задачей, существенно уступает в этом разработке современных декомпиляторов. При этом функцию требуется создать единожды, а затем лишь корректировать.

В Прототипе реализован простейший алгоритм данной функции (в виде одноименного модуля), который хотя и может быть посчитан тривиальным, но даже на нем (как будет показано далее), генетическая декомпиляция обладает удовлетворительной работоспособностью.

Основной принцип работы алгоритма функции базируется на следующих двух идеях.

Идея 1. Подобие двух АК, имеющих текстовый вид, может быть (конечно же в простейшем случае) оценено, как совпадение их количества строк, состава отдельных строк и содержимого всего кода. За каждое такое совпадение начисляется определенное количество баллов, суммирование которых и составляет значение, возвращаемое функцией приспособляемости. Таким образом, большие значения функция будет возвращать для тех экземпляров ИК, характеристики АК которых ближе к характеристикам заданного АК; при этом, приоритетом является полное совпадение кодов или хотя бы корреляция их ассемблерных строк. У такой идеи есть существенный недостаток, который (как показало предварительное тестирование Прототипа) ощутимо снижает работоспособность генетической декомпиляции. Поскольку далеко не каждый случайный набор конструкций языка программирования может быть скомпилирован в АК, то для большинства экземпляров ИК функция будет возвращать 0 баллов, так как формально АК экземпляра даже не был получен. Чтобы хотя бы частично нейтрализовать этот недостаток, была выдвинута и реализована следующая идея.

Идея 2. Прототип используется для проверки концепции генетической декомпиляции в ИК на языке C, особенностью синтаксиса которого является поддержка так называемой однопроходности, когда для компиляции отдельных конструкций языка отсутствует необходимость в «забегании вперед» по ИК и обработке последующих конструкций. Фактически, АК может генерироваться сразу по мере набора ИК. Такая особенность приводит к тому, что конструкции ИК имеют прямое отображе-

ние на инструкции АК (хотя и с некоторым разбросом, поскольку одна конструкция может преобразовываться в несколько инструкций). Как результат, близость конструкций двух ИК в начале и конце текста будет соответствовать близости инструкций в начале и конце АК. Поэтому ИК, начальные и конечные участки которого компилируются в аналогичные участки заданного АК априори будет считаться более приспособленным, чем не имеющий таких участков. Таким образом, целесообразно не просто сравнивать два АК – полученный из ИК и заданный, а оценивать схожесть их начальных и конечных участков (например, постепенным увеличением их длины). Это, в частности, позволит повысить количество успешных компиляций ИК и, тем самым, избавиться от недостатка, названного автором, как «проклятие нулевого значения функции приспособляемости для некомпilierуемого ИК». К сожалению, подобное соответствие трудно применимо для участков в середине кода, поскольку сложно сопоставить адреса ИК и АК; впрочем, это все же не является невозможным и в будущем гипотетически позволит существенно повысить качество вычисления функции приспособляемости.

Псевдокод алгоритмов

Приведем далее алгоритм работы главной функции Прототипа – *MainProcees()*, отражающей работу его модулей (см. рисунок 1). Функция на вход принимает пути к файлам, необходимым для компиляции, и настройки ядра генетического алгоритма; а на выходе возвращает восстановленный ИК, компилируемый в заданный АК (путь к которому указан в составе первого параметра). Принцип работы функции описан ниже с помощью интуитивно понятного псевдокода Алгоритма 1.

Алгоритм 1: MainProcess

Input:

FilePaths – настройки путей к файлам

GeneticParams – параметры генетического алгоритма

Output:

Text – исходный код, компилируемый
в заданный ассемблерный код

Begin

```
1: Compiler.Init(FilePaths);  
2: Population = GeneticCore(GeneticParams,  
    &EvaluateFitness(), &ApplyMutation(),  
    &ApplyCrossover(), &ApplySelection());
```

3: Do

```
4:   Population.RunEpoch();  
5:   Logger.Write(Population.Chromosomes);  
6: Until Population.IsCompleted()
```

```
7: Text = Population.BestChromosome.ToText;
```

```
8: Return Text;
```

End

Приведем построчное описание работы алгоритма.

В строке 1 инициализируются пути модуля компиляции *Compiler*.

В строке 2 создается объект популяции *Population*, инициализируемый параметрами генетического алгоритма и функцией вычисления приспособляемости *EvaluateFitness()*, процедурами мутации *ApplyMutation()*, скрещивания *ApplyCrossover()* и селекции *ApplySelection()*. Принцип работы этих процедур достаточно тривиален и был приведен ранее при описании соответствующих модулей. Алгоритм работы функции приспособляемости более подробно будет рассмотрен далее. Также в этот момент формируется начальная (0-я) популяция.

В строке 3 начинается цикл по эволюционному развитию популяций экземпляров ИК.

В строке 4 производится получение новой популяции путем применения мутации, скрещивания и селекции, а также оценивания приспособляемости экземпляров.

В строке 5 производится логирование информации о текущей популяции для отслеживания процесса эволюции.

В строке 6 заканчивается цикл, начатый в строке 2. Условием окончания является получение популяции, неизменной во времени – т.е. все экземпляры которой имеют одинаковое значение функции приспособляемости. Данное значение не обязательно является максимальным, поскольку генетический алгоритм способен находить локальные максимумы функции, которые не являются глобальными, что представляет собой отдельную задачу, как правило решаемую подстройкой параметров работы.

В строке 7 в переменную *Text* генерируется текст ИК, полученный из экземпляра последней популяции, обладающей наилучшей приспособляемостью – т.е. любой из популяций, следуя условию окончания цикла в строке 6.

В строке 8 полученный текст ИК возвращается из функции.

Приведем далее алгоритм работы функции приспособляемости *EvaluateFitness()*, идеи работы которой были описаны выше. Функция на вход принимает хромосому экземпляра, представлявшего собой список конструкций его ИК в виде текстовых токенов, а на выходе возвращает балльное значение приспособляемости экземпляра (чем выше значение, тем ближе АК экземпляра к заданному). Принцип работы функции описан с помощью интуитивно понятного псевдокода Алгоритма 2.

Приведем построчное описание работы алгоритма.

В строке 1 инициализируется базовое значение приспособляемости *Fitness* (путем приравнивания его к нулю).

Algorithm 2: EvaluateFitness

Input:

Tokens – ИК в виде списка токенов текста (т.е. конструкций языка)

Output:

Fitness – значение фитнес функции для экземпляра ИК

Begin

```

1: Fitness = 0;
2: For i = 0 .. Tokens.Length Do
3:   tokensPart = Tokens.Take(i + 1);
4:   text = tokensPart.ToText();
5:   fit = CompileAndEvaluatePartialFitness(text);
6:   Fitness += COEFF_DIRECT_PARTIAL *
              fit * (i + 1);
7: End For
8: For i = 0 .. Tokens.Length Do
9:   tokensPart = Tokens.Skip(i + 1);
10:  text = tokensPart.ToText();
11:  fit = CompileAndEvaluatePartialFitness(text);
12:  Fitness += COEFF_REVERT_PARTIAL *
              fit * (Tokens.Length - i - 1);
13: End For
14: Return Fitness;
End

```

В строке 2 начинается цикл по увеличению значений индекса *i* с 0 до количества токенов из входного параметра.

В строке 3 выделяется часть начальных токенов (*tokensPart*) длиной текущего индекса цикла плюс 1.

В строке 4 из выделенных токенов формируется текст (*text*) ИК.

В строке 5 вычисляется значение приспособляемости сформированного текста с использованием функции алгоритма *CompileAndEvaluatePartialFitness()* для получения частичной приспособляемости от области текста ИК (которая будет описана далее).

В строке 6 значение приспособляемости для выделенной части токенов прибавляется к общему значению приспособляемости с применением корректирующего коэффициента *COEFF_DIRECT_PARTIAL*. Также, чем из большего числа токенов был сформирован текст ИК, тем на большую величину будет умножено и значение его приспособляемости – стимулируя тем самым генетический алгоритм формировать более «удачные» последовательности ген, соответствующих скомпилированному АК, близкому к заданному.

В строке 7 оканчивается цикл, начатый в строке 2.

Строки с 8-й по 13-ю практически полностью идентичны строкам с 2-й по 7-ю с тем отличием, что в строке 3 выделяется часть конечных, а не начальных токенов.

В строке 14 вычисленное значение приспособляемости возвращается из функции.

Приведем далее алгоритм работы функции частной приспособляемости *CompileAndEvaluatePartialFitness()*, используемой алгоритмом *EvaluateFitness()*. Функция на вход принимает текст ИК, а на выходе возвращает балльное значение приспособляемости соответствующего экземпляра. Принцип работы функции описан с помощью интуитивно понятного псевдокода Алгоритма 3.

Алгоритм 3: *CompileAndEvaluatePartialFitness*
Input:

Text – текст ИК

Output:

Fitness – значение фитнес функции для экземпляра ИК

Begin

```

1: Fitness = 0;
2: If Text In Database.Keys Then
3:   Fitness = Database[Text];
4: Else
5:   Compiler.Write(Text);
6:   Status = Compiler.Execute();
7:   If Status == True Then
8:     Fitness += SCORE_CODE_IS_COMPILED;
9:   Lines = Compiler.Load();
10:  LinesOrig = Compiler.LoadOriginal();
11:  IF Lines.Count == LinesOrig.Count Then
12:    Fitness += SCORE_SAME_NUMBER_OF_LINES;
13:  End If
14:  MinCount = Min(Lines.Count,
                  LinesOrig.Count);
15:  For i == 0 .. MinCount Do
16:    If Lines[i] == LinesOrig[i] Then
17:      Fitness += SCORE_SAME_LINE;
18:    End If
19:  End For
20:  If Lines.Count == LinesOrig.Count
  And Lines.Count == MinCount Then
21:    Fitness += SCORE_SAME_TEXT;
22:  End If
23: End If
24: Database[Text] = Fitness;
25: End If
26: Return Fitness;
End

```

Приведем построчное описание работы алгоритма.

В строке 1 инициализируется базовое значение приспособляемости *Fitness* (путем приравнивания его к нулю).

В строке 2 начинается основная ветка условия, выполняемая, если в базе данных (*Database*) присутствует значение приспособляемости для текста ИК (*Text*), переданного в алгоритм в качестве параметра.

В строке 3 возвращается ранее посчитанное значение приспособляемости для текста ИК.

В строке 4 начинается альтернативная ветка условия, выполняемая, если текст ИК не найден в базе данных.

В строке 5 происходит запись текста в файл временного ИК для последующей компиляции; для этого используется объект компиляции *Compiler*.

В строке 6 производится компиляция ИК, записанного во временный файл, в АК, записываемый в другой временный файл, с возвращением результата процесса в переменную *Status*.

В строке 7 начинается основная ветка условия, выполняемая, если статус компиляции оказался успешным.

В строке 8 увеличивается значение приспособляемости на заданное число баллов *SCORE_CODE_IS_COMPILED* – стимулируя тем самым генетический алгоритм формировать экземпляры с компилируемым ИК.

В строке 9 считываются строки АК из временного файла (полученного в строке 6) в массив *Lines*.

В строке 10 считываются строки заданного АК в массив *LinesOrig*.

В строке 11 начинается основная ветка условия, выполняемая, если количество ассемблерных строк скомпилированного и заданного кода равны.

В строке 12 увеличивается значение приспособляемости на заданное число баллов *SCORE_SAME_NUMBER_OF_LINES* – стимулируя тем самым генетический алгоритм формировать экземпляры с таким же количеством ассемблерных строк, как и у заданного.

В строке 13 оканчивается ветка проверки, начатая в строке 11.

В строке 14 вычисляется минимальное количество строк среди скомпилированного и заданного АК с сохранением значения в *MinCount*.

В строке 15 начинается цикл по увеличению значений индекса *i* с 0 до минимального количества ассемблерных строк, сохраненных в *MinCount*.

В строке 16 начинается основная ветка условия, выполняемая, если строка с индексом *i* скомпилированного и заданного АК совпали.

В строке 17 увеличивается значение приспособляемости на заданное число баллов *SCORE_SAME_LINE* – стимулируя тем самым генетический алгоритм формировать экземпляры, АК которых содержит строки, совпадающие со строками заданного.

В строке 18 оканчивается ветка условного выполнения, начатая в строке 16.

В строке 19 оканчивается цикл, начатый в строке 15.

В строке 20 начинается основная ветка условия, выполняемая, если все строки скомпилированного и заданного АК совпали (т. е. ИК экземпляра полностью компилируется в заданный АК).

В строке 21 увеличивается значение приспособляемости на заданное число баллов *SCORE_SAME_TEXT* – стимулируя тем самым генетический алгоритм сохранять в поколении экземпляры с ИК, в точности компилируемые в заданный АК.

В строках 22, 23 и 25 оканчивается ветка условного выполнения, начатая в строках 20, 7 и 4 соответственно.

В строке 24 происходит сохранение текста ИК и значение его приспособляемости в базе данных.

В строке 26 вычисленное значение приспособляемости возвращается из функции.

Интерфейс

Поскольку Прототип создан исключительно для проверки концепции генетической декомпиляции, то он имеет минимально необходимый интерфейс. Прототип представляет собой консольное приложение, принимающее в качестве параметров пути к следующим файлам:

- шаблон, служащий основой для генерации новых вариантов ИК;
- заданный АК, который является целевым для работы декомпиляции и с которым сравниваются все другие АК;
- ИК, из которого получается заданный АК (в процессе работы Модуля запуска); этот ИК считается отсутствующим в задаче декомпиляции, однако он упрощает тестирование Прототипа для различных вариантов заданного АК;
- временный ИК, генерируемый согласно файлу шаблона и хромосоме экземпляра ИК;
- временный АК, компилируемый из временного ИК;
- внешний компилятор, вызываемый Прототипом для получения временного АК из временного ИК.

Также прототип принимает следующие настройки (включая параметры алгоритма генетической декомпиляции):

- частота мутаций в виде доли особей одной популяции, хромосомы которых участвуют в мутации (по умолчанию равно 0,2 или 20 %);
- частота скрещиваний в виде доли особей одной популяции, хромосомы которых участвуют в скрещивании (по умолчанию равно 0,2 или 20 %);
- размер одной популяции в виде количество особей популяции, как изначальной, так и отбираемой в результате селекции (по умолчанию равно 10).

Как хорошо можно увидеть, какая-либо специфика языка программирования или типа процессора во входных параметрах отсутствует, а вся взаимосвязь между ИК и АК (и, соответственно, МК) определяется используемым внешним компилятором (последний параметр в списке путей). Вывод всей информации (полученного результата, ошибок, лога процесса и отладочной информации) Прототипом осуществляется в текстовую консоль.

ЭКСПЕРИМЕНТ

Для непосредственной проверки концепции генетической декомпиляции проведем ряд базовых экспериментов с помощью разработанного Прототипа.

Ограничения

Для упрощения проведения эксперимента и отсечения несущественного функционала Прототипа, а также ставя целью именно подтверждение концепции, а не полноценное тестирование решения, введем следующие 6 ограничений.

Ограничение 1. Будем восстанавливать АК для отсутствующего ИК, представляющего следующее тело функции, суммирующей 3 аргумента (на языке C):

```
Function: TestFunc
1: int test (int x, int y, int z) {
2:   int ret = x + y + z;
3:   return ret;
4: }
```

Согласно коду, функция *func()* в качестве аргументов принимает три переменные (типа *Integer*) – *x*, *y* и *z*, затем их суммирует во временную переменную *ret* и возвращает ее значение.

Ограничение 2. Будем с помощью генетического алгоритма создавать популяции экземпляров ИК, соответствующих только самому математическому выражению, состоящему из следующей последовательности конструкций языка C – «*x+y+z*». Таким образом, синтаксическое «обрамление» выражение в виде сигнатуры функции и конструкции возврата ее значения через временную переменную учитываться не будет.

Ограничение 3. Для сравнения скомпилированного и заданного АК будем использовать только его часть, относящуюся к вычислению выражения, указанного в Ограничении 2. Эта часть в ассемблерной записи имеет следующий вид, расположенный между метками строк 2 и 3 функции *TestFunc()*:

```
; Line 2
mov     eax, DWORD PTR y[rsp]
mov     ecx, DWORD PTR x[rsp]
add     ecx, eax
mov     eax, ecx
add     eax, DWORD PTR z[rsp]
mov     DWORD PTR ret[rsp], eax
; Line 3
```

Ограничение 4. В качестве возможных конструкций будем использовать их достаточно малый набор, состоящий из 6 элементов – токенов языка: имена переменных – «*x*», «*y*», «*z*» и «*w*», а также математические выражения – «*+*» и «*-*».

Ограничение 5. Фактом окончания эволюции (т. е. ситуация, когда функция *Population.IsCompleted()* в псевдокоде алгоритма *MainProcess* возвращает *True*) будем считать получение подряд 100 поколений, экземпляры которого имеют одинаковое значение приспособляемости – т. е. эволюция оказывается

в некотором экстремуме, из которого не может выйти (или другими словами, в ситуации, когда экземпляры ИК не могут улучшить свою приспособляемость).

Ограничение 6. Все предустановленные значения коэффициентов, баллов, условий окончания декомпиляции и пр. получены эмпирически, а их уточнения являются отдельно стоящей задачей, выходящей за рамки текущего исследования.

Сценарий 1. Базовая проверка работоспособности

Перед запуском Прототипа оценим возможности решения подобной задачи полным перебором. В этом случае необходимо составить выражение из 5 конструкций (см. Ограничение 2), каждая из которых может быть одним из множества 6 элементов (см. Ограничение 4). Простые вычисления позволяют получить полное число комбинаций текстов ИК при переборе, как $6 \times 6 \times 6 \times 6 \times 6 = 7776$. А учитывая тот факт, что любой ИК должен быть преобразован в МК внешним компилятором (даже несмотря на то, что большинство вариантов попросту не смогут быть скомпилированы), увеличение числа комбинаций существенно повысит время декомпиляции.

Произведем выполнение Прототипа по базовому сценарию – декомпиляции одиночного АК, в соответствии с указанными ограничениями и параметрами генетического алгоритма по умолчанию. Это приведет к выводу в консоль следующего лога (часть несущественных строк пропущено, что обозначено в логе строкой «...»).

```
[ Epoch: 0 ] MAX : { x x x x x } => 201 (10:0)
[ Epoch: 1 ] MAX : { x x x x x } => 706 (2:0)
...
[ Epoch: 10 ] MAX : { x x x x x } => 706 (10:2)
[ Epoch: 11 ] MAX : { - y x x x } => 808 (2:0)
...
[ Epoch: 14 ] MAX : { - y + + x } => 1717 (1:0)
[ Epoch: 15 ] MAX : { - + x x x } => 1810 (1:0)
...
[ Epoch: 25 ] MAX : { - + x x x } => 1810 (1:0)
[ Epoch: 26 ] MAX : { y + x x x } => 1982 (1:0)
...
[ Epoch: 32 ] MAX : { y + x x x } => 1982 (1:0)
[ Epoch: 33 ] MAX : { z + y + x } => 1989 (2:0)
...
[ Epoch: 43 ] MAX : { z + y + x } => 1989 (10:7)
[ Epoch: 44 ] MAX : { x + y + x } => 1997 (1:0)
...
[ Epoch: 55 ] MAX : { x + y + x } => 1997 (10:3)
[ Epoch: 56 ] MAX : { x + y + z } => 7002 (1:0)
...
[ Epoch: 63 ] MAX : { x + y + z } => 7002 (8:0)
[ Epoch: 64 ] MAX : { x + y + z } => 7002 (10:1)
...
[ Epoch: 163 ] MAX : { x + y + z } => 7002 (10:100)
```

Строки лога имеют следующий формат:

```
[ Epoch: N_EPOCH ] MAX : { TEXT } => FITNESS
(N_BEST:N_EPOCH_WITH_BEST)
```

где N_EPOCH означает номер поколения (0 – для начального, неподверженного мутациям и скрещиваниям); $TEXT$ – текст ИК для экземпляра с наилучшей приспособляемостью; $FITNESS$ – ее значение; N_BEST – количество особей, имеющих наилучшую приспособляемость в текущем поколении; $N_EPOCH_WITH_BEST$ – количество поколений, все особи которого имеют наилучшую приспособляемость (используется для определения факта завершения процесса декомпиляции).

Как хорошо видно по логу, процесс декомпиляции завершился на 163-м поколении, притом получив верный результат – ИК выражения « $x + y + z$ ».

Интерпретация процесса декомпиляции

Восстановим и интерпретируем эволюцию особей ИС в процессе генетической декомпиляции, используя лог, полученный ранее.

Поколение 0 является изначальным (соответствующим некомпиллируемому тексту – « $x x x x x$ »), приспособляемость (т. е. близость к заданному АК) экземпляров ИК которого равна 201. Гены экземпляров фактически могут быть сформированы случайным образом и не представляет особого научно-практического интереса.

В поколении 1 произошли изменения (здесь и далее под ними подразумеваются мутация и скрещивание), в результате которых 4-й токен был изменен с « x » на « $+$ », что повысило максимальную приспособляемость до 706. Естественно, возможно были и другие мутации, которые не отражаются, поскольку лог содержит текст ИК только с локально максимальной приспособляемостью.

В поколении 11 первый токен был изменен с « x » на « $-$ », а второй – « x » на « y », увеличив тем приспособляемость до 808.

Затем, вплоть до поколения 43, гены (т. е. токены ИК) экземпляров претерпевали изменения, представляя собой ошибочную ветку эволюции. Причина ошибочности заключается в том, что искомый ИК начинается с конструкции « x » вместо присутствующего в поколениях « $-$ », чего эволюции удалось достичь лишь в 44-м поколении.

Затем, продолжая мутировать, скрещиваться и селективировать, было сформировано поколение 56, как раз и представляющее искомый ИК. И хотя в данном поколении присутствовал всего лишь один экземпляр, имеющий глобально максимальную приспособляемость, равную 7002, однако уже все экземпляры 64-го поколения обладали таким значением.

На протяжении последующих 100 поколений (т. е. до 163-го включительно) все экземпляры также имели одинаковую приспособляемость, что и посчиталось алгоритмом, как завершение работы.

Важным выводом, который можно сделать из анализа и интерпретации лога, является устойчивость генетической декомпиляции к отклонениям эволюции по «ошибочным» веткам развития (т. е. отход от истинного ИК, компилируемого в заданный МК); такое отклонение соответствует поколениям с 11 по 43. Это говорит о потенциальной достижимости алгоритмом глобального максимума функции приспособляемости даже в случае неудачных мутаций и скрещиваниях, основанных на генераторе случайных чисел.

Подсчет Прототипом количества реальных компиляций ИК (и его частей согласно работе алгоритма *EvaluateFitness()* в процессе вычисления приспособляемости) позволил получить значение 449 (естественно, с учетом работы Модуля базы данных компиляции, имеющего оптимизационное назначение). Таким образом, применение генетической декомпиляции по сравнению с полным перебором токенов ИК сократило количество ресурсоемких вызовов внешнего компилятора в 7776/449 ~ 17 раз. При этом, очевидно, что добавление в список возможных конструкций языка всего их множества катастрофически (для времени выполнения) увеличит время полного перебора, хотя гипотетически на скорость работы Прототипа повлияет существенно меньше.

Сценарий 2. Вычисление результативности

Естественно, ожидание того, что алгоритм Прототипа будет всегда давать верные результаты, даже при учете всех 6 введенных ограничений, было бы слишком амбициозным. И простейшее тестирование путем многократного запуска Прототипа подтверждают это – в ряде случаев «выживает» популяция, ИК экземпляров которой на протяжении 100 поколений обладает одинаково высокой приспособляемостью, при этом не компилируясь в заданный МК. Поэтому далее проведем эксперимент по нахождению результативности Прототипа, как доли его запусков, приведших к верному ИК (т. е. соответствующих заданному МК) по отношению ко всем запускам.

В процессе данного сценария было произведено 10000 запусков Прототипа в специальном исследовательском режиме, выводящем полученный ИК (с префиксом *Text*), значение его приспособляемости (с префиксом *Fitness*) и количество поколений (с префиксом *Epoches*). Время эксперимента на персональном компьютере средней мощности составило около 17 мин. Часть полученного лога представлена ниже.

```
(XX.XX.2021 18:41:49) Text = x + y + z, Fitness = 7002, Epoches = 133
(XX.XX.2021 18:42:01) Text = - y + - y, Fitness = 1816, Epoches = 146
(XX.XX.2021 18:42:13) Text = x + y + z, Fitness = 7002, Epoches = 227
...
```

```
(XX.XX.2021 18:58:30) Text = x + y + z, Fitness = 7002, Epoches = 176
(XX.XX.2021 18:58:30) Text = x + y + z, Fitness = 7002, Epoches = 288
(XX.XX.2021 18:58:30) Text = x + y + z, Fitness = 7002, Epoches = 149
```

Результаты статистической систематизации лога приведены в таблице 1, имеющей следующие столбцы:

- 1) № – номер решения, соответствующий одному из максимумов функции приспособляемости, определенных алгоритмом, как глобальный;
- 2) Текст ИК – текст на языке C, компиляция которого получает МК, наиболее близкий (с точки зрения генетического алгоритма) к требуемому;
- 3) Количество решений – общее число решений с одинаковым текстом ИК, полученных генетическим алгоритмом;
- 4) Доля решения – округленная процентная доля решений с данным ИК по отношению ко всем решениями (т. е. к 10000);
- 5) Значение приспособляемости – количество баллов, полученных при сравнении МК, скомпилированного из экземпляров ИК полученного решения, с заданным МК;
- 6) Среднее количество поколений – количество итераций эволюции, после которой значение приспособляемости экземпляров одного поколения стабилизировалось (т. е. не менялось 100 раз);
- 7) Первое истинное поколение – номер поколения, экземпляры которого обладали одинаковой приспособляемостью в течение последующих 100 итераций (значение равно среднему количеству итераций минус 100).

ТАБЛИЦА 1. Результаты статистической систематизации лога работы Прототипа

TABLE 1. Results of the Prototype's Log Statistical Systematization

1	2	3	4	5	6	7
1	x + y + z	7374	0,74 %	7002	181	81
2	x - y + z	1	≈ 0 %	1998	140	40
3	x + y - z	1537	0,15 %	1997	152	52
4	- y - - y	1088	11 %	1816	167	67

Согласно результатам табличного анализа можно сделать следующие выводы.

Во-первых, всего было найдено 4 решения, каждое из которых соответствует одному из максимумов функции приспособляемости. При этом все решения представляют собой компилируемый код, что гипотетически еще раз подтверждает потенциал предложенной концепции.

Во-вторых, одно из решений является истинным (под номером 1), поскольку его ИК компилируется в АК, тождественный заданному.

В-третьих, доля верных решений составляет 74 %, что превышает долю ближайшего конкурента (под номером 3) в 7374/1537 ~ 5 раз. Следо-

вательно, значение 74 % может считаться результативностью Прототипа генетической декомпиляции. Графическая интерпретация всех полученных решений представлена на рисунке 2 (с соблюдением примерных соотношений между значениями приспособляемости).

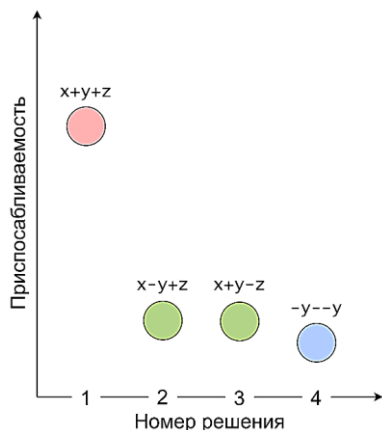


Рис. 2. Приспособляемость полученных решений при множественной генетической декомпиляции

Fig. 2. Adaptability of the Obtained Solutions for Multiple Genetic Decompilation

Также, при установлении факта, что алгоритм нашел локальный, а не глобальный максимум (в остальных $\frac{1+1537+1088}{10000} \sim 0,26$, т. е. 26 % случаев), достаточно будет осуществить декомпиляцию еще несколько раз, поскольку уже после второго запуска процент ошибки составит $\left(\frac{1+1537+1088}{10000}\right)^2 \sim 0,07$, т. е. 7 %. Такой прием позволит существенно увеличить результативность Прототипа, доведя его практически до 100 %.

В-четвертых, значение приспособляемости истинного решения (под номером 1) отличается от остальных (под номером 2, 3 и 4) практически в 3,5 раза, что дает потенциал для снижения количества ошибок алгоритма (т. е. выбора неверных максимумов) путем корректировки параметров самого генетического алгоритма для «покидания» границ локального экстремума (например, увеличением размера популяции, частоты мутаций, механизма скрещивания и т. п.).

И, в-пятых, первое поколение экземпляров, завершающих генетическую декомпиляцию, не превышает 100, что означает достаточно быстрое эволюционное развитие.

Сценарий 3. Оценка оптимизации компиляции

Основной операцией, снижающей оперативность работы Прототипа, является использование внешнего компилятора. При этом, если бы даже механизм преобразования ИК в АК был встроен в Прототип, то он все равно занимал бы значительную долю времени. В интересах этого был создан Модуль базы данных компиляций, хранящий значе-

ния приспособляемости для всех скомпилированных ранее ИК. Оценим его возможности по оптимизации путем выполнения эксперимента по сценарию, заключающемуся в отслеживании количества реальных компиляций в процессе генетической декомпиляции. Полученная зависимость в виде гистограммы представлена на рисунке 3.

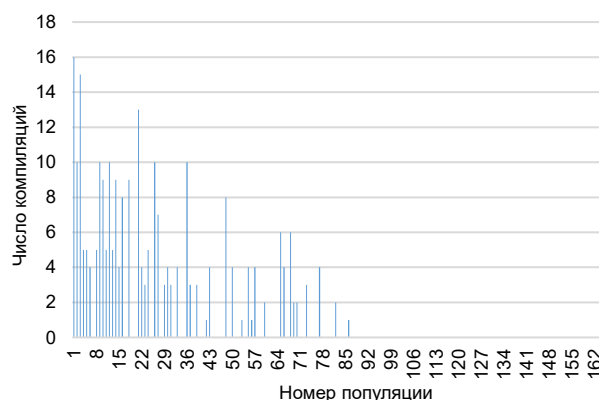


Рис. 3. Зависимость количества компиляций исходного кода от номера популяции

Fig. 3. The Dependence of Compilations' Source Code Number on Population Number

Как хорошо видно (см. рисунок 3), снижение количества компиляций с преобразованием ИК в АК имеет снижающийся тренд (линейный или обратно экспоненциальный). Так, уже после 90-го поколения реальная компиляция отсутствует полностью, все последующие значения функции приспособляемости берутся из базы данных; что существенно понижает скорость декомпиляции.

Сценарий 4. Подбор параметров генетического алгоритма

Оценим то, насколько подстройка генетического алгоритма влияет на его результативность. Для этого проведем эксперимент по сценарию, в котором осуществляется перебор параметров генетического алгоритма следующим образом:

- размер популяции меняется от 2 до 20 с шагом 1 (по умолчанию было 10);
- доля мутаций меняется от 0,0 до 1,0 с шагом 0,1 (по умолчанию было 0,2);
- размер селекций меняется от 0 до 1,0 с шагом 0,1 (по умолчанию было 0,2).

Следовательно, в ходе проведенного эксперимента, перебиралось $19 \times 11 \times 11 = 2299$ комбинаций параметров.

Для каждого набора параметров осуществлялось 100-кратное проведение декомпиляции (т. е. генерация ИК и вычисление приспособляемости), что позволило получить достаточно адекватную усредненную результативность Прототипа.

Таким образом, в ходе эксперимента было произведено $2299 \times 100 = 229900$ запусков Прототипа, а общее время эксперимента заняло примерно 430 мин.

По мере увеличения размера популяции (особенно при высоких значениях доли мутации и скрещивания) росло и время работы алгоритма. Это объяснимо тем, что при высоких долях большее число особей в популяции подвергается изменениям, требующим вычислений функции приспособленности, что сказывается на времени выполнении, даже несмотря на оптимизацию за счет применения базы данных. Однако итоговый рост времени декомпиляции не оказался критичным.

Используя полученный лог работы Прототипа, была построена зависимость минимальной, средней и максимальной результативности декомпиляции от размера популяции при всех значениях долей мутации и скрещивания (рисунок 4).

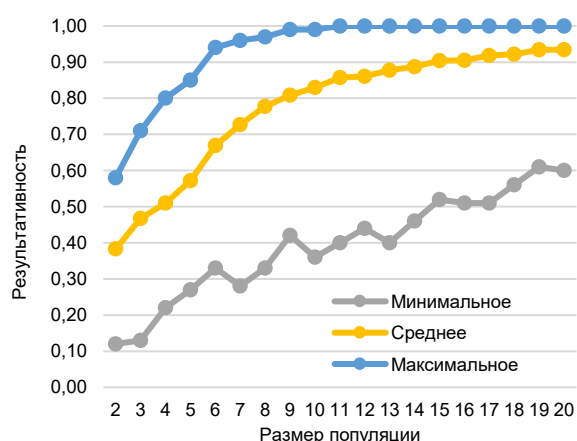


Рис. 4. Зависимость результативности генетической декомпиляции от размера популяции

Fig. 4. The Dependence between Genetic Decompilation's Performance on Population Size

Анализ лога работы Прототипа и графика на рисунке 4 позволяет сделать следующие предварительные выводы. Уже при размере популяций, равной 11, максимальное значение результативности достигает 1,0 – при долях мутаций и скрещиваний, равных парам значений (0,9; 0,1) и (1,0; 0,00), соответственно. Таким образом, «правильный» выбор параметров генетического алгоритма позволяет со 100 % вероятностью определять ИК, соответствующий заданному МК. Также прослеживается общая тенденция к увеличению среднего значения результативности, обосновывая то, что увеличение размера популяции приведет и к заметному повышению качества работы генетической декомпиляции. При этом, даже минимальный размер популяции, равный 2, в среднем, практически в половине случаев (а, точнее, следуя графику на рисунке 4 в 38 %) обеспечивает успешную декомпиляцию. Также на размерах популяции, более 15, доля результативности превышает середину в 50 %. Эта популяция может считаться точкой бифуркации в работоспособности Прототипа, поскольку даже при самой неудачной комбинации остальных параметров генетического алгоритма доля верных решений будет превалировать над долей неверных.

Анализ результатов

Исходя из результатов проведенных экспериментов, концепцию генетической декомпиляции можно считать подтвержденной, что следует из следующих утверждений.

Согласно Сценарию 1 эксперимента Прототип обладает базовой работоспособностью, а интерпретация работы генетической декомпиляции является адекватной и закономерной.

Согласно Сценарию 2 эксперимента Прототип имеет существенную результативность, позволяя в 3 из 4 раз корректно производить декомпиляцию. При этом процент успеха может быть повышен достаточно простыми техническими приемами, включающими подбор параметров.

Согласно Сценарию 3 реализованная оптимизация позволяет в процессе эволюционного развития существенно повысить скорость работы за счет сокращения реальных вызовов внешнего компилятора (что практически невозможно в случае применения полного перебора).

Согласно Сценарию 4 подбор оптимальных параметров генетического алгоритма (размер популяции, доля мутаций и скрещиваний) гипотетически позволяет достичь верного нахождения ИК в 100 % случаев.

Также в экспериментах не затронута подстройка константных коэффициентов и баллов, которые также могут оказать существенное влияние на успешность декомпиляции.

ЗАКЛЮЧЕНИЕ

На текущем этапе исследования проверялась концепция генетической декомпиляции, для чего был реализован соответствующий Прототип, на котором проводился ряд сценариев из состава эксперимента. Результаты последних могут служить обоснованием подтверждения концепции, хотя и пример АК (а, следовательно, ИК и МК) можно считать недостаточно сложным.

В текущем состоянии реализация полноценного генетического декомпилятора по предложенной концепции вряд ли осуществима, поскольку существует ряд проблем, не позволяющих проверить работоспособность Прототипа на более сложных примерах. Тем не менее, с точки зрения автора, устранение проблем носит чисто технический (и, в некотором смысле, логический) характер, не ставя под сомнения верность концепции в целом.

Продолжением исследования должно стать всестороннее тестирование Прототипа с целью технического (а не концептуального) усовершенствования его слабых сторон для проведения первых тестов на МК реальных программных продуктов. Это позволит не только полностью доказать состоятельность предложенной концепции, но и произве-

сти сравнение Прототипа, соответствующего новому 4-му этапу эволюции техник декомпиляции, с существующими аналогами, относящимися ко 2-му и 3-му этапам. В результате можно будет оценить перспективность общего вектора развития изложенной теоретико-практической «мысли» в данной предметной области.

Необходимо отметить, что автор понимает всю смелость предложенной концепции, гипотетиче-

ски способной раз и навсегда решить проблему декомпиляции, притом инвариантной не только от языка программирования ИК, но и от мнемоники записи АК, а также процессора выполнения МК. В связи с этим, автор готов адекватно воспринять критику проведенного исследования, его идей и результатов, а также выслушать любые авторитетные точки зрения касательно проблематики затронутой предметной области.

ФИНАНСИРОВАНИЕ

Работа выполнена при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Список используемых источников

1. Гурин Р.Е. Обзор и анализ инструментов, которые осуществляют верификацию бинарного кода программы // Новые информационные технологии в автоматизированных системах. 2014. № 17. С. 514–518.
2. Тихонов А.Ю., Аветисян А.И. Комбинированный (статический и динамический) анализ бинарного кода // Труды Института системного программирования РАН. 2012. Т. 22. С. 131–152.
3. Каушан В.В. Поиск ошибок выхода за границы буфера в бинарном коде программ // Труды Института системного программирования РАН. 2016. Т. 28. № 5. С. 135–144.
4. Бугеря А.Б., Ефимов В.Ю., Кулагин И.И., Падарян В.А., Соловьев М.А., Тихонов А.Ю. Программный комплекс для выявления недеklarированных возможностей в условиях отсутствия исходного кода // Труды Института системного программирования РАН. 2019. Т. 31. № 6. С. 33–64. DOI:10.15514/ISPRAS-2019-31(6)-3
5. Buinevich M., Izrailov K., Vladiko A. Metric of vulnerability at the base of the life cycle of software representations // Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT, Chuncheon, South Korea, 11–14 February 2018). IEEE, 2018. PP. 1–8. DOI:10.23919/ICACT.2018.8323940
6. Трошина Е.Н., Чернов А.В. Восстановление типов данных в задаче декомпилирования в язык C // Прикладная информатика. 2009. № 6(24). С. 99–117.
7. Буйневич М.В., Израйлов К.Е., Покусов В.В., Тайлаков В.А., Федудина И.Н. Интеллектуальный метод алгоритмизации машинного кода в интересах поиска в нем уязвимостей // Защита информации. Инсайд. 2020. № 5(95). С. 57–63.
8. Obert J., Loffredo T. Efficient Binary Static Code Data Flow Analysis Using Unsupervised Learning // Proceedings of the 4th International Conference on Artificial Intelligence for Industries (AI4I, Laguna Hills, USA, 20–22 September 2021). IEEE, 2021. PP. 89–90. DOI:10.1109/AI4I51902.2021.00030
9. Jia X., Bin Z., Chao F., Chaojing T. An Automatic Evaluation Approach for Binary Software Vulnerabilities with Address Space Layout Randomization Enabled // Proceedings of the International Conference on Big Data Analysis and Computer Science (BDACS, Kunming, China, 25–27 June 2021). IEEE, 2021. PP. 170–174. DOI:10.1109/BDACS53596.2021.00045
10. Израйлов К.Е. Применение генетических алгоритмов для декомпиляции МК // Защита информации. Инсайд. 2020. № 3(93). С. 24–30.
11. Загинайло М.В., Фатхи В.А. Генетический алгоритм как эффективный инструмент эволюционных алгоритмов // Инновации. Наука. Образование. 2020. № 22. С. 513–518.
12. Максимова Е.А. Модель состояний субъектов критической информационной инфраструктуры при деструктивных воздействиях в статичном режиме // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 65–72. DOI:10.31854/1813-324X-2021-7-3-65-72.

* * *

The Genetic Decompilation Concept of the Telecommunication Devices Machine Code

K. Izrailov^{1, 2} 

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

²St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, 199178, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-95-109

Received 1st December 2021

Revised 20th December 2021

Accepted 21st December 2021

For citation: Izrailov K. The Genetic Decompilation Concept of the Telecommunication Devices Machine Code. *Proc. of Telecom. Universities*. 2021;7(4):95–109. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-95-109

Abstract: Reverse engineering correct source code from a machine code to find and neutralize vulnerabilities is the most pressing problem for the field of telecommunications equipment. The decompilation techniques applicable for this have potentially reached their evolutionary limit. As a result, new concepts are required that can make a quantum leap in problem solving. Proceeding from this, the paper proposes the concept of genetic decompilation, which is a solution to the problem of multiparameter optimization in the form of iterative approximation of instances of the source code to the "original" one which will compile to the given machine code. This concept is tested by conducting a series of experiments with the developed software prototype using a basic example of machine code. The results of the experiments prove the proof of the concept, thereby suggesting new innovative directions for ensuring information security in this subject area.

Keywords: information security, telecommunications equipment, machine code, vulnerability, reverse engineering, decompilation, artificial intelligence, genetic algorithm, proof of concept.

FUNDING

The reported study was partially funded by the budget project 0073-2019-0002.

References

1. Gurin R.E. Review and Analysis of Tools that Verify the Binary Code of the Program. *Novye informatsionnye tekhnologii v avtomatizirovannykh sistemakh*. 2014;17:514–518. (in Russ.)
2. Tikhonov A.Yu., Avetisyan A.I. Combined (Static and Dynamic) Analysis of Binary Code. *Proceedings of the Institute for System Programming of the RAS*. 2012;22:131–152. (in Russ.)
3. Kaushan V.V. Buffer Overrun Detection Method in Binary Code. *Proceedings of the Institute for System Programming of the RAS*. 2016;28(5):135–144. (in Russ.)
4. Bugerya A.B., Efimov V.Yu., Kulagin I.I., Padaryan V.A., Solovov M.A., Tikhonov A.Yu. A Software Complex for Revealing Malicious Behavior in Untrusted Binary Code. *Proceedings of the Institute for System Programming of the RAS*. 2019;31(6):33–64. (in Russ.) DOI:10.15514/ISPRAS-2019-31(6)-3
5. Buinevich M., Izrailov K., Vladko A. Metric of vulnerability at the base of the life cycle of software representations. *Proceedings of the 20th International Conference on Advanced Communication Technology, ICACT, 11–14 February 2018, Chuncheon, South Korea*. IEEE; 2018. p.1–8. DOI:10.23919/ICAICT.2018.8323940
6. Troshina K.N., Chernov A.V. Type Reconstruction for C Decompilation. *Journal of Applied Informatics*. 2009;6(24):99–117. (in Russ.)
7. Buinevich M.V., Izrailov K.E., Pokusov V.V., Tailakov V.A., Fedulina I.N. An Intelligent Method of Machine Code Algorithmization for Vulnerabilities Search. *Zashita informacii. Inside*. 2020;5(95):57–63. (in Russ.)
8. Obert J., Loffredo T. Efficient Binary Static Code Data Flow Analysis Using Unsupervised Learning. *Proceedings of the 4th International Conference on Artificial Intelligence for Industries, AI4I, 20–22 September 2021, Laguna Hills, USA*. IEEE; 2021. p.89–90. DOI:10.1109/AI4I51902.2021.00030
9. Jia X., Bin Z., Chao F., Chaojing T. An Automatic Evaluation Approach for Binary Software Vulnerabilities with Address Space Layout Randomization Enabled. *Proceedings of the International Conference on Big Data Analysis and Computer Science, BDACS, 25–27 June 2021, Kunming, China*. IEEE; 2021. p.170–174. DOI:10.1109/BDACS53596.2021.00045
10. Izrailov K.E. Applying of Genetic Algorithms to Decompile Machine Code. *Zashita informacii. Inside*. 2020;3(93):24–30. (in Russ.)
11. Zaginailo M.V., Fatkhi V.A. Genetic Algorithm as an Effective Tool for Evolutionary Algorithms. *Innovatsii. Nauka. Obrazovanie*. 2020;22:513–518. (in Russ.)
12. Maximova E.A. Model of the States of Critical Information Infrastructure Subjects under Destructive Influences in Static Mode. *Proc. of Telecom. Universities*. 2021;7(3):65–72. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-65-72.

Сведения об авторе:

**ИЗРАИЛОВ
Константин Евгеньевич**

кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, старший научный сотрудник Санкт-Петербургского федерального исследовательского центра Российской академии наук,
konstantin.izrailov@mail.ru

 <https://orcid.org/0000-0002-9412-5693>

Artificial Intelligence-Based Aircraft Accident Threat Parrying Method

A. Kulik¹ 

¹Bauman Moscow State Technical University,
Moscow, 105005, Russian Federation

*E-mail: kulikalekse@yandex.ru

Информация о статье

Received 28th October 2021

Revised 16th November 2021

Accepted 18th November 2021

For citation: Kulik A. Artificial Intelligence-Based Aircraft Accident Threat Parrying Method. *Proc. of Telecom. Universities*. 2021;7(4):110–117. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-110-117

Abstract: An anti-aircraft accident method is proposed, implemented in the decision support module, which is the main element of the flight safety control system and is a dynamic expert system. On the basis of the proposed method, recommendations are formed to the threat countering crew accidents using the information about its psychophysical state, the technical state of an aircraft, external influencing factors, as well as a forecast of changes in flight conditions. The advantage of the proposed method is the ability to identify the immediate threat of an accident, as well as the development of management decisions to reduce the impact of the cause of the accident on flight safety. The peculiarity of the method of parrying the threat of an aircraft accident is the classification of management decisions depending on the flight conditions of the aircraft, which will reduce the computational costs for generating a threat parrying signal. Numerical modeling of the work using the assessment of a set of decision support rules made it possible to confirm its performance. The results can be used in systems development for safety of an aircraft's flight, the mathematical support of decision support systems.

Keywords: flight safety, expert system, decision support.

Introduction

In recent years, the active development of aviation technology has largely helped to raise the level of flight safety of aircraft of various types. One of the methods to ensure flight safety is the use of various decision support systems as part of the onboard complex of the vessel. For example, an intelligent decision support system that is element of a complex control system and used for intelligent recommendation to aircraft crew actions in the form of expert solutions [1].

The operation of the system is based on obtaining and evaluating information about the hardware and software condition of the onboard equipment and the flight conditions of the aircraft. Another example of aircraft flight safety devices are systems that averting the threat of an aircraft incident on the runway [2–3]. Such systems transmit information to the aircraft crew in the form of sound and light alerts, characterizing the excess of the permissible speed and the wrong flight route during the landing approach.

There is also the “Method for supporting an aircraft operator in hazardous situations” [4], during the implementation of which knowledge baselines are formed regarding the flight modes of aircraft and could

be the threats of aircraft incidents. Later, on the basis of the expert system, the serviceability of the airborne equipment complex (AEC) of the aircraft, the effectiveness of the pilot's actions and the type of signaling is defined.

Based on the results of the operation of the expert system, information is generated about the failure of the AEC elements, the deterioration of flight conditions, the degree of an aviation accident. Based on the information received and analyzed, the system issues instructions to the pilot to resist an aviation catastrophe. In the absence of a positive reaction from the pilot parry the threat, the aircraft is controlled by an automatic control system.

Also, the operation of the system includes the operator's actions by the ground control point, which, with the help of a password, can allow the crew to control the aircraft without restrictions from the side of the aircraft's automatic flight control system (AFCS). With the planned elimination of the danger of an aircraft accident is required without limiting the actions of the raft, then the operator of the ground control post enters the corresponding password, which is transmitted to the expert system of the aircraft. In

case of operational parrying of the aircraft accident and violation aircraft flight operation mode, its control is transmitted to the AFCS of the aircraft.

The disadvantage of such systems is the lack of an integrated approach to evaluation of aircraft flight safety on the basis of the aggregate influence of external and internal influence factors, including considering the prognosis of changes in them. The use of emergency forecasting devices at an early stage allows the team to warn the accident in advance and subsequently fend it off. Therefore, a promising option for enhancing aircraft flight safety is its flight safety control system. The structural diagram of the aircraft safety control system is shown in Figure 1.

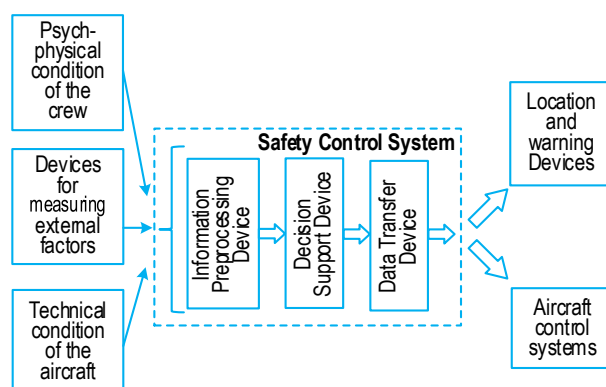


Fig 1. Structural Diagram of the Aircraft Safety Control System

The main elements of the proposed aircraft flight safety control system are information preprocessing device, decision support device and data transfer device. The preliminary data processing consists in the formation of electrical signals characterizing the excess current values of aircraft flight safety coefficients based on data obtained from the information measuring systems of the onboard equipment complex. Later, on the basis of information about changes in the flight conditions of the aircraft, the decision support device forms a conclusion characterizing the degree of danger of the flight event and methods for its elimination.

In the meantime, each group contains a list of input variables that measure the values of flight safety factors and their effect on flight conditions. A feature of these factors is their weak formalization. Therefore, the input variables of the flight safety control system are transformed into the form of linguistic variables. Each linguistic variable is defined on a set of fuzzy values that relate to a certain space-time interval. The representation of the input data of the decision support unit in the form of linguistic variables allows their processing by the fuzzy logic device, which is widely used in decision support devices and aircraft control systems [5–12].

Formulation of the problem

The purpose of this work is to design the method for decision support (DS) for the crew, which allows the formation of recommendations to the pilot and signals

to the aircraft control system to counter the accident threat, based on the current and predicted flight conditions of the aircraft.

To achieve this goal, it is necessary to carry out the following main stages: formalization of the input variables of the algorithm, formation of a set of decision support rules and modeling of an accident threat assessment.

Formalization of Input Variables

The proposed decision support device belongs to the class of dynamic expert systems, a feature of which is the formation of instructions for the operator to counter an accident, taking into account the change in the state of the input variables at a given time interval. The structure scheme of the decision support device (DSD) is shown in Figure 2 [13].

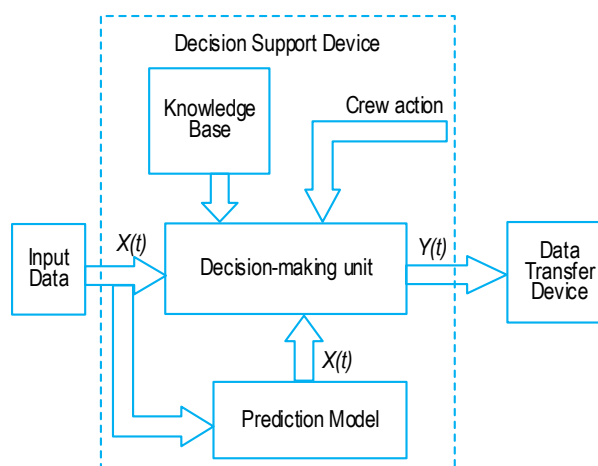


Fig. 2. Structure Scheme Decision Support Device

Here $X(t)$ – array of input data after preprocessing; $\hat{X}(t)$ – the results of predicting the threat of an aviation accident; $Y(t)$ – output values from decision support units that describe the instructions given to the pilot to avert the risk of an emergency or to parry signals by onboard automated systems.

The input of the device receives variables that are associated with external and internal influences and affect the safe flight environment of the aircraft. Flight safety assessment is carried out on the basis of information on the technical state of the control object, psychophysical characteristics of the crew and flight weather conditions. Also, the inputs of the decision support unit are the values of the prognosis of changes in the controlled variables, the flight conditions of the aircraft and the current value of the accident risk. The output values of the device are instructions generated for the pilot to eliminate the risk of the catastrophic, as well as signals to counter it provided by onboard automation systems. A formalized representation of the input variables of the decision-making unit is presented in Table 1.

TABLE 1. Input Variables of the Decision – Making Block

№	Group	Variable	Current Variable Designation	Forecast Variable Designation	Variable Values	Variable Value Notation
1.	The Psychophysical State of the Pilot	Fatigue	X_{11}	$\widetilde{X}_{11}$	Low Average High	F_1 F_2 F_3
		Attention	X_{12}	$\widetilde{X}_{12}$	High Average Low Distracted	K_1 K_2 K_3 K_4
		Level of Training (Competence)	X_{13}	$\widetilde{X}_{13}$	High Average Low	F_1 F_2 F_3
		Stress	X_{14}	$\widetilde{X}_{14}$	No Low Average High	K_1 K_2 K_3 K_4
2.	Aircraft Technical Condition	Failure of Functionally Significant Elements	X_{21}	$\widetilde{X}_{21}$	Minor Emergency Catastrophic	F_1 F_2 F_3
		Deformation of Structural Members	X_{22}	$\widetilde{X}_{22}$	Absent Minor Significant Critical	K_1 K_2 K_3 K_4
		Aircraft Controllability and Stability	X_{23}	$\widetilde{X}_{23}$	High Average Low	F_1 F_2 F_3
		Error in the Software of Aircraft Control Systems	X_{24}	$\widetilde{X}_{24}$	Absent Minor Significant Critical	K_1 K_2 K_3 K_4
3.	External Influencing Factors	Headwind	X_{31}	$\widetilde{X}_{31}$	Weak Average Strong	F_1 F_2 F_3
		Visibility	X_{32}	$\widetilde{X}_{32}$	Good Bad	K_1 K_2
		Side Wind	X_{33}	$\widetilde{X}_{33}$	Weak Average Strong	F_1 F_2 F_3
4.	Pre-Processing Results	Flight Conditions	Z	$\widetilde{Z}$	Free Hard Emergency Catastrophic	K_1 K_2 K_3 K_4

The table shows the following variables:

a) Current Variables

X_{1i} – variables characterizing the psychophysical state of the pilot; X_{2i} – variables characterizing an aircraft technical condition; X_{3i} – variables characterizing an external influencing factors; Z – variables characterizing the pre-processing results;

b) Forecast Variables – $\widetilde{X}_{1i}$; $\widetilde{X}_{2i}$; $\widetilde{X}_{3i}$; $\widetilde{Z}$.

The table shows that each group is characterised by a set of input variables, on the basis of whom the state of flight protection factor and their affect on the risk of an emergency are evaluated. The peculiarity of this factors is their weak formalizability, therefore, the flight protection parameters of decision-making sustentancetors are represented in a linguistic form.

Together to evaluate the current flight environment of the airplane, it is expedient to use the feature of forecasting the threat of an aircraft incident, which provides for threefold stages: measurement of the

values of influence factors at a given range of flight, receiving their relationships over the prognostic time, estimating the critical values of these parameters during the prognostication time with the determination of the moment of their emergence. As a consequence of the proposed approaches to evaluating and forecasting the risk of an aircraft accident, it is feasible to determine the reason affecting the crash during a given time period, as well as to develop guidelines for the team to counter an aircraft accident. The representation of the input data of the decision support unit in the form of linguistic variables allows their processing using the fuzzy logic apparatus, which is widely used in decision support devices and aircraft control systems [14–20].

Formation of a Set of Rules for Decision Support

Table 1 shows that the decision support rule has a rather complex structure, the implementation of which

can lead to high computational costs. Therefore, it is advisable to structure the set of decision support rules into groups of aircraft flight conditions. It should be noted that the composition of the set of rules depends on the control object, its on-board equipment, functions performed and is determined in the process of developing the aircraft flight safety control system. Taking into account the division of the flight conditions of the vehicle into classes and applying the precedent matrix presented in [18], we obtain the following set of decision support rules.

1) Flight conditions are accident-free $Z = K_1$:

RULE <1>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_1, K_1\} \& X_{2j} = \{F_1, K_1\} \& X_{3j} = \\ = \{F_1, K_1\} \text{ THEN } Y = \{G_1\}, \end{aligned} \quad (1)$$

here G_1 – threat of aviation accident is absent, parrying is not required.

2) Flight conditions are hard $Z = K_2$:

RULE <2.1>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_3, K_3\} \& X_{2j} = \{F_1, K_1\} \& X_{3j} = \\ = \{F_1, K_2\} \text{ THEN } Y = \{G_2\}, \end{aligned}$$

RULE <2.2>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_3, K_4\} \& X_{2j} = \{F_1, K_1\} \& X_{3j} = \\ = \{F_1, K_2\} \text{ THEN } Y = \{G_2\}, \end{aligned} \quad (2)$$

RULE <2.3>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_2, K_2\} \& X_{2j} = \{F_1, K_1\} \& X_{3j} = \\ = \{F_1, K_2\} \text{ THEN } Y = \{G_2\}, \end{aligned}$$

here G_2 – the threat of accident is counteracted by means of automation, the object's controllability is increased by signals from automatic control systems, stability and controllability are improved.

3) Flight conditions are emergency $Z = K_3$:

RULE <3.1>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_1, K_3\} \& X_{2j} = \{F_3, K_4\} \& X_{3j} = \\ = \{F_2, K_1\} \text{ THEN } Y = \{G_3\}, \end{aligned}$$

RULE <3.2>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_1, K_1\} \& X_{2j} = \{F_2, K_4\} \& X_{3j} = \\ = \{F_3, K_1\} \text{ THEN } Y = \{G_3\}, \end{aligned} \quad (3)$$

RULE <3.3>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_3, K_4\} \& X_{2j} = \{F_2, K_3\} \& X_{3j} = \\ = \{F_1, K_1\} \text{ THEN } Y = \{G_4\}, \end{aligned}$$

RULE <3.4>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_2, K_2\} \& X_{2j} = \{F_1, K_1\} \& X_{3j} = \\ = \{F_3, K_2\} \text{ THEN } Y = \{G_4\}, \end{aligned}$$

here G_3 – signaling to the crew about failures on board the control object, threat of accident with subsequent parrying by the pilot on the instruction are transmitted of the speech translator; G_4 – ..., a threat, followed by

countermeasures by reconfiguring the control system of the object and landing on the nearest suitable site.

4) Flight conditions are catastrophic $Z = K_4$:

RULE <4.1>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_2, K_3\} \& X_{2j} = \{F_3, K_4\} \& X_{3j} = \\ = \{F_2, K_1\} \text{ THEN } Y = \{G_5\}, \end{aligned} \quad (4)$$

RULE <4.2>:

$$\begin{aligned} \text{IF } X_{1j} = \{F_3, K_4\} \& X_{2j} = \{F_3, K_4\} \& X_{3j} = \\ = \{F_3, K_4\} \text{ THEN } Y = \{G_5\}, \end{aligned}$$

here G_5 – signaling to the crew about failures on board the control object, the threat of accident with the requirement to leave the control object.

From the presented set of rules it can be realized that in presence of failures of aircraft control systems and deterioration of weather conditions of the flight, an emergency situation may arise, which is parried by the pilot. If during the flight there was a deterioration in the psychophysical phase of the pilot and weather conditions with a good technical condition of the control object, then the emergency situation is countered by the aircraft safety control system. From the presented set of rules, it can be understood that in device, is similar to that presented by formulas (1–4) in terms of the flight condition. The formed set of rules for countering the risk of the crash is used in the algorithm of the crew decision support device, the action of which is signaling at generating and issuing instructions to the crew to prevent an accident with the identification of the source of its threat.

Using the proposed set of rules and the values of the input variables of the aircraft flight safety control system, the simulation of the risk of an aviation crash was performed out with the issuance of instruction to the crew on its parry. Modeling of flight conditions was carried out for difficult and trouble-free aircraft flight conditions, taking into account failures of onboard equipment and changes in flight weather conditions. The characteristics of the results of simulation the flight conditions of the aircraft are shown in Figure 3–4.

In the course of computational simulation of the flying environment of the aircraft the following stars were received:

- with linguistic variables being one, the significance of flight conditions is 1.0, which equates to an accident-free flying mode, hence there is no danger of an emergency, and countering the danger is not needed when the significance is equal in (Figure 3);

- with linguistic input variables corresponding to difficult flight conditions (a low level of aircraft controllability and an increase in crew fatigue from a monotonous load), an improvement in flight conditions by means of automation is required, which corresponds to (Figure 4).

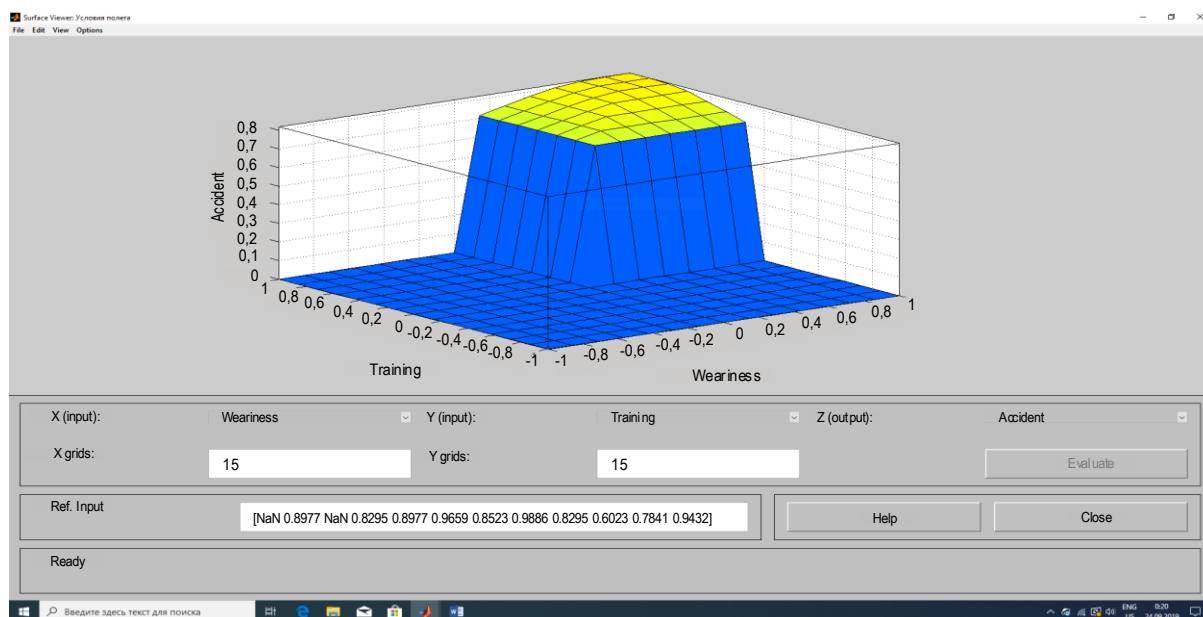


Fig. 3. Characteristics of the Results of Numerical Simulation of Aircraft Flight Conditions for an Accident-Free Situation

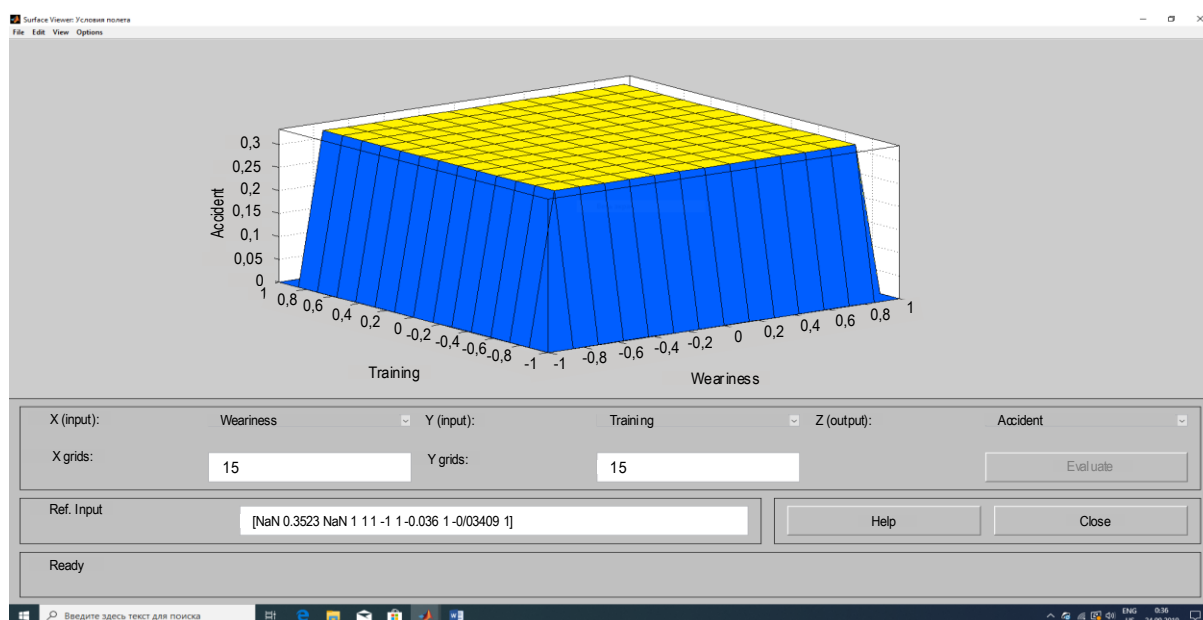


Fig. 4. Characteristics of the Results of Numerical Simulation of Aircraft Flight Conditions for a Complex Flight Condition

```

C:\USERS\ALEXEY\APPDATA\LOCAL\TEMP\GOALS000.EXE
Uslovia poleta
1. Uslovia poleta bezavarinie
2. Uslovia poleta sloznie
3. Uslovia poleta avarinie
4. Uslovia poleta katastroficheskie
5. Vihod iz program.

=>1
x11=f1-ustalost nizkay1. Yes
1x12=k1-vnimanie visokoe1. Yes
1x13=f1-uroven kompetencii vysokiy1. Yes
1x14=k1-stressa net1. Yes
1x21=f1-otkazov net1. Yes
1x22=k1-deformacii net1. Yes
1x23=f1-upravliaemost visokay1. Yes
1x24=k1-neznacitelnay oshibka P.O.1. Yes
1x31=f1-vstrechniy veter slabiy1. Yes
1x32=k1-vidimost horoshay1. Yes
1x33=f1-bokovoy veter slabiy1. Yes
1Ugroza AP otsutstvuet

```

a)

```

C:\USERS\ALEXEY\APPDATA\LOCAL\TEMP\GOALS000.EXE
Uslovia poleta
1. Uslovia poleta bezavarinie
2. Uslovia poleta sloznie
3. Uslovia poleta avarinie
4. Uslovia poleta katastroficheskie
5. Vihod iz program.

=>2
x11=f3-ustalost visokay1. Yes
1x12=k4-vnimanie rassenoel. Yes
1x13=f3-uroven kompetencii nizkiy1. Yes
1x14=k4-stressa visokiy1. Yes
1x21=f1-otkazov net1. Yes
1x22=k1-deformacii net1. Yes
1x23=f1-upravliaemost visokay1. Yes
1x24=k1-neznacitelnay oshibka P.O.1. Yes
1x31=f1-vstrechniy veter slabiy1. Yes
1x32=k2-vidimost plohay1. Yes
1x33=f1-bokovoy veter slabiy1. Yes
1Ugroza AP. Pariruetnya avtomatikoi.

```

b)

Fig. 5. Characteristics of the Test Results of the Decision Support System: a) under Non-Emergency Flight Conditions of the Aircraft; b) under Difficult Aircraft Flight Conditions

Based on the test methodology of the aircraft flight safety control system [21] and numerical simulation of flight conditions, the simulation of the formation of recommendations for countering the risk of the crash was carried out, the results of which are shown in Figure 5. From the information presented in Figure 5b, it follows that the decision support device is able to form instruction for the pilot on the actions of the risk of an accident through the means of on-board indication and signaling of the aircraft.

Based on the results of numerical simulation, it is feasible to define the conformity of a collection of rules of a decision support device to the index of completeness (IC) and absence of inconsistency (AI). So, when $IC = 1$, it corresponds to taking into account all possible states of input variables and changes in flight conditions. In turn, the validity of $AI \leq 0,4$ characterizes the absence of inconsistency between the output variables of the set of decision support rules for the same values of the input variables.

Thus, the proposed method makes it feasible to formulate advice to the crew and management signaling to parry the risk of an accident, taking into consideration the foretold changes in extrinsic and internal factors influencing the flight condition of the airship.

Conclusion

In the course of the work, a method of fending off the danger of an aircraft accident was designed, consisting in the creation of command instructions for the crew and signals of on-board automation equipment to counter the danger of an aircraft accident using data on the current and predicted flying conditions of the aircraft.

At the same moment, the input variables of the decision support unit were analyzed, a set of rules for the knowledge base was formed, on that basis simulations be conducted to evaluate and counter the risk of an aviation accident. When compiling a set of rules, they were assessed for completeness and the absence of inconsistency, the indicators of which characterize the formed set of rules for the possibility of being applied as part of the aviation system. The decision support method in the event of an aviation accident threat makes it possible to determine the actions of the crew in the process of piloting the vessel, depending on the air situation and the values of the variables affecting the flight safety. Based on the method of decision-making support of the crew, an algorithm for parrying the threat of an accident is proposed, the action of which is aimed at generating a signal that initializes instructions to the crew on countering the accident. A distinctive feature of the algorithm is the formation of an aircraft control signal in automatic mode in the absence of a positive response from the pilot to counter the threat of an accident. In addition, when developing the algorithm, a classification of the set of rules was proposed depending on the flight conditions of the aircraft, which allows reducing the computational costs for generating a signal to parry the threat of an accident. Further work on the creation of aircraft flight safety control systems is aimed at its software and hardware implementation, followed by ground testing and testing as part of flying laboratories. At the same time, ground tests of the system presuppose its testing at the semi-natural simulation stand with simulated aircraft flight and changing the values of flight safety variables, which will ensure verification of its software.

Reference

1. Sapogov V.A., Anisimov K.S., Novozhilov A.V. Fail-Safe Computer System for Complex of Aircraft Flight Control Systems. *Trudy MAI*. 2011;45. (in Russ.)
2. Glubokaya M.G. The look of the onboard Decision Support System on Passenger Aircraft Takeoff Stage. *Izvestiya RAN. Teoriya i sistemy upravleniya*. 2009;3:105–121. (in Russ.)
3. Shevchenko A.M., Nachinkina G.N., Solonnikov Y.I. Modeling of the Pilot Information Support Tools at the Aircraft Takeoff Stage. *Proceedings of the Moscow Institute of Electromechanics and Automation (MIEA)*. 2012;5:54–64. (in Russ.)
4. Sukholitko V.A. *Method of Operator Support in Dangerous Situations*. Patent RF, no. 2205442 C1 G05D, 02.10.2001. (in Russ.)
5. Wolf W. Cyber-physical system. *Computer*. 2009;42(3):88–89. DOI:10.1109/MC.2009.81
6. Rad C.R., Hancu O., Takacs I.A., Olteanu G. Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. *Agriculture and Agricultural Science Procedia*. 2015;6:73–79. DOI:10.1016/j.aaspro.2015.08.041
7. Lee J., Bagheri B., Kao H.-A. A Cyber-Physical Systems architecture for Industry. 4.0-based manufacturing systems. *Manufacturing Letters*. 2015;3:18–23. DOI:10.1016/j.mfglet.2014.12.001
8. Kupriyanovsky V., Namiot D., Sinyakov S. A Cyber-physical system as the basis for the digital economy. *The International Journal of Open Information Technologies*. 2016;4(2):18–25.
9. Kosko B. Fuzzy Systems as Universal Approximators. *IEEE Transactions on Computers*. 1994;43(11):1329–1333. DOI:10.1109/12.324566
10. Cordon O., Herrera F.A. General study on genetic fuzzy systems. *In Genetic Algorithms in Engineering and Computer Science*. John Wiley & Sons; 1995. p.33–57.
11. Averchenkov V.I., Miroshnikov V.V., Podvesovskiy A.G., Korostelyov D.A. Fuzzu and Hierarchical Models for Decision Support in Software Systems Implementation. *Proceedings of the 11th on Joint Conference Knowledge-Based Software Engineering, 17–20 September 2014, Volgograd, Russia. Communications in Computer and Information Science*. Cham: Springer; 2014. vol.466. p.410–422. DOI:10.1007/978-3-319-11854-3_35
12. Denisov M., Kozin A., Kamaev V., Davydova S. Solution on Decision Support in Determining of Repair Action Using Fuzzy

Logic and Agent System. *Proceedings of the 11th on Joint Conference Knowledge-Based Software Engineering, 17–20 September 2014, Volgograd, Russia. Communications in Computer and Information Science*. Cham: Springer; 2014. vol.466. p.533–541. DOI:10.1007/978-3-319-11854-3_46

13. Bolshakov A.A., Kulik A.A., Sergushov I.V., Skripal E.N. Design the Method for Aircraft Accident of Prediction. *Mekhatronika, Avtomatizatsiya, Upravlenie*. 2018;19(6):416–423. (in Russ.) DOI:10.17587/mau.19.416-423

14. Bolshakov A.A., Kulik A.A., Sergushov I.V., Skripal E.N. Development the Control System Algorithms Functioning of Flight Safety for the Aircraft of Helicopter Type. *Izvestia of Samara Scientific Center of the Russian Academy of Sciences*. 2016;18(1-2): 358–362. (in Russ.)

15. Fedunov B.E., Prokhorov M.D. Conclusion on the Precedent Knowledge Bases Airborne Intelligence Systems. *Iskusstvennyj intellekt i prinjatie reshenij*. 2010;3:63–72. (in Russ.)

16. Bahanov L.E., Demkin M.A., Fedunov B.E. Mathematical model of aircraft motion for knowledge bases of on-board operational advising expert systems. *Izvestiya RAN. Teoriya i sistemy upravleniya*. 2010;1:103–111. (in Russ.)

17. Nejmark M.S., Cesarskij L.G., Filimonjuk L.YU. Decision support model for aircraft entering the airport's area of responsibility. *All-Russian Scientific-Technical Journal "Polyot" ("Flight")*. 2013;3:31–37. (in Russ.)

18. Gavrilova T.A., Horoshevskiy V.F. *Knowledge Bases of Intelligent Systems*. St. Petersburg: Piter Publ.; 2000. 384 p. (in Russ.)

19. Kuklev E.A. Flight Safety Control of the Basis of Uncertain Risk Evaluation with Non-Routine Flight Conditions Involved. *Civil Aviation High Technologies*. 2016;226:199–205. (in Russ.)

20. Bolshakov A.A., Kulik A.A., Sergushov I.V., Skripal E.N. Aviation Accident Threat Intelligent Assessment Method. *Vestnik komp'yuternykh i informatsionnykh tekhnologii (Herald of Computer and Information Technologies)*. 2018;5(167):3–9. (in Russ.) DOI:10.14489/vkit.2018.05.pp.003-009

21. Kulik A.A. Development of Methods for Test of Air Flight Safety System. *Vestnik of Samara State Technical University. Technical Sciences Series*. 2019;4(64):30–42. (in Russ.)

* * *

Метод парирования угрозы авиационного происшествия на основе искусственного интеллекта

А.А. Кулик¹ 

¹Московский государственный технический университет имени Н.Э. Баумана, Москва, 105005, Российская Федерация

Информация о статье

DOI:10.31854/1813-324X-2021-7-4-110-117

Поступила в редакцию 28.10.2021

Поступила после рецензирования 16.11.2021

Принята к публикации 18.11.2021

Ссылка для цитирования: Кулик А.А. Метод парирования угрозы авиационного происшествия на основе искусственного интеллекта // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 110–117. DOI:10.31854/1813-324X2021-7-4-110-117

Аннотация: Предлагается метод парирования угрозы авиационного происшествия, реализованный в модуле поддержки принятия решений, который является основным элементом системы управления безопасностью полета летательного аппарата и представляет динамическую экспертную систему. На основе предложенного метода формируются рекомендации экипажу по парированию угрозы авиационного происшествия на основе информации о его психофизическом состоянии, техническом состоянии объекта управления, внешних воздействующих факторов, а также прогноза изменения условий полета. Преимущество предложенного метода является возможность идентификации непосредственной угрозы авиационного происшествия, а также выработка управленческих решений по уменьшению влияния причины происшествия на безопасность полета. Особенность метода парирования угрозы авиационного происшествия заключается в классификации управленческих решений в зависимости от условий полета воздушного судна, что позволит снизить вычислительные затраты на формирование сигнала парирования угрозы. Численное моделирование работы с использованием оценки набора правил поддержки принятия решений позволило подтвердить его работоспособность. Полученные результаты могут быть использоваться при разработке систем управления безопасностью полета летательных аппаратов, а именно математического обеспечения систем поддержки принятия решений.

Ключевые слова: *безопасность полета, экспертная система, поддержка принятия решений.*

Список используемых источников

1. Сапогов В.А., Анисимов К.С., Новожилов А.В. Отказобезопасная вычислительная система для комплексных систем управления полетом летательных аппаратов // Труды МАИ. 2010. № 45.
2. Глубокая М.Г. Облик бортовой системы поддержки принятия решений на этапе взлета пассажирского самолета // Известия РАН. Теория и системы управления. 2009. № 3. С. 105–121.
3. Шевченко А.М., Начинкина Г.Н., Солонников Ю.И. Моделирование средств информационной поддержки пилота на этапе взлета самолета // Труды Московского института электромеханики и автоматики (МИЭА). 2012. № 5. С. 54–64.
4. Сухолитко В.А. Способ поддержки оператора в опасных ситуациях. Патент на изобретение RUS 2205442 C1 G05D1/00 от 02.10.2001. Оpubл. 27.05.2003.
5. Wolf W. Cyber-physical system // Computer. 2009. Vol. 42. Iss. 3. PP. 88–89. DOI:10.1109/MC.2009.81
6. Rad C.R., Hancu O., Takacs I.A., Olteanu G. Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture // Agriculture and Agricultural Science Procedia. 2015. Vol. 6. PP. 73–79. DOI:10.1016/j.aaspro.2015.08.041
7. Lee J., Bagheri B., Kao H.-A. A Cyber-Physical Systems architecture for Industry. 4.0-based manufacturing systems // Manufacturing Letters. 2015. Vol. 3. PP. 18–23. DOI:10.1016/j.mfglet.2014.12.001
8. Kupriyanovsky V., Namiot D., Sinyakov S. A Cyber-physical system as the basis for the digital economy // The International Journal of Open Information Technologies. 2016. Vol. 4. № 2. PP. 18–25.
9. Kosko B. Fuzzy Systems as Universal Approximators // IEEE Transactions on Computers. 1994. Vol. 43. Iss. 11. PP. 1329–1333. DOI:10.1109/12.324566
10. Cordon O., Herrera F.A. General study on genetic fuzzy systems // In Genetic Algorithms in Engineering and Computer Science. John Wiley & Sons. 1995. PP. 33–57.
11. Averchenkov V.I., Miroshnikov V.V., Podvesovskiy A.G., Korostelyov D.A. Fuzzu and Hierarchical Models for Decision Support in Software Systems Implementation // Proceedings of the 11th on Joint Conference Knowledge-Based Software Engineering (Volgograd, Russia, 17–20 September 2014). Communications in Computer and Information Science. Cham: Springer, 2014. Vol. 466. PP. 410–422. DOI:10.1007/978-3-319-11854-3_35
12. Denisov M., Kozin A., Kamaev V., Davydova S. Solution on Decision Support in Determining of Repair Action Using Fuzzy Logic and Agent System // Proceedings of the 11th on Joint Conference Knowledge-Based Software Engineering (Volgograd, Russia, 17–20 September 2014). Communications in Computer and Information Science. Cham: Springer, 2014. Vol. 466. PP. 533–541. DOI:10.1007/978-3-319-11854-3_46
13. Большаков А.А., Кулик А.А., Сергушов И.В., Скрипаль Е.Н. Метод прогнозирования авиационного происшествия летательного аппарата // Мехатроника, автоматизация, управление. 2018. Т. 19. № 6. С. 416–423. DOI:10.17587/mau.19.416-423.
14. Большаков А.А., Кулик А.А., Сергушов И.В. Разработка алгоритмов функционирования системы управления безопасностью полета летательного аппарата вертолетного типа // Известия Самарского научного центра РАН. 2016. Т. 18. № 1-2. С. 358–362.
15. Федунев Б.Е., Прохоров М.Д. Вывод по прецеденту в базах знаний бортовых интеллектуальных систем // Искусственный интеллект и принятие решений. 2010. № 3. С. 63–72.
16. Баханов Л.Е., Демкин М.А., Федунев Б.Е. Математическая модель движения самолета для баз знаний бортовых оперативно-советующих экспертных систем // Известия РАН. Теория и системы управления. 2010. № 1. С. 103–111.
17. Неймарк М.С., Цесарский Л.Г., Филимонок Л.Ю. Модель поддержки принятия решений при входе воздушных судов в зону ответственности аэропорта // Полет. Общероссийский научно-технический журнал. 2013. № 3. С. 31–37.
18. Гаврилова Т.А., Хорошевский В.Ф. Базы знаний интеллектуальных систем. СПб: Питер, 2000. 384 с.
19. Куклев Е.А. Управление безопасностью полетов воздушных судов на основе нечетких оценок рисков возникновения нештатных условий полетов // Научный вестник МГТУ ГА. 2016. № 226. С. 199–205.
20. Большаков А.А., Кулик А.А., Сергушов И.В., Скрипаль Е.Н. Интеллектуальный метод оценки угрозы авиационного происшествия // Вестник компьютерных и информационных технологий. 2018. № 5(167). С. 3–9. DOI:10.14489/vkit.2018.05.pp.003-009
21. Кулик А.А. Разработка методики испытания системы управления безопасностью полета воздушного судна // Вестник Самарского государственного технического университета. Серия: Технические науки. 2019. № 4(64). С. 30–42.

Сведения об авторе:

КУЛИК
Алексей Анатольевич

кандидат технических наук, доцент, доцент кафедры Системы автоматического управления Московского государственного технического университета имени Н.Э. Баумана, kulikalekse@yandex.ru

 <https://orcid.org/0000-0002-4099-1641>

ТРУДЫ МОЛОДЫХ УЧЕНЫХ

*Основой всей научной работы служит убеждение,
что мир представляет собой упорядоченную
и познаваемую сущность...*

Альберт Эйнштейн

1.2.2

2.2.6

2.2.13

2.2.14

2.2.15

2.2.16

2.3.1

2.3.6

Безопасная передача информации при помощи двух методов бесключевой криптографии

А.С. Герасимович¹ ^{*}

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

^{*}Адрес для переписки: Alexgera93@gmail.com

Информация о статье

Поступила в редакцию 06.12.2021

Поступила после рецензирования 21.12.2021

Принята к публикации 22.12.2021

Ссылка для цитирования: Герасимович А.С. Безопасная передача информации при помощи двух методов бесключевой криптографии // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 119–127. DOI:10.31854/1813-324X-2021-7-4-119-127

Аннотация: В статье рассматриваются два протокола обеспечения информационной безопасности, использующие свойства каналов связи между пользователями. Первый из них основан на известном протоколе передачи конфиденциальных сообщений Шамира. Доказывается, что в нем может быть реализована криптосистема РША, но неприменимы такие криптосистемы, как Рабина, Мак-Элис, на решетках и потоковые шифры. Основное содержание статьи посвящено описанию второго протокола распределения ключей по постоянному и бесшумному каналу связи (типа Интернет). Доказано, что он может обеспечить высокую надежность распределения ключей и требуемый уровень их секретности в терминах Шенноновской информации, причем при отсутствии каких-либо дополнительных требований к каналам связи и безо всяких криптографических предположений.

Ключевые слова: криптосистемы с открытым ключом, распределение ключей, безопасность на физическом уровне, усиление секретности, квантовые компьютеры, протоколы.

1. Введение

Общеизвестно, что основным методом обеспечения информационной безопасности является стойкое шифрование сообщений. Это тем более верно сейчас, поскольку появились открытые стандарты шифрования [1, 2]: 3DES, AES, GOST, RSA и другие, которые, насколько можно судить по доступным литературным источникам, обеспечивают невозможность выделения зашифрованной информации без знания ключей дешифрования и в обозримом будущем. Однако, именно такие ключи, а также их распределение между пользователями, нуждаются в обмене конфиденциальной информацией, и оказываются «узким местом» современной криптографии.

Действительно, в современном «Цифровом Мире» такие ключи должны передаваться каким-то цифровым способом между пользователями по каналам связи, что требует их защиты от перехвата злоумышленниками. Казалось бы, такая проблема была уже решена ранее благодаря изобретению У. Диффи и М. Хеллмана [2], так называемых криптосистем с открытым ключом (КОК). Хотя более точно их можно было бы назвать криптосистемами

с открытыми ключами шифрования. В случае КОК, шифрование сообщений производится на общедоступных ключах, тогда как дешифрование выполняется на закрытых ключах; и их имеют только пользователи, которым принадлежит передаваемая конфиденциальная информация. Причем знание открытых ключей не облегчает нахождение закрытых ключей. Подобные условия обеспечиваются сложностью решения (в обозримое время) так называемых трудных математических задач. Например, таких, как факторизация целых чисел, вычисление дискретных логарифмов и так далее. Это условие называют обычно «криптографическими предположениями» (*от англ. Cryptographic Assumptions*).

Хотя изобретение КОК и явилось в свое время подлинной революцией в криптографии, но со временем выяснились его некоторые слабости, такие как:

– возможность простого полиномиального решения трудных задач при помощи квантовых компьютеров, которые в будущем времени возможно будут реализованы [3];

– необходимость иметь сертифицированный центр для накопления и передачи открытых ключей пользователям;

– достаточная сложность теоретико-числовых вычислений для выполнения процедур шифрования или дешифрования в системах КОК.

Для решения первой проблемы были предложены так называемые постквантовые криптосистемы, то есть такие, которые не могут быть взломаны даже при практическом появлении квантовых компьютеров. Такова, например, криптосистема Мак-Элиса [1], которая, однако, требует большой длины ключа и высокой вычислительной сложности шифрования/дешифрования. Еще одним направлением возможного распределения ключей является использование квантовой криптографии [4], однако ее использование не всегда возможно, так как требует наличия специального квантового оборудования.

В последнее время развивается так же такое направление распределения ключей, или точнее обеспечения безопасности шифрования, как Keyless Cryptography, основанное на присутствии некоторых, обладающих определенными физическими свойствами, физических каналов связи (*от англ. Physical Layer Security*) [5]. Именно развитию этого направления и посвящена настоящая статья.

В разделе 2 исследуются алгоритмы, позволяющие обеспечить безопасность шифрования за счет использования каналов с обратной связью и, так называемых криптосистем коммутативного шифрования (КШ). В разделе 3 описывается метод распределения ключей, основанный на использовании постоянных бесшумных открытых каналов связи (типа Интернет) и концепции усиления секретности. Заключение подводит итог данной работе, и представляет возможные перспективы проведения исследований в данных направлениях в будущем.

2. Использование коммутативного шифрования

В [6] был описан предложенный ранее Шамиром метод шифрования/дешифрования безо всякого предварительного распределения ключевых данных. Для его использования необходимо выполнение следующего требования для алгоритмов шифрования, которое можно условно назвать коммутативным шифрованием (КШ):

$$f_{K_A}(f_{K_B}(M)) = f_{K_B}(f_{K_A}(M)), \quad (1)$$

где $f_{K_A}(M)$, $f_{K_B}(M)$ – алгоритмы (функции) шифрования сообщения M на ключах K_A , K_B , соответственно. В словесной формулировке требование (1) означает, что результат шифрования любого сообщения M не зависит от того, в каком порядке будут использованы ключи: сначала K_B , а потом K_A , или наоборот, сначала K_A , а потом K_B .

Действительно, при выполнении условия (1) передача зашифрованного сообщения M от корреспондента A к корреспонденту B с возможностью его расшифровки последним, причем при отсутствии всякого предварительного распределения общих ключей между A и B , доказывается представленным на рисунке 1 протоколом (при наличии у A и B каналов обратной связи).

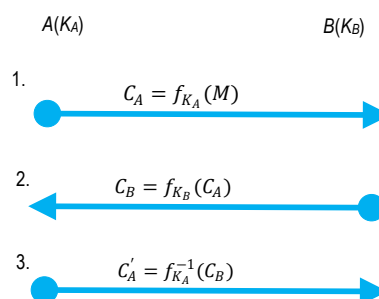


Рис. 1. Протокол секретной передачи сообщений

Fig. 1. Secret Message Transfer Protocol

Так, $C_B = f_{K_B}(C_A) = f_{K_B}(f_{K_A}(M))$, и тогда:

$$C'_A = f_{K_A}^{-1}(C_B) = f_{K_A}^{-1}(f_{K_B}(f_{K_A}(M))). \quad (2)$$

При выполнении условия (1), получаем из (2):

$$\begin{aligned} C'_A &= f_{K_A}^{-1}(f_{K_B}(f_{K_A}(M))) = \\ &= f_{K_A}^{-1}(f_{K_A}(f_{K_B}(M))) = f_{K_B}(M). \end{aligned} \quad (3)$$

Поскольку по определению преобразований шифрования $f_{K_A}(M)$ и дешифрования $f_{K_A}^{-1}(M)$ на одном и том же ключе они дают исходное M , получаем в (3) действительно $f_{K_B}(M)$. Наконец, B восстанавливает M , выполняя преобразование дешифрования $f_{K_B}^{-1}(f_{K_B}(M)) = M$. Заметим, что условие (1) требуется только для преобразования шифрования, но не для обоих преобразований – шифрования и дешифрования!

Однако возникает вопрос, существуют ли какие-то преобразования шифрования, удовлетворяющие (1)? Докажем далее, что примером алгоритма, соответствующего условию (1), может служить широко известная криптосистема Райвеста – Шамира – Адлемана (РША), описанная в [1, 7], а также в других источниках.

Как известно, для шифра РША выполняются следующие условия:

- $n = p \cdot q$, где $p \neq q$ простые числа; n – модуль;
- $\varphi = (p-1)(q-1)$;
- $1 \leq e_A \leq \varphi$, $1 \leq e_B \leq \varphi$, где e_A , e_B – целые положительные числа, причем $\gcd(e_A, \varphi) = 1$, $\gcd(e_B, \varphi) = 1$, $1 \leq M \leq n-1$ целые числа.

Тогда, если A и B имеют одинаковые модули n , то условие (1) может быть представлено следующим образом:

$$(M^{e_A} \bmod n)^{e_B} \bmod n = (M^{e_B} \bmod n)^{e_A} \bmod n. \quad (4)$$

Справедливость (4) следует из хорошо известных свойств модульных операций, однако поскольку в источниках [2] и [6] явно это равенство отсутствует, то имеет смысл доказать его ниже еще раз для убедительности.

Очевидно, что по определению модульных операций

$$M^{e_A} \bmod n = M^{e_A} - nl, \quad (5)$$

где l – некоторое целое положительное число.

Подставляя (5) в левую часть (4), получим:

$$\begin{aligned} (M^{e_A} \bmod n)^{e_B} \bmod n &= (M^{e_A} - nl)^{e_B} \bmod n = \\ &= (M^{e_A \cdot e_B} - n * \text{БН})^{l_B} \bmod n, \end{aligned} \quad (6)$$

где БН – бином Ньютона без первого члена из с вынесенным общим множителем n .

Далее по свойству модульных операций, получим из (6):

$$n * \text{БН} \bmod n = 0, \quad (7)$$

тогда из (6) и (7) получим:

$$(M^{e_A} \bmod n)^{e_B} \bmod n = M^{e_A \cdot e_B} \bmod n. \quad (8)$$

Аналогично (8), легко показать, что для правой части (4) будет справедливо аналогичное равенство:

$$(M^{e_B} \bmod n)^{e_A} \bmod n = M^{e_B \cdot e_A} \bmod n. \quad (9)$$

Совпадение (8) и (9) доказывает справедливость равенства (4).

Пример. Пусть $p = 3$, $q = 5$, $M = 2$, $e_A = 3$, $e_B = 5$. Тогда можно проверить, что обе части (4) равны 8.

Поскольку, как уже было сказано выше, данный алгоритм соответствует системе РША, то очевидно, что в этом случае алгоритм шифрования в (1) будет иметь вид:

$$E = f_{K_{A(B)}}(M) = M^{e_{A(B)}} \bmod n, \quad (10)$$

а алгоритм дешифрования:

$$f_{K_{A(B)}}^{-1}(E) = E^{d_{A(B)}} \bmod n, \quad (11)$$

где $d = e^{-1} \bmod \varphi$.

Стойкость данной криптосистемы будет определяться криптографическим предположением о невозможности факторизации модуля n для допустимого времени криптоанализа и допустимого объема оборудования; другим требованием для обеспечения защищенности такой криптосистемы является предположение о сложности вычисления дискретных логарифмов, поскольку иначе на втором шаге протокола криптоаналитик, зная C_B , сможет вычислить ключ дешифрования d [1]. Поскольку система РША является «самодостаточной», то, казалось бы, описанный выше протокол и не потребует, если конечно, на стадии шифрования известен открытый ключ $e_{A(B)}$ противоположного корреспондента. Это

может быть достигнуто или при помощи открытой передачи такого ключа по каналу связи от A к B или наоборот, или же от сертифицированного центра, который предварительно получает такие ключи и гарантирует их подлинность.

Некоторым преимуществом описанного выше протокола может служить факт, что корреспондент, шифрующий сообщение, может даже и не знать открытого корреспондента, которому оно предназначается, что не отменяет, конечно, необходимости аутентификации пользователей для исключения атаки имперсонализации.

В качестве еще одного претендента на выполнение условия (1), рассмотрим криптосистему Рабина [1]. В этом случае, в качестве открытого ключа выступает целое число $n = p \cdot q$, где p и q – простые неизвестные числа, а в качестве секретного ключа используются именно эти числа. Шифрование выполняется по правилу:

$$C = M^2 \bmod n, \quad (12)$$

где сообщение M – любое целое число в интервале $0 \leq M \leq n - 1$.

Применительно к данному случаю условие (1) принимает следующий вид:

$$(M^2 \bmod n_A)^2 \bmod n_B = (M^2 \bmod n_B)^2 \bmod n_A. \quad (13)$$

Легко проверить, что, по крайней мере, при некотором выборе параметров равенство (13) не выполняется. Действительно, если взять $p = 3$, $q = 5$, что дает $n_A = 15$ и $p = 11$, $q = 7$, а $n_B = 77$, то при выборе сообщения $M = 5$ левая часть (13) оказывается равной 23, а правая – 10 и, следовательно, равенство (13) не выполняется. То есть криптосистема Рабина не годится для использования в протоколе, описанном на рисунке 1. Заметим, что доказательство равенства (4) «не проходит» из-за невозможности доказать равенство аналогичное (7).

В ряде работ последнего десятилетия, в частности в работе Shor [8], было показано, что некоторые трудные задачи (такие, например, как задача факторизации и дискретного логарифмирования) могут быть решены в полиномиальное время при использовании так называемых квантовых компьютеров. Хотя практическая реализация таких компьютеров все еще остается нерешенной проблемой [3], но не учитывать такой возможности, пусть и в далеком будущем, было бы недальновидным решением. Поэтому появились целые направления разработки так называемых постквантовых криптосистем. Такие алгоритмы гарантируют невозможность полиномиального решения трудных задач, на которых основаны эти криптосистемы, даже при практической реализации квантовых компьютеров.

К постквантовым относится, например, криптосистема Мак-Элис [1, 7]. Как следует из ее описания, ключом шифрования классической криптосистемы

Мак-Элис является матрица $\hat{G} = SGP$, где S – несингулярная квадратная матрица $k \times k$; G – порождающая матрица некоторого линейного двоичного кода; P – перестановочная $n \times n$ матрица. Тогда преобразования шифрования сообщения M для пользователя A и B будут иметь вид, соответственно:

$$\begin{aligned} f_{KA}(M) &= M\hat{G}_A \oplus Z_A; \\ f_{KB}(M) &= M\hat{G}_B \oplus Z_B, \end{aligned} \quad (14)$$

где Z_A, Z_B – случайные двоичные векторы длиной n и заданного веса t ; M – двоичная последовательность длиной k ; $\oplus$ – операция побитового сложения по mod 2.

Поскольку процедура шифрования изменяет длину сообщения от k к n , то повторное шифрование с различными ключами вообще не имеет смысла. Однако даже, если пользователи предварительно согласуют свои открытые ключи так, чтобы у одного из них параметр k был бы заменен на n , а n – на $n' > n$, то левая и правая части выражения (1) примут вид:

$$\begin{aligned} f_{KA}(f_{KB}(M)) &= (M\hat{G}_B \oplus Z_B)\hat{G}_A \oplus Z_A = \\ &= M\hat{G}_B\hat{G}_A \oplus Z_B\hat{G}_A \oplus Z_A, \end{aligned} \quad (15)$$

$$\begin{aligned} f_{KB}(f_{KA}(M)) &= (M\hat{G}_A \oplus Z_A)\hat{G}_B \oplus Z_B = \\ &= M\hat{G}_A\hat{G}_B \oplus Z_A\hat{G}_B \oplus Z_B. \end{aligned} \quad (16)$$

Видно, что (15) и (16) не будут совпадать, хотя бы из-за несовпадения векторов Z_A и Z_B . Поэтому использование криптосистемы Мак-Элис в представленном виде оказывается невозможным.

Еще одним примером постквантовых криптосистем является криптосистема на решетках [9]. Можно также проверить, что и для таких криптосистем условие (1) не выполняется. Очевидно, что такое условие не выполняется и для симметричных блочных криптосистем, таких, например, как 3DES, GOST или AES.

На первый взгляд кажется, что условие (1) может быть тривиально выполнено при использовании потоковых шифров [1, 7]. Действительно, пусть используется потоковый шифр с гаммированием, когда формирование криптограммы $E(M, K)$ задается следующим соотношением:

$$E(M, K) = M \oplus \gamma(K), \quad (17)$$

где M – произвольная двоичная последовательность; $\gamma(K)$ – двоичная последовательность (гамма), которая формируется как функция секретного ключа K при помощи его линейных и нелинейных преобразований; $\oplus$ – поэлементное сложение по mod 2.

Тогда для двух пользователей A и B , использующих ключи K_A и K_B , соответственно, выполнение условия (1) оказывается очевидным:

$$f_{KA}(f_{KB}(M)) = M \oplus \gamma(K_B) \oplus \gamma(K_A), \quad (18)$$

$$f_{KB}(f_{KA}(M)) = M \oplus \gamma(K_A) \oplus \gamma(K_B).$$

Однако использование в данном случае приведенного выше уравнения дает следующий протокол, показанный на рисунке 2.

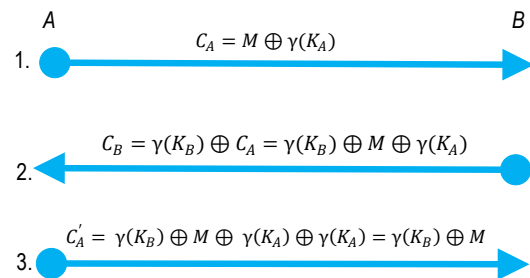


Рис. 2. Протокол секретной передачи сообщений для потокового шифра

Fig. 2. Secret Message Transfer Protocol for a Stream Cipher

Из рисунка 2 видно, что перехватчик, получая последовательности на третьем и втором этапах $\gamma(K_B) \oplus M$ и $\gamma(K_B) \oplus M \oplus \gamma(K_A)$, может поэлементно сложить их по mod 2, что дает $\gamma(K_A)$, а далее – найти сообщения M после сложения по mod 2 последовательности $\gamma(K_A)$ и последовательности, найденной им на первом этапе. Таким образом, использование потокового шифра для секретной передачи сообщений M при помощи приведенного ранее протокола также оказывается невозможным, что очевидно является следствием линейного сложения сообщения с гаммами. Заметим, что факт невозможности использования потоковых шифров в протоколе, показанном на рисунке 2, был установлен ранее в [6].

Наличие каналов обратной связи между пользователями позволяет выполнить секретное распределение между ними ключевых данных при дополнительных ограничениях на эти каналы. Так, в работе [10] предполагается, что, хотя данные каналы могут иметь или не иметь шума и быть доступными для перехвата, но они должны быть анонимными по отношению к обоим пользователям, то есть не позволять перехватчикам определить, кому принадлежат биты, наблюдаемые в каналах обмена от A к B , или наоборот. Такой сценарий рассмотрен в работе [10], где каждый из пользователей A и B генерирует случайные цепочки $K_A[1], \dots, K_A[2n]$, $K_B[1], \dots, K_B[2n]$, которые открыто публикуются с сопровождением номера битов $i = 1, 2, \dots, 2n$, но без описания принадлежности их к авторам A или B . По предварительному согласованию, пользователи A и B изымают из обращения совпадающие биты для каждого индекса $i = 1, 2, \dots, 2n$, тогда как A выбирает в качестве совместного ключа K_{AB} свои оставшиеся, упорядоченные по возрастанию i биты, причем B выбирает в качестве общего ключа K'_{AB} его оставшиеся, но инвертированные биты, что обеспечивает равенство ключей $K_{AB} = K'_{AB}$. Основная проблема заключается именно в возможности обеспечения анонимности источника (A или B) для каждого бита. В той же работе [10] проводится несколько примеров создания

таких анонимных каналов. Одним из них оказывается использование «третьего лица», которое ретранслирует в широкоэвещательную сеть биты ключей A и B , без указания пользователя, от которого был получен каждый бит.

3. Обмен ключами по постоянному, открытому и бесшумному каналу связи (типа Интернет)

В фундаментальном обзоре [5] приводятся различные сценарии распределения ключей в рамках использования общего подхода к обеспечению информационной безопасности, названного авторами Physical Layer Security. Данный подход не отказывается полностью от использования криптографических методов, например, криптосистем с открытым ключом, хэш-функций, Вайнеровской концепции подслушивающего канала, открытого обсуждения [11] и т. п., но использует данные методы только в условиях естественной или даже искусственной рандомизации каналов связи.

Однако недостатком практических всех методов, представленных в настоящем обзоре, является не реализуемые на практике требования к каналам связи. Примерами таких нереальных ограничений могут служить ограничения на мощность шума в каналах перехвата или количества антенн у перехватчика при использовании технологии MIMO и т. п.

В последнее время появилось несколько публикаций [12, 13], в которых такие недоказуемые на практике требования отсутствуют. Эти методы предполагают достаточно сложную обработку сигналов. Цель же настоящей статьи состоит в том, что она показывает возможность решения задачи распределения ключей между двумя пользователями, опирающейся на «ключевую идею», что каждый пользователь обладает хотя бы частью секретов, недоступных перехватчику, но в то же время не использует какие-либо криптографические предположения.

Опишем далее протокол, предложенный недавно в работе [14], поскольку он пока не был опубликован в русскоязычных статьях. В отличие от протокола, описанного в [15], он реализуется при помощи двухшаговой процедуры обмена информацией по каналу связи, в то время как в [15] выполняется четырехшаговая процедура, требующая больших временных затрат. На рисунке 3 представлен такой протокол, где G и P – это $n \times n$ матрицы, генерируемые легальными пользователями A и B , также, как и матрицы N_A , N_B искусственного шума. Элементы этих матриц представляют собой независимые гауссовские величины с нулевыми средними и заданными дисперсиями. Из рисунка 3 видно, что после взаимной передачи матриц по каналам связи, A и B вычисляют матрицы $\tilde{K}_A$, $\tilde{K}_B$, соответственно, и затем находят «сырые ключи» $\tilde{\tilde{K}}_A$, $\tilde{\tilde{K}}_B$, квантуя собственные числа соответствующих матриц, как $EV(\tilde{K}_A)$, $EV(\tilde{K}_B)$. В то же время, перехватчик

E оптимально находит после квантования зашумленные биты ключа между A и B , как и показано на рисунке 3: $EV(\tilde{K}_E)$, где $\tilde{K}_E = (G + N_A)(P + N_B)$.

Моделирование протокола, представленного на рисунке 3, показывает, что расхождение бит ключей $\tilde{\tilde{K}}_A$, $\tilde{\tilde{K}}_B$ между легитимными пользователями оказывается даже больше, чем расхождение бит ключа между легитимными пользователями и перехватчиком E . Для того, чтобы исправить такую ситуацию, был использован специальный протокол (PIMC, называемый протоколом преимущественного улучшения основного канала). Суть протокола PIMC состоит в том, что пользователь B повторяет каждый бит ключа S -раз и посылает эти биты по каналу связи к A , в то время как A принимает S -блоки тогда и только тогда, когда все они состоят из одинаковых бит (нулей или единиц). В противном случае A посылает B сигнал стирания этого блока.

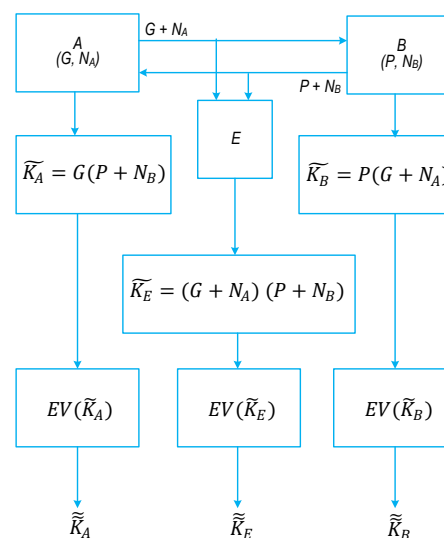


Рис. 3. Двухшаговый протокол, выполняемый по открытому и бесшумному каналу связи (типа Интернет)

Fig. 3. Two-Step Protocol Performed through an Open and Silent Communication Channel (Such as the Internet)

Для получения хорошей статистики бит ключа используется схема, показанная на рисунке 4, из которого видно, что B генерирует шумовые биты γ , как биты ключа между A и B , используя физический генератор шума. Биты γ складываются с битами ключа $\tilde{\tilde{K}}_B$, выделенными по правилу, показанному на рисунке 3.

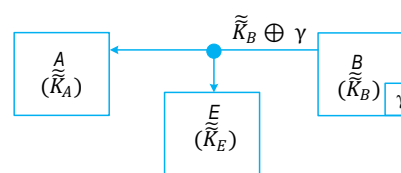


Рис. 4. Схема генерирования и пересылки бит ключа от пользователя B к пользователю A

Fig. 4. Scheme for Generating and Sending Key Bits from User B to User A

Далее A формирует свой ключ K_A по правилу:

$$\begin{aligned} K_A &= \widetilde{K}_B \oplus \gamma \oplus \widetilde{K}_A = \\ &= \widetilde{K}_A \oplus \varepsilon_{AB} \oplus \widetilde{K}_A \oplus \gamma = \gamma \oplus \varepsilon_{AB}, \end{aligned} \quad (20)$$

где ε_{AB} – битовый шум между $\widetilde{K}_A, \widetilde{K}_B$.

В то же время перехватчик E , зная схему, показанную на рисунке 4, формирует свои ключи по правилу:

$$\begin{aligned} K_E &= \widetilde{K}_E \oplus \gamma \oplus \widetilde{K}_B = \\ &= \widetilde{K}_B \oplus \varepsilon_{BE} \oplus \gamma \oplus \widetilde{K}_B = \gamma \oplus \varepsilon_{BE}. \end{aligned} \quad (21)$$

В работе [14] показано, что после применения протокола РИМС вероятность ошибок $\tilde{P}_l$ между ключами A и B , будет определяться соотношением:

$$\tilde{P}_l = \frac{P_l^S}{P_l^S + (1 - P_l)^S}, \quad (22)$$

где P_l – вероятность ошибок (вероятность появления единицы) в образце шума ε_{AB} .

Перехватчик E принимает K_E по (21) и контролирует сообщения от A к B о стирании бит. Тогда, как показано в [14], вероятность ошибок у E относительно бит ключа γ будет определяться соотношением:

$$\tilde{P}_e = \sum_{i=\frac{S+1}{2}}^S \binom{S}{i} P_e^i (1 - P_e)^{S-i}, \quad (23)$$

где P_e – вероятность ошибок в векторе ε_{BE} .

Поскольку в действительности ключевые потоки K_A и K_E имеют зависимые ошибки, то для уточнения дальнейших расчетов необходимо было провести их моделирование. В работе [14] было произведено моделирование протокола, показанного на рисунке 3, и РИМС для различных параметров S и величин дисперсии σ^2 искусственного шума, с целью вычисления вероятности ошибок $\tilde{P}_l$ и $\tilde{P}_e$. Наиболее предпочтительным оказался выбор размеров матриц 64×64 . В таблице 1 приведены результаты такого моделирования.

Из таблицы 1 видно, что при некотором выборе параметров S и σ^2 вероятности ошибок в битах ключей для основного канала ($\tilde{P}_l$) и канала перехвата ($\tilde{P}_e$) значительно расходятся между собой после использования РИМС протокола. Однако такое расхождение оказывается недостаточным, как для обеспечения надежного совпадения ключей в основном канале, так и для пренебрежимой утечки в канале перехвата. Поэтому целесообразно повысить надежность совпадения ключей K_A и K_B при помощи использования корректирующего кода, передавая проверочные биты такого кода по открытому каналу связи.

В качестве такого кода целесообразным оказалось выбрать линейный код с малой плотностью

проверок (LDPC-код), поскольку он, с одной стороны, приближается к «пределу Шеннона», а с другой стороны, обеспечивает реализуемый по сложности метод исправления ошибок [16, 17].

ТАБЛИЦА 1. Результаты моделирования вероятности ошибок $\tilde{P}_l$ и $\tilde{P}_e$ для различных параметров S и σ^2

TABLE 1. Simulation Results for Error Probabilities $\tilde{P}_l$ and $\tilde{P}_e$ with Various Parameters S and σ^2

$S \backslash \sigma^2$	0,1	0,2	0,3	0,4	$\tilde{P}_l, \tilde{P}_e$
1	0,0816	0,0851	0,0859	0,0963	$\tilde{P}_l$
	0,0922	0,117	0,140	0,154	$\tilde{P}_e$
3	0,00362	0,00402	0,00407	0,00396	$\tilde{P}_l$
	0,0185	0,0439	0,0673	0,0822	$\tilde{P}_e$
5	0,000193	0,000294	0,000258	0,000226	$\tilde{P}_l$
	0,00875	0,0314	0,053	0,0699	$\tilde{P}_e$
7	$1,44 \cdot 10^{-5}$	$3 \cdot 10^{-5}$	$1,79 \cdot 10^{-5}$	$1,68 \cdot 10^{-5}$	$\tilde{P}_l$
	0,00529	0,0256	0,0455	0,059	$\tilde{P}_e$

Что же касается требования уменьшения утечки информации по каналу перехвата, то для этого целесообразно использовать процедуру, называемую *усилением секретности*. Она подробно описана в работе [18] и заключается в применении хэширования при помощи хэш-функций, выбранных из универсального класса и последующего «выкалывания» некоторых элементов. В работе [18] была выведена граница для количества Шенноновской информации, утекающей к перехватчику после такой процедуры (с учетом передачи проверочных бит по каналу связи). Эта граница имеет следующий вид:

$$I \leq \frac{2^{-(k-t_c-l_0-r)}}{\alpha \ln 2}, \quad (24)$$

где k – длина цепочки бит ключа, разделенного между пользователями A и B после выполнения протокола РИМС; l_0 – фактическая длина ключа после выполнения процедуры усиления секретности; t_c – информация Реньи (или *коллизийная* информация), полученная по каналу перехватчика с вероятностью ошибки $\tilde{P}_e$; r – количество проверочных бит LDPC кода, передаваемых между легальными пользователями по открытому каналу связи; α – коэффициент, приближающиеся к 0,42 при больших $k, k-r$.

В работе [14] были выбраны следующие первичные параметры протокола, обеспечивающие его требуемые свойства $n = 64, \sigma^2 = 0,4, S = 5$, что позволило получить следующие вероятности ошибок для основного канала и для канала перехвата $\tilde{P}_l = 0,0002, \tilde{P}_e = 0,0699$. (см. таблицу 1). В этой же работе, путем расчетов и моделирования был выбран LDPC код с параметрами: $k = 24039, r = 961$, который обеспечивает основную длину ключа $l_0 = 3659$ бит, а также вероятность блоковой ошибки после декодирования $P_{ed} = 2,5 \cdot 10^{-3}$ и утечку информации к перехватчику $I = 9 \cdot 10^{-4}$ бита.

При выборе других параметров LDPC кода $k = 50001$, $r = 1999$ можно получить финальную длину ключа $l_o = 7624$, $P_{ed} = 8 \cdot 10^{-4}$ и $l = 1,4 \cdot 10^{-3}$ бита.

В работе [14] была выведена формула для объема трафика (Tr), требуемого для данного протокола выработки совместного ключа и представленного на рисунке 1 с учетом дополнительного выполнения протокола PIMC:

$$Tr = 2,66 \cdot 10^{-6} \frac{Sk n}{((1 - P_l)^S + P_l^S)^2} \quad (25)$$

Расчет объема трафика по этой формуле при выборе LDPC кода с параметрами $k = 24039$, $r = 961$ дает величину 32 МБ, что является приемлемым для практики.

Как уже отмечалось ранее, для выработки чисто случайной двоичной последовательности γ , показанной на рисунке 4, рекомендуется использовать аппаратно реализованный генератор. В качестве такого генератора предложено использовать генератор Crypton USB-DRN, производимый фирмой «Анкад» [19]. На рисунке 5 показан внешний вид этого генератора, выполненного в размерах flash-памяти.



Рис. 5. Вид генератора Crypton USB-DRN фирмы «Анкад»

Fig. 5. View of the Crypton USB-DRN Generator by "Ankad"

В работе [14] было произведено дополнительное тестирование статистических свойств этого генератора при помощи NIST тестов, которые показали его близость к чисто случайной (и непредсказуемой) двоичной последовательности.

Представленный выше протокол распределения ключевых данных между пользователями требует, как и любой другой протокол распределения ключей, обеспечения аутентификации легитимных

пользователей. В противном случае активный перехватчик E может, используя такой же протокол, навязать легитимным пользователям общие с ними ключи. Для воспрепятствования таким возможным действиям перехватчика, можно использовать различные методы аутентификации, начиная с простых, когда подлинность пользователя, выполняющего протокол, подтверждается его известным голосовым сообщением, переданным по дополнительному телефонному каналу [6] или такими более надежными методами, как протокол Нидхама – Шредера [20] или при помощи процедуры «спаривания» устройств, когда возможно их предварительное физическое взаимодействие [21].

4. Заключение

В настоящей работе были исследованы некоторые методы обеспечения информационной безопасности при помощи такого, появившегося сравнительно недавно, направления, как бесключевая криптография. Доказано, что один из таких методов обеспечивает возможность передачи зашифрованных криптосистем США информации без предварительного распределения как закрытых, так и открытых ключей. С другой стороны, показано, что при использовании таких криптосистем с открытым ключом как Рабина, Мак-Элиса, а также потокового шифра, получить такой же результат оказывается невозможным. Подробно описан и исследован протокол распределения ключей для его выполнения в общедоступных и бесшумных каналах с постоянными параметрами (типа Интернет). В отличие от похожего протокола, описанного в [15], он требует меньшего объема трафика, выполняемого по каналам связи. Для обеспечения хорошей статистики ключевых данных было предложено использовать аппаратный датчик случайных чисел и схему выработки сырого ключа, показанную на рисунке 4.

В дальнейшем перспективным может оказаться переход от передачи матриц по каналам связи к обмену обычными случайными числами, что обеспечит значительное уменьшение объема трафика для такого обмена. Однако такая модернизация требует проведения дальнейших углубленных исследований.

БЛАГОДАРНОСТЬ

Автор выражает благодарность профессору Коржику В.И. за помощь при подготовке и обсуждении работы.

Список используемых источников

1. Коржик В.И., Яковлев В.А. Основы криптографии. СПб: Интермедия, 2016. 312 с.
2. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22. Iss. 6. PP. 644–654. DOI:10.1109/TIT.1976.1055638
3. Dyakonov M.I. Is Fault-Tolerant Quantum Computation Really Possible? // In Luryi S., Xu J., Zaslavsky A. Future Trends in Microelectronics. John Wiley & Sons, 2007. PP. 4–18.
4. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // Journal of Cryptology. 1992. Vol. 5. PP. 3–28.
5. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey // IEEE Communications Surveys & Tutorials. 2014. Vol. 16. Iss. 3. PP. 1550–1573. DOI:10.1109/SURV.2014.012314.00178

6. Schneier B. Applied Cryptography. Montreal: JW Publ. Inc., 1994.
7. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997. DOI:10.1201/9780429466335
8. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Santa Fe, USA, 20–22 November 1994). IEEE Computer Society Press, 1994. PP. 124–134.
9. Goldreich O., Goldwasser S., Halevi S. Public-key cryptography from lattice reduction problems // Proceedings of the 17th Annual International Cryptology Conference (Santa Barbara, USA, 17–21 August 1997). Lecture Notes in Computer Science. Vol. 1291. Berlin, Heidelberg: Springer, 1997. PP. 112–131. DOI:10.1007/BFb0052231
10. Alpern B., Schneider F.B. Key exchange using 'keyless cryptography' // Information Processing Letters. 1983. Vol. 16. Iss. 2. PP. 79–81. DOI:10.1016/0020-0190(83)90029-7
11. Maurer U.M. Secrete key agreement by public discussion from common information // IEEE Transactions on Information Theory. 1993. Vol. 39. Iss. 3. PP. 733–742. DOI:10.1109/18.256484
12. Yakovlev V., Korzhik V., Morales-Luna G. Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization // IEEE Transactions on Information Theory. 2008. Vol. 54. Iss. 6. PP. 2535–2549. DOI:10.1109/TIT.2008.921689
13. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Protocol of key distribution over public noiseless channels executing without cryptographic assumptions // International Journal of Computer Science and Application. 2020. Vol. 17. Iss. 1. PP. 1–14.
14. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Optimization of the Key Sharing Protocol for Noiseless Public Channels without the Use of Cryptographic Assumptions // Proceedings of the 44th International Convention on Information, Communication and Electronic Technology (MIPRO, Opatija, Croatia, 27 September–1 October 2021). IEEE, 2021. PP. 1202–1207. DOI:10.23919/MIPRO52101.2021.9596703
15. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G. Information theoretically secure key sharing protocol executing with constant noiseless public channels // Matematicheskie Voprosy Kriptografii. 2021. Vol. 12. Iss. 3. PP. 125–141. DOI:10.4213/mvk378
16. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low Density Parity Check Codes // Electronics Letters. 1997. Vol. 33. Iss. 18. PP. 457–458.
17. Fossorier M. P.C., Mihaljevic M., Imai H. Reduced complexity iterative decoding of low density parity check codes based on belief propagation // IEEE Transactions on Communications 1999. Vol. 47. Iss. 5. PP. 673–680. DOI:10.1109/26.768759
18. Korjik V., Morales-Luna G., Balakirsky V.B. Privacy Amplification Theorem for Noisy Main Channel // Proceedings of the 4th International Conference on Information Security (ISC 2001, Malaga, Spain, 1–3 October 2001). Lecture Notes in Computer Science. Vol. 2200. Berlin, Heidelberg: Springer, 2001. PP. 18–26. DOI:10.1007/3-540-45439-X_2
19. Подорожный И.В. Обзор аппаратных генераторов случайных чисел // Молодой ученый. 2015. № 1(105). URL: <http://moluch.ru/archive/105/24688> (дата обращения 24.06.2020)
20. Needham R.M., Schroeder M.D. Using encryption for authentication in large network of computers // Communications of the ACM. 1978. Vol. 21. Iss. 12. PP. 993–999. DOI:10.1145/359657.359659
21. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. Vol. 11. Iss. 6. PP. 1306–1320. DOI:10.1109/TIFS.2015.2505626

* * *

Secure Information Transfer Using Two Keyless Cryptography Methods

A. Gerasimovich¹ 

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-119-127

Received 6th December 2021

Revised 21st December 2021

Accepted 22th December 2021

For citation: Gerasimovich A. Secure Information Transfer Using Two Keyless Cryptography Methods. *Proc. of Telecom. Universities*. 2021;7(4):119–127. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-119-127

Abstract: In the current paper, some methods of information security protocols based on physical layer security are considered. It is proved that well known Shamir's protocol can be applied to RSA cryptosystem but not to Rabin, MacEllice and trellis based cryptosystems.

The main stream of this paper is a description of key sharing protocol on constant public and noiseless channels (like Internet). It is shown that it is able to provide a high reliability and control of security in terms of Shannon's information providing nothing-additional requirements to communication channels and without any cryptographic assumptions.

Keywords: public key cryptosystem, key distribution, Shannon's information, privacy amplification, physical layer security quantum computers.

References

1. Korzhik V.I., Yakovlev V.A. *Fundamentals of Cryptography*. St. Petersburg: Intermediia Publ.; 2016. 312 p. (in Russ.)
2. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976;22(6):644–654. DOI:10.1109/TIT.1976.1055638
3. Dyakonov M.I. Is Fault-Tolerant Quantum Computation Really Possible? In Luryi S., Xu J., Zaslavsky A. *Future Trends in Microelectronics*. John Wiley & Sons; 2007. p.4–18.
4. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography. *Journal of Cryptology*. 1992;5:3–28
5. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials*. 2014;16(3):1550–1573. DOI:10.1109/SURV.2014.012314.00178
6. Schneier B. *Applied Cryptography*. Montreal: JW Publ. Inc.; 1994
7. Menezes A.J., van Oorschot P.C., Vanstone S.A. *Handbook of Applied Cryptography*. Boca Raton: CRC Press; 1997. DOI:10.1201/9780429466335
8. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 20–22 November 1994, Santa Fe, USA*. IEEE Computer Society Press; 1994. p.124–134.
9. Goldreich O., Goldwasser S., Halevi S. Public-key cryptography from lattice reduction problems. *Proceedings of the 17th Annual International Cryptology Conference, 17–21 August 1997, Santa Barbara, USA. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 1997. vol.1291. p.112–131. DOI:10.1007/BFb0052231
10. Alpern B., Schneider F.B. Key exchange using 'keyless cryptography'. *Information Processing Letters*. 1983;16(2):79–81. DOI:10.1016/0020-0190(83)90029-7
11. Maurer U.M. Secrete key agreement by public discussion from common information. *IEEE Transactions on Information Theory*. 1993;39(3):733–742. DOI:10.1109/18.256484
12. Yakovlev V., Korzhik V., Morales-Luna G. Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization. *IEEE Transactions on Information Theory*. 2008;54(6):2535–2549. DOI:10.1109/TIT.2008.921689
13. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Protocol of key distribution over public noiseless channels executing without cryptographic assumptions. *International Journal of Computer Science and Application*. 2020;17(1):1–14.
14. Korzhik V., Starostin V., Kabardov M., Gerasimovich A., Yakovlev V., Zhuvikin A. Optimization of the Key Sharing Protocol for Noiseless Public Channels without the Use of Cryptographic Assumptions. *Proceedings of the 44th International Convention on Information, Communication and Electronic Technology, MIPRO, 27 September–1 October 2021, Opatija, Croatia*. IEEE; 2021. p.1202–1207. DOI:10.23919/MIPRO52101.2021.9596703
15. Korzhik V.I., Starostin V.S., Kabardov M.M., Gerasimovich A.M., Yakovlev V.A., Zhuvikin A.G. Information theoretically secure key sharing protocol executing with constant noiseless public channels. *Matematicheskie Voprosy Kriptografii*. 2021;12(3):125–141. DOI:10.4213/mvk378
16. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low Density Parity Check Codes. *Electronics Letters*. 1997;33(18):457–458.
17. Fossorier M. P.C., Mihaljevic M., Imai H. Reduced complexity iterative decoding of low density parity check codes based on belief propagation. *IEEE Transactions on Communications*. 1999;47(5):673–680. DOI:10.1109/26.768759
18. Korjik V., Morales-Luna G., Balakirsky V.B. Privacy Amplification Theorem for Noisy Main Channel. *Proceedings of the 4th International Conference on Information Security, ISC 2001, 1–3 October 2001, Malaga, Spain. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 2001. vol.2200. p.18–26. DOI:10.1007/3-540-45439-X_2
19. Podorozhnyi I. V. Overview of Hardware Random Number Generators. *Molodoy uchenyi*. 2015;1(105). Available from: <http://moluch.ru/archive/105/24688> [Accessed 24th June 2020] (In Rus.)
20. Needham R.M., Schroeder M.D. Using encryption for authentication in large network of computers. *Communications of the ACM*. 1978;21(12):993–999. DOI:10.1145/359657.359659
21. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // *IEEE Transactions on Information Forensics and Security*. 2016. Vol. 11. Iss. 6. PP. 1306–1320. DOI:10.1109/TIFS.2015.2505626

Сведения об авторе:

**ГЕРАСИМОВИЧ
Александр Сергеевич**

аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Alexgera93@gmail.com

 <https://orcid.org/0000-0002-9174-531X>

Обнаружение аномалий в трафике устройств Интернета вещей

И.Н. Муренин¹^{*}

¹Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербург, 199178, Российская Федерация

^{*}Адрес для переписки: imurenin@gmail.com

Информация о статье

Поступила в редакцию 06.12.2021

Поступила после рецензирования 20.12.2021

Принята к публикации 21.12.2021

Ссылка для цитирования: Муренин И.Н. Обнаружение аномалий в трафике устройств Интернета вещей // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 128–137. DOI:10.31854/1813-324X-2021-7-4-128-137

Аннотация: В статье предложено искать аномалии в трафике устройств Интернета вещей на основе анализа временных рядов и оценки нормального и аномального поведения с помощью статистических методов. Основная цель заключается в комбинировании статистических методов для обнаружения аномалий с использованием неразмеченных данных и построении ключевых характеристик профилей устройств. В рамках данного подхода разработаны и реализованы методики построения признаков и границ нормального поведения, а также обнаружения аномалий на основе анализа трафика. Для их оценки использовалась генерация журналов поступающих с устройств событий с аномальной разметкой. Эксперименты показали, что наилучшие результаты по обнаружению аномалий в трафике устройств Интернета вещей дает метод выявления выбросов с помощью GESD-теста.

Ключевые слова: обнаружение аномалий, анализ временных рядов, Интернет вещей, сетевой трафик, статистические методы.

Введение

Технологии Интернета вещей обмениваются данными без необходимости взаимодействия человека с человеком или человека с компьютером. Интернет вещей все чаще используется организациями для оптимизации своих операций и является одной из самых быстрорастущих технологических областей; к концу 2030 г. Интернет вещей будет насчитывать 50 миллиардов устройств. Инновации в области Интернета вещей вносят свой вклад в улучшение реальных интеллектуальных приложений (например, инфраструктур городов, здравоохранения, транспорта и образования).

Одновременное передовое и широкомасштабное внедрение технологии Интернета вещей создало новые проблемы безопасности [1, 2]. Изучением технологий создания безопасных систем и анализа их защищенности занимаются как зарубежные, так и российские ученые [3–5]. Устройства Интернета вещей подключаются в основном через беспроводные сети, в такой среде злоумышленник может легко получить как физический, так и логический доступ к этим устройствам и вызвать критические последствия [6]. Соблюдение требований безопасности Интернета вещей явля-

ется нетривиальной задачей ввиду разнородности архитектур, большого количества уязвимостей и интеграции новых и нестандартных инфраструктурных и программных решений [7, 8].

Следующим шагом в эволюции систем Интернета вещей, таких как умные дома, системы здравоохранения, автоматизация систем и промышленный Интернет вещей, является их интеграция в социальные сети [9]. Например, интеграция умных домов в социальную сеть формирует более высокий иерархический уровень их взаимодействия, который дает новые возможности и преимущества, в частности, с точки зрения управления, хранения и обработки информации, улучшения обслуживания конечных пользователей, предотвращения и коллективного реагирования на чрезвычайные ситуации и события и т. д. Однако, интеграция умных домов в социальные сети приводит к появлению новых уязвимостей [10].

В данной работе предлагается подход к обнаружению аномалий в трафике устройств Интернета вещей. Под аномалией понимается значение, которое отклоняется от нормы в такой степени, чтобы его можно было рассматривать как редкое исключение. Подход включает формирование при-

знаков поведения устройств на основе агрегации временных рядов и оценку нормального и аномального поведения на основе статистических методов. Для оценки границ нормального поведения были использованы такие методы, как интерквантильный размах, GESD-тест, Grubs-тест и экспоненциальное сглаживание. Новизна подхода состоит в комбинировании нескольких статистических методов для обнаружения аномалий и предложенном механизме генерации журналов трафика устройств, который используется для оценки результатов обнаружения. Для проведения экспериментов с применением различных методов были сгенерированы журналы, содержащие данные, описывающие трафик устройств с всевозможными видами аномальной активности. В работе представлена оценка количества обнаруженных аномалий каждого типа с использованием предложенных статистических методов. Эксперименты показали, что наилучшие результаты по обнаружению аномалий в трафике устройств Интернета вещей дает метод обнаружения аномалий с помощью GESD-теста.

Работа организована следующим образом. Раздел «Анализ существующих решений» содержит обзор релевантных работ по обнаружению аномалий в трафике устройств инфраструктуры Интернета вещей. Раздел «Обнаружение аномалий в трафике» описывает предложенный подход к обнаружению аномалий и особенности используемых методов оценки. В разделе «Генерация журналов активности устройств и оценка предложенного подхода» представлено описание подхода к генерации журналов для проведения экспериментов и полученные результаты обнаружения аномалий.

Анализ существующих решений

Авторы [11] создали испытательный стенд «умный дом» для сбора потребительского трафика Интернета вещей. На основе этих экспериментов был разработан новый инструмент для моделирования и имитации трафика Интернета вещей. Его можно использовать в качестве основы для композиции сценариев для моделирования сред Интернета вещей, например, умных домов. Также были извлечены данные, содержащие аномальную активность из общедоступного набора данных, выполнено сравнение синтетического и реального трафика, а также сгенерирован новый трафик на основе генерации пакетов для каждого устройства с разными временными периодами и вычисления энтропии параметров трафика для оценки зависимых от устройства атрибутов.

Атрибуты и свойства трафика существенно различались для разных сценариев и каждого типа устройства Интернета вещей, также можно было наблюдать влияние аномального трафика. Кроме

того, авторы представили новый метод идентификации устройств Интернета вещей, основанный на вычислении значений энтропии характеристик трафика. Были использованы алгоритмы машинного обучения, такие как «случайный лес» (*от англ. Random Forest*), для классификации устройств на основе значения энтропии трафика Интернета вещей в различных сценариях. Результаты показали, что предложенный метод позволяет классифицировать устройства с точностью до 94 %.

Основной вклад статьи [12] – это введение функции обнаружения аномалий в трафике устройства с учетом местоположения, которая использует хэш-функцию Nilsimsa. Поскольку предложенный в статье метод LSAD (*аббр. от англ. Locality Sensitive Anomaly Detection* – «локальное чувствительное обнаружение аномалий») не требует извлечения функций из данных, его легче адаптировать, чем аналоги, основанные на использовании методов машинного обучения, и обеспечить аналогичные возможности обнаружения без какой-либо настройки параметров.

LSAD использует Nilsimsa и генерирует набор хэшей из безопасных потоков трафика устройства и вычисляет пороговое значение T . Пороговое значение T определяется путем простого измерения среднего подобия хэшей, сгенерированных из неопасных потоков трафика. Метки неопасного трафика и вычисленное пороговое значение сохраняются в базе данных для обнаружения аномального трафика.

Авторы продемонстрировали эффективность LSAD для обнаружения пятнадцати различных объемных (то есть направленных на превышение пропускной способности канала) атак и провели сравнение с современной системой машинного обучения и популярными одноклассовыми моделями машинного обучения. Результаты показывают, что LSAD достигает среднего истинно-положительного показателя (*от англ. True-Positive Rate*) выше 97 %, используя только 1 мин трафика Интернета вещей.

В работе [13] представлено исследование поведенческой кластеризации устройств инфраструктуры Интернета вещей. Исследование проводилось на реальной базе данных, которая собирает пакеты LoRaWAN (*аббр. от англ. Low-power Wide-Area Network* – «энергоэффективная сеть дальнего радиуса действия»), полученные сетью, развернутой итальянским оператором. Для того, чтобы найти группы пакетов с аналогичным поведением, использовался алгоритм k -средних. Для надежности результатов кластеризации были совместно рассмотрены два внутренних индекса валидации (WCSS и Davies – Bouldin), которые также помогли в решении проблемы поиска наилучшего значения k для разбиения.

Благодаря проведенному исследованию авторы смогли зафиксировать ключевые особенности поведения системы, которые заключались в том, что на одной стороне есть кластеры, которые собирают пакеты, характеризующиеся нормальным поведением, а с другой стороны, некоторые пакеты имеют довольно плохую производительность в системе (в основном из-за условий радиосвязи). Более того, авторы смогли наблюдать, что некоторые устройства генерируют пакеты, которые всегда назначаются одному и тому же кластеру. Эти устройства находятся в стабильном состоянии. Напротив, у некоторых устройств есть пакеты в нескольких кластерах, что означает, что не все их пакеты ведут себя одинаково. Предложенный подход продемонстрировал свою пригодность также для целей обнаружения аномалий.

Следующая работа [14] представляет новую систему обнаружения аномалий для прикладных систем домашней автоматизации HAWatcher (*аббр. от англ.* Home Automation Watcher – «мониторинг домашней автоматизации»). Предлагается метод интеллектуального анализа данных, который использует разнообразную семантическую информацию для построения гипотетических корреляций (когда корреляция описывает, как состояние одного устройства или события коррелирует с другим), и журналы событий в качестве свидетельства для их проверки. Поскольку корреляции объяснимы в соответствии с семантикой, их можно легко интерпретировать для разрешения конфликтов с интеллектуальными приложениями, которые удобно обновлять в соответствии с изменениями. Затем корреляции используются специальным модулем теневого выполнения для моделирования нормального поведения устройств в виртуальной среде. Смоделированные состояния сравниваются с состояниями в реальном мире посредством контекстной и последовательной проверки, а несоответствия во время сравнения определяются как аномалии. Подход оценивался на четырех реальных испытательных стендах с различными случаями аномалий (всего 62), продемонстрировав низкий уровень ложных обнаружений аномалий (0,04 %).

Исследование, описанное в [15], направлено на получение выгоды от интеграции умных домов в социальную сеть с точки зрения повышения безопасности как отдельного умного дома, так и всей социальной сети. Идентификация устройств в каждом из умных домов основана на мониторинге сетевого трафика и создании профилей умных устройств, присутствующих в сети. Профили состоят из набора функций, которые описывают поведение интеллектуальных устройств в сети, включая период активности устройства и период его спящего режима. На основании этого составляется белый список разрешенных профилей работы устройства и формируется кластер; для проверки

наличия профиля в его белом списке использовался алгоритм «случайный лес». Если наблюдаемый профиль отсутствует в белом списке, делается запрос на другие кластеры, образующие социальную сеть, для сравнения профиля последовательности пакетов, полученных в кластере, со своими собственными белыми списками. Для оценки эффективности предложенной системы был проведен ряд экспериментальных исследований. Результаты экспериментов показали общую точность системы на уровне 97,21 % при среднем уровне ошибок первого рода – 5,94 %.

Авторы [16] построили классификатор с использованием машинного обучения без учителя, используя автокодировщики. Предложенная модель учится эффективно восстанавливать входные данные, которые очень похожи на нормальный сетевой трафик, но плохо восстанавливают аномальный или атакующий. Таким образом, ошибку реконструкции обученной модели машинного обучения можно использовать в качестве классификатора, чтобы отличить нормальный сетевой трафик от известного или неизвестного атакующего трафика. Авторы демонстрируют, что такой подход не менее эффективен, чем использование классификатора на основе машины опорных векторов SVM (*аббр. от англ.* Support Vector Machines), при этом он значительно лучше выявляет новые типы атак.

Как только атака обнаружена, одним из способов смягчения последствий является блокирование атакующего трафика в самом источнике с помощью программно определяемых сетей SDN (*аббр. от англ.* Software-Defined Network). Однако идентификация источников атаки может быть сложной задачей, поскольку злоумышленники могут попытаться замаскировать атаку в сетевом трафике. Для обучения классификаторов нормальному поведению сети использовался общедоступный набор данных о безвредном трафике Интернета вещей. Кроме того, чтобы преодолеть препятствие, связанное с отсутствием общедоступных наборов данных для DDoS-атак (*аббр. от англ.* Distributed Denial of Service – «распределенный отказ в обслуживании») в Интернете вещей, авторы создали большую имитационную локальную сеть, состоящую из виртуальных устройств Интернета вещей и промышленных контроллеров, а также программные инструменты и скрипты, которые позволяют запускать атаки различных типов и интенсивности с выбранного набора виртуальных устройств. Авторы обучили и протестировали предложенные модели классификации для обнаружения атак по данным трафика, а также представили подход, основанный на машинном обучении для выявления скомпрометированных источников при подмене IP-адреса.

В работе [17] показано, что можно создать высокоточную модель неконтролируемого обучения

для обнаружения ботнетов Интернета вещей с ограниченным набором функций. Основным вкладом этого исследования является подробный анализ дискриминационных возможностей функций и сравнение эффективности обнаружения одной общей модели с отдельными моделями. Сокращенный набор функций позволяет потреблять меньше вычислительных ресурсов и может привести к более интерпретируемым результатам. Показано, что одна модель, в которой используются классические методы обучения (такие как SVM или Isolation Forest) с менее, чем десятью функциями, может обеспечить приемлемую скорость обнаружения, что предпочтительно с точки зрения масштабируемости. Другой важный вывод заключается в том, что, хотя одна общая модель обучения для всех устройств Интернета вещей может достичь разумных показателей обнаружения, создание отдельной модели для каждого устройства дает более высокие показатели обнаружения.

В представленных подходах, кроме работы [14], использующей корреляционный анализ для обнаружения аномалий, применяются методы машинного обучения с учителем и без учителя и кластеризация. При этом не используется возможность обнаружения выбросов в данных и построения значений для нормального поведения трафика на основе статистических методов. К преимуществам последних относится простота в использовании, скорость вычислений и возможность работы с неразмеченными данными, а также возможность получать результаты даже в тех случаях, когда неизвестна аналитическая связь между различными параметрами трафика. В данном исследовании предлагается использовать эти преимущества в рамках разрабатываемого подхода к обнаружению аномалий в трафике устройств Интернета вещей.

Обнаружение аномалий в трафике

Разработанный автором подход предполагает, что исходные данные, описывающие трафик устройств Интернета вещей внутри сети, содержатся в журналах, разделенных по дням активности. Обычно каждая строка такого журнала описывает сообщение, полученное от определенного устройства. И может включать следующую информацию: время активности, различные атрибуты текущего пользователя и текущего устройства, сетевые подключения, информацию о приложении, информацию о возможных ошибках подключения и авторизации и т. д.

Предлагаемый подход включает 3 основных этапа: извлечения признаков, оценки нормального поведения и обнаружения аномалий. На этапе извлечения признаков формируются их векторы для данного устройства или пользователя на основе агрегирования шкалы времени. На этапе оценки

поведения вычисляется нормальный диапазон для различных значений признаков для всех устройств или пользователей. Этап обнаружения аномалий отвечает за проверку активности пользователя или устройства и ищет значительные отклонения, известные как аномалии.

Для реализации каждого этапа была разработана соответствующая методика. Выходными данными методики извлечения признаков являются признаки устройств, созданные на основе агрегированного по времени количества сообщений из различных столбцов журнала, сохраненные в словаре. Входными данными методики извлечения признаков являются журналы, описывающие трафик устройств в сети.

Функциональность методики извлечения признаков позволяет загружать журналы трафика устройств, объединять несколько журналов в один, фильтровать активные устройства, создавать и сохранять признаки устройств. Методика предназначена для извлечения сущностей, описывающих ключевые характеристики поведения устройств, для оценки нормального и аномального поведения устройств. Для этого был проведен ряд экспериментов. Направление экспериментов в первую очередь связано с поиском аномальной активности устройств, поскольку их необычное поведение может указывать на мошенническую деятельность и в меньшей степени влиять на человеческий фактор. Рассматриваются только активные устройства, которые имеют как минимум несколько сообщений (5–10), порог фильтрации для общего количества сообщений определяется как входной параметр. Затем для целевых устройств создается несколько признаков (их имена также определяются как входной параметр) на основе агрегированного по времени количества сообщений из определенных столбцов исходных журналов. Эти признаки представляют ключевые характеристики поведения устройства и могут указывать на наличие аномальной активности. Размер временного окна для агрегирования определяется как входной параметр. Его значение зависит от свойств случайного процесса, т. е. характера активности устройств, и определяет размерность каждого признака. Данный интервал должен обеспечивать возможность отследить некоторые незначительные изменения в активности устройства и в то же время обобщить паттерны его активности. В ходе экспериментов использовалось значение временного окна, равное 60 с, для трафика, который включал в себя сообщения от устройств, поступающих на протяжении нескольких дней.

В зависимости от полей автор выделяет 5 типов признаков:

1) частота сообщений – строятся временные ряды для всех сообщений от уникального устройства

за определенный интервал времени с шагом H с: например, $H = 60$ с;

2) количество входов – строятся временные ряды для сообщений входа в систему с уникального устройства за определенный интервал времени с шагом H с: например, $H = 60$ с;

3) количество повторяющихся сообщений – строится временной ряд для сообщений с одинаковыми атрибутами, идущих подряд друг за другом, от уникального устройства за определенный интервал времени с шагом H с: например, $H = 60$ с;

4) интервалы между сообщениями – строится последовательность значений интервалов времени между подряд идущими сообщениями, полученными от уникального устройства;

5) количество ошибок – строятся временные ряды для сообщений с ошибками устройства от уникального устройства за определенный интервал времени с шагом H с: например, $H = 60$ с.

Пример общей активности устройства в определенный интервал времени и образец активности для текущего устройства для $H = 60$ с показаны на рисунке 1.

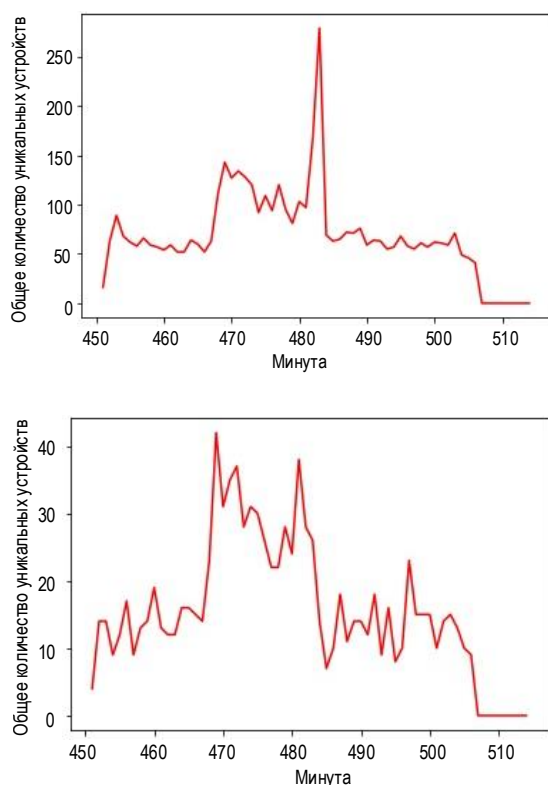


Рис. 1. Примеры паттернов активности устройств

Fig. 1. Examples of Device Activity Patterns

Следующим шагом предложенного подхода является оценка нормальной активности устройств для различных признаков с помощью методики оценки нормального поведения. Ее входными данными является словарь признаков активных устройств, а выходными – границы нормального поведения устройств для каждого признака.

Цель данного этапа – вычислить диапазон нормальных значений для каждого признака каждого устройства. Для этого используются 4 статистических метода оценки: интерквантильный размах (iqr), Grubs-тест, GESD-тест и экспоненциальное сглаживание.

Интерквантильный размах представляет собой разницу между первой ($Q1$) и третьей ($Q3$) квартилями, при его вычислении границы нормального поведения для значения признака f вычисляются согласно формуле:

$$\begin{aligned} iqr &= Q3(f) - Q1(f); \\ left &= Q1(f) - scale * iqr; \\ right &= Q3(f) + scale * iqr. \end{aligned} \quad (1)$$

где параметр $scale = 1,5$ может использоваться для поиска незначительных выбросов, не попадающих в пределы внутренних границ набора данных, а $scale = 3$ используется для поиска значительных выбросов, вышедших за внешние границы.

Критерий Граббса (Grubs-тест) – статистический тест, используемый для определения выбросов. Критерий Граббса определяет один выброс за одну итерацию. Этот выброс исключается из набора данных и тест повторяется до тех пор, пока не будут обнаружены все выбросы. Он рассчитывается на основе среднего и среднеквадратичного отклонения наблюдаемых значений:

$$G = \frac{\max |Y_i - \bar{Y}|}{s}, \quad (2)$$

где s – среднеквадратическое отклонение.

Критерий Граббса определяется для гипотез: в наборе данных нет выбросов (основной) и в наборе данных присутствует как минимум один выброс (альтернативной).

GESD (аббр. от англ. Generalized Extreme Studentized Deviate Test) – тест используется для обнаружения одного или нескольких выбросов в одномерном наборе данных. Он проверяет нулевую гипотезу «В данных нет выбросов» против конкурирующих «В данных есть i выбросов», $i = 1, \dots, n$. Тестовая статистика рассчитывается в виде:

$$\begin{aligned} \alpha_i &= \frac{(n-i)t_{p,n-t-1}}{\sqrt{(n-i+t_{p,n-t-1}^2)}}; \quad i = 1, 2, \dots, r; \\ p &= 1 - \frac{\alpha}{2(n-i+1)}, \end{aligned} \quad (3)$$

где n – размер вектора признаков; $t_{p,v}$ – 100 p -процентная точка t -распределения с v степенями свободы.

После поиска и исключения выбросов из набора данных с помощью двух описанных выше статистических тестов диапазон нормальных значений наблюдаемого признака определяется, исходя из

значений минимального и максимального элемента в полученном наборе данных.

Экспоненциальное сглаживание – это практический метод выравнивания временных рядов с использованием экспоненциальной оконной функции. В то время как в простом скользящем среднем прошлые наблюдения имеют одинаковый вес, экспоненциальные функции используются для назначения экспоненциально убывающих весов с течением времени. Последовательность необработанных данных $\{x_i\}$ начинается с момента времени $t = 0$, а результат алгоритма экспоненциального сглаживания обычно записывается как $\{s_t\}$. Процесс экспоненциального сглаживания может быть описан следующим образом:

$$s_0 = x_0; \quad s_t = \alpha x_t + (1 - \alpha)s_{t-1}, \quad t > 0, \quad (4)$$

где $0 < \alpha < 1$ – параметр сглаживания.

Для расчета границ нормального поведения на основе экспоненциального сглаживания используют нормированную разницу между исходным и восстановленным временным рядом, а также ее среднее и среднеквадратичное отклонение, на основе которых вычисляется доверительный интервал:

$$d = |x - s|; \quad d_{\text{scaled}} = \frac{d - d_{\min}}{d_{\max} - d_{\min}}; \quad (5)$$

$$\text{left} = \overline{d_{\text{scaled}}} - t_{\alpha/2} S,$$

где $t_{\alpha/2}$ – уровень построения доверительного интервала (используется значение 1,96: доверительный интервал – 95 %).

Устройства, имеющие недостаточные показатели активности (всего несколько сообщений), могут быть отфильтрованы с помощью порога, заранее заданного вручную, затем выполняется вычисление границ с указанной последовательностью методов, по умолчанию вначале используется GESD-метод, затем тест Граббса, затем интерквантильный размах, затем экспоненциальное сглаживание. На протестированных журналах GESD-метод показывает наилучшие результаты, соответственно для каждого метода были получены 113, 6, 3 и 53 устройства с ненулевыми границами нормальной активности для исходных данных. Исходя из результатов применения GESD-метода, вычисляются границы только для оставшихся устройств для каждого следующего метода. Это также сокращает время вычислений и дает возможность использовать различные методы для оценки нормального поведения одновременно, что позволяет определить границы нормального поведения для большего количества устройств.

После определения нормальных диапазонов признаков методика проверяет информацию о ранее рассчитанном диапазоне и по возможности использует их (объединяя со значениями в словаре границ нормального поведения). Если для ана-

лизируемого устройства нет информации о ранее рассчитанном диапазоне нормальных значений или имеются неопределенные или нулевые нормальные значения признаков, то эта информация сохраняется и соответствующие значения обновляются.

Заключительный этап предложенного подхода представляет собой обнаружение аномалий с помощью методики обнаружения аномалий. В качестве входных данных для обнаружения аномалий используются нормальные значения признаков и характеристики устройства. Выходными данными методики обнаружения аномалий являются: их количество для каждого признака каждого устройства, атрибуты времени начала для аномалий, некоторые статистики устройства на основе его аномальных временных атрибутов.

Процесс обнаружения аномалии состоит из следующих шагов.

Шаг 1. Обнаружение аномалии в значениях каждого признака для каждого устройства. Данный шаг реализуется путем сравнения значений каждого признака для каждого устройства с диапазонами нормальных значений.

Шаг 2. Определение атрибутов аномалий, таких как идентификатор устройства, название признака, интенсивность аномалии и время аномалии. Интенсивность аномалии определяется как отношение расстояния между значением признака и ближайшей границей диапазона к значению признака, в случае, когда значение признака равно нулю, интенсивность равна отношению целевого расстояния к расстоянию между правой и левой границами нормального диапазона. Время аномалии определяет временной интервал аномальной активности, продолжительность которого определяется параметром H , рассматривается только время начала аномалии.

Шаг 3. Фильтрация аномалий. Аномалии фильтруются по порогам интенсивности, указанным для каждого признака в заранее определенном параметре, который представляет собой последовательность весов интенсивностей для каждого признака. Это необходимо для того, чтобы была возможность исключить из рассмотрения незначительные отклонения от нормального поведения, не представляющие интереса. Данные веса задаются вручную и позволяют сократить количество ложно-положительных обнаружений в случаях, когда потенциально аномальные значения отклоняются от нормальных всего на несколько процентов.

Шаг 4. Вычисление итоговых значений. На данном шаге вычисляется количество аномалий для каждого признака каждого устройства, определяются атрибуты времени начала для аномалий и вычисляются следующие статистики устройства на основе его аномальных временных атрибутов, а

именно – количество дней общей активности, аномальной активности и последних последовательных дней нормальной активности. После этого вычисляются веса аномалий на основе отношения интервалов времени аномалии ко всем интервалам активности для всех признаков (или их целевого подмножества) с целью последующего применения для обнаружения атак и анализа рисков информационной безопасности.

Для проведения экспериментов был реализован подход в рамках программного прототипа на языке Python, каждая методика вместе со своими входными и выходными параметрами составляла отдельный модуль, в том числе и методика генерации журналов активности устройств, описанная в следующем разделе.

Генерация журналов активности устройств и оценка предложенного подхода

Для оценки предложенного подхода для обнаружения аномалий в трафике устройств использовался механизм генерации журналов на основе использования распределений исходных атрибутов устройства, таких как временные метки, входы с устройства, сетевые адреса, возникшие ошибки и т. д. В процессе генерации в журнал добавлялись аномалии для каждого из признаков для некоторых случайных устройств с заданной вероятностью, затем итоговая разметка сравнивалась с результатами обнаружения на журнале, полученном в процессе генерации.

На основе входных данных определялось частотное распределение сообщений с устройств и на его основе осуществлялась генерация идентификатора устройства и его профиля, который содержал всевозможные значения атрибутов для данного устройства. На основе этого профиля осуществлялась генерация аномальной активности путем изменения целевых атрибутов устройства с заданной вероятностью, которая затем добавлялась в генерируемый журнал. Оценка на основе корреляций с использованием коэффициента корреляции Спирмена применялась для формирования множества зависимых и независимых атрибутов устройства, зависимые атрибуты (например, версия программного обеспечения, идентификатор пользователя) генерировались на основе их распределений относительно текущего устройства, независимые (например, адреса сетевых шлюзов, IP-адреса) – на основе общего распределения атрибута по журналу, либо на основе других атрибутов. На рисунке 2 представлена общая схема подхода к генерации журнала активности устройств.

Ниже перечислены основные шаги для генерации журнала активности устройств.

Шаг 1. Выбираем устройство из общего множества устройств в соответствии с исходным распределением частот входов.

Шаг 2. Определяем и генерируем для устройства время входа на основе выбора исходных временных интервалов с небольшим фиксированным случайным отклонением.

Шаг 3. Определяем для устройства множество его атрибутов, таких как попытки логина, сетевые адреса, ошибки и т. д. Для этого необходимо проверить, какие атрибуты зависят от конкретного устройства.

Шаг 4. Генерируем для устройства необходимые атрибуты.

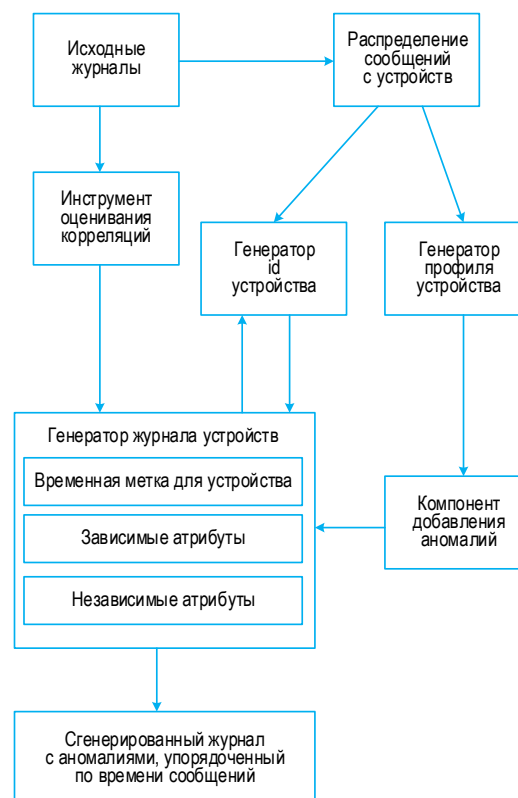


Рис. 2. Общая схема подхода к генерации журнала активности устройств

Fig. 2. General Scheme of Approach to Generating a Device Activity Log

Выполняем шаги 1–4 нужное число раз, в зависимости от требуемого количества строк в журнале; в конце – упорядочиваем все по времени.

После генерации в журнал были добавлены аномалии для каждого признака, которые включали:

- нетипичное (большее или меньшее) количество сообщений от устройства;
- нетипичное количество попыток авторизации устройства;
- нетипичное количество подряд идущих сообщений от устройства;
- нетипичные интервалы отклика устройства (промежутки между отдельными сообщениями);
- нетипичное количество ошибок, возникших при соединении с устройством.

После генерации журнала были построены признаки устройств, определены значения, соответ-

ствующие нормальному поведению и обнаружены различные аномалии. Общее количество уникальных устройств в сгенерированном логе составило 4804. Количественная оценка обнаруженных аномалий в сгенерированном журнале приведена в таблице 1. Точность обнаружения аномалий представляет собой отношение количества найденных аномалий к общему количеству аномалий для данного признака.

Таким образом, средняя точность обнаружения аномалий в сгенерированном журнале по всем видам характеристик устройств составила 79 %.

Лучше всего обнаруживаются аномалии, связанные с изменением временных интервалов между сообщениями от устройства, хуже всего – аномалии, связанные с количеством повторяющихся сообщений. Это может быть связано с незначительным изменением частоты сообщений при генерации, которое могло попасть в рамки диапазона нормальных значений. Возможно, требуется более чувствительная настройка методов определения границ нормального поведения конкретно для данной характеристики.

ТАБЛИЦА 1. Количественная оценка обнаруженных аномалий в сгенерированном журнале

TABLE 1. Quantification of Detected Anomalies in the Generated Log

Признак	Количество аномалий		Из них:			Точность
	в сгенерированном логе	обнаруженных	истинно-положительные	ложно-отрицательные	ложно-положительные	
Частота сообщений	82	73	68	9	5	83 %
Количество входов	31	45	25	1	19	80 %
Количество повторяющихся сообщений	41	29	25	12	3	61 %
Интервалы между сообщениями	81	86	72	7	7	89 %
Количество ошибок	47	40	34	9	4	72 %
Общее количество	282	273	224	38	38	79 %

Заключение

В данной работе предложен подход к обнаружению аномалий в трафике устройств Интернета вещей, основанный на построении численных характеристик профилей устройств, определении их нормальных значений и поиску отклонений от нормы на основе статистических методов, а именно интерквантильного размаха, Grubs-теста, GESD-теста и экспоненциального сглаживания. Описаны методики анализа трафика устройств Интернета вещей, входящие в разработанный подход, предложенные признаки выявления аномалий, механизм генерации журналов событий для устройств, а также численная оценка обнаруженных аномалий в сгенерированном журнале с помощью предложенного подхода. Эксперименты показали, что в сгенерированном журнале средняя точность обнаружения аномалий по всем признакам составила

79 %, лучшие результаты в 89 % были получены для признака, измеряющего частоту сообщений, полученных от устройства. В данном исследовании использовались различные статистические методы для обнаружения аномалий в трафике устройств Интернета вещей, которые имеют такие преимущества, как гибкость, универсальность, скорость вычислений и возможность работы с неразмеченными данными. К недостаткам предложенного подхода можно отнести отсутствие оценки предложенных методик, на основе размеченных данных с аномалиями.

Дальнейшие улучшения предложенного подхода связаны с анализом большего количества признаков и сравнении эффективности предложенных методов с методами, основанными на использовании машинного обучения.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа подготовлена при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Список используемых источников

1. Tariqa N., Khan F.A., Asimic M. Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis // *Procedia Computer Science*. 2021. Vol. 191. PP. 425–430. DOI:10.1016/j.procs.2021.07.053
2. Sengupta J., Ruj S., Das Bit S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT // *Journal of Network and Computer Applications*. 2019. Vol. 149. DOI:10.1016/j.jnca.2019.102481
3. Котенко И.В., Степашкин М.В., Богданов В.С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // *Проблемы информационной безопасности. Компьютерные системы*. 2006. № 2. С. 7–24.
4. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // *Защита информации. Инсайд*. 2011. № 3(39). С. 68–75.
5. Enoch S.Y., Ge M., Hong J.B., Kim D.S. Model-based Cybersecurity Analysis: Past Work and Future Directions. Cornell University, 2021. URL: <https://arxiv.org/abs/2105.08459> (дата обращения 21.12.2021)
6. Torres N., Pinto P., Lopes S.I. Security Vulnerabilities in LPWANs – An Attack Vector Analysis for the IoT Ecosystem // *Applied Sciences*. 2021. Vol. 11. Iss. 7. DOI:10.3390/app11073176
7. Alansari Z., Anuar N.B., Kamsin A., Belgaum M.R., Alshaer J., Soomro S., et al. Internet of Things: Infrastructure, Architecture, Security and Privacy // *Proceedings of the International Conference on Computing, Electronics & Communications Engineering (ICCECE, Southend, UK, 6–17 August 2018)*. IEEE, 2018. DOI:10.1109/ICCECOME.2018.8658516
8. Hamza A., Gharakheili H.H., Sivaraman V. IoT Network Security: Requirements, Threats, and Countermeasures. Cornell University, 2020. URL: <https://arxiv.org/abs/2008.09339> (дата обращения 21.12.2021)
9. Bouazza H., Zohra L.F., Said B. Integration of Internet of Things and Social Network: Social IoT General Review // *Proceedings of the First International Conference on Computing (ICC 2019, Riyadh, Saudi Arabia, 10–12 December 2019) on Advances in Data Science, Cyber Security and IT Applications*. Communications in Computer and Information Science. Vol. 1098. Cham: Springer, 2019. PP. 312–324. DOI:10.1007/978-3-030-36368-0_26
10. Ali O., Ishak M.K., Bhatti M.K.L. Emerging IoT domains, current standings and open research challenges: a review // *PeerJ Computer Science*. 2021. DOI:10.7717/peerj-cs.659
11. Nguyen-An H., Silverston T., Yamazaki T., Miyoshi T. IoT Traffic: Modeling and Measurement Experiments // *IoT*. 2021. Vol 2(1). PP. 140–162. DOI:10.3390/iot2010008
12. Charyyev B., Gunes M.H. Detecting Anomalous IoT Traffic Flow with Locality Sensitive Hashes // *Proceedings of the Global Communications Conference (GLOBECOM, Taipei, Taiwan, 7–11 December 2020)*. IEEE, 2020. DOI:10.1109/GLOBECOM42002.2020.9322559
13. Garlisi D., Martino A., Zouwayhed J., Pourrahim J., Cuomo F. Exploratory approach for network behavior clustering in LoRaWAN // *Journal of Ambient Intelligence and Humanized Computing*. 2021. DOI:10.1007/s12652-021-03121-z
14. Fu C., Zeng Q., Du X. HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes // *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2021. PP. 4223–4240. URL: <https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong> (дата обращения 21.12.2021)
15. Nicheporuk A., Nicheporuk A., Sachenko A., Sachenko O., Kazantsev A. A System for Detecting Anomalies and Identifying Smart Home Devices Using Collective Communication // *Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS (IntelITSIS, 2021, Khmelnytskyi, Ukraine, 24–26 March 2021)*. URL: <http://ceur-ws.org/Vol-2853/paper44.pdf> (дата обращения 21.12.2021)
16. Bhatia R., Benno S., Esteban J., Lakshman T.V., Grogan J. Unsupervised machine learning for network-centric anomaly detection in IoT // *Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA '19)*. New York: Association for Computing Machinery, 2019. PP. 42–28. doi:10.1145/3359992.3366641
17. Nömm S., Bahşi H. Unsupervised Anomaly Based Botnet Detection in IoT Networks // *Proceedings of the 17th International Conference on Machine Learning and Applications (ICMLA, Orlando, USA, 17–20 December 2018)*. IEEE, 2018. DOI:10.1109/ICMLA.2018.00171

* * *

Detection of IoT Device Traffic Anomalies

I. Murenin¹ 

¹Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
St. Petersburg, 199178, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-128-137

Received 6th December 2021

Revised 20th December 2021

Accepted 21th December 2021

For citation: Murenin I. Detection of Anomalies in the Traffic of IoT Devices. *Proc. of Telecom. Universities*. 2021;7(4): 128–137. (in Russ.) DOI:10.31854/ 1813-324X-2021-7-4-128-137

Abstract: The article proposes an approach to finding anomalies in the traffic of IoT devices based on time series analysis and assessing normal and abnormal behavior using statistical methods. The main goal of the proposed approach is to combine statistical methods for detecting anomalies using unlabeled data and plotting key characteristics of device profiles. Within this approach the following techniques for traffic analysis has been developed and implemented: a technique for a feature extraction, a normal behavior boundary building technique and an anomaly detection technique. To evaluate the proposed approach, we used a technique for generating event logs from devices with the generation of anomalous markup. The experiments shown that the GESD-test gives the best results for anomaly detection in IoT traffic.

Keywords: anomaly detection, time series analysis, IoT, network traffic, statistical methods.

References

1. Tariqa N., Khan F.A., Asimc M. Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis. *Procedia Computer Science*. 2021;191:425–430. DOI:10.1016/j.procs.2021.07.053
2. Sengupta J., Ruj S., Das Bit S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IloT. *Journal of Network and Computer Applications*. 2019;149. DOI:10.1016/j.jnca.2019.102481
3. Kotenko I.V., Stepashkin M.V., Bogdanov V.S. Architectures and Models of Active Vulnerabilities Analysis Based on Simulation of Malefactors' Actions. *Information Security Problems. Computer Systems*. 2006;2:7–24 (in Russ.)
4. Kotenko I.V., Desnitskiy V.A., Chechulin A.A. Research of technology for designing safe embedded systems in the project of the European Community SecFutur. *Zašita informacii. Inside*. 2011;3(39):68–75.
5. Enoch S.Y., Ge M., Hong J.B., Kim D.S. *Model-based Cybersecurity Analysis: Past Work and Future Directions*. Cornell University; 2021. Available from: <https://arxiv.org/abs/2105.08459> [Accessed 21th December 2021]
6. Torres N., Pinto P., Lopes S.I. Security Vulnerabilities in LPWANs – An Attack Vector Analysis for the IoT Ecosystem. *Applied Sciences*. 2021;11(7). DOI:10.3390/app11073176
7. Alansari Z., Anuar N.B., Kamsin A., Belgaum M.R., Alshaer J., Soomro S., et al. Internet of Things: Infrastructure, Architecture, Security and Privacy. *Proceedings of the International Conference on Computing, Electronics & Communications Engineering, iCCECE, 6–17 August 2018, Southend, UK*. IEEE; 2018. DOI:10.1109/iCCECOME.2018.8658516
8. Hamza A., Gharakheili H.H., Sivaraman V. *IoT Network Security: Requirements, Threats, and Countermeasures*. Cornell University, 2020. Available from: <https://arxiv.org/abs/2008.09339> [Accessed 21th December 2021]
9. Bouazza H., Zohra L.F., Said B. Integration of Internet of Things and Social Network: Social IoT General Review. *Proceedings of the First International Conference on Computing, ICC 2019, 10–12 December 2019, Riyadh, Saudi Arabia on Advances in Data Science, Cyber Security and IT Applications. Communications in Computer and Information Science*. Cham: Springer; 2019. vol.1098. p.312–324. DOI:10.1007/978-3-030-36368-0_26
10. Ali O., Ishak M.K., Bhatti M.K.L. Emerging IoT domains, current standings and open research challenges: a review. *PeerJ Computer Science*. 2021. DOI:10.7717/peerj-cs.659
11. Nguyen-An H., Silverston T., Yamazaki T., Miyoshi T. IoT Traffic: Modeling and Measurement Experiments. *IoT*. 2021;2(1):140–162. DOI:10.3390/iot2010008
12. Charyyev B., Gunes M.H. Detecting Anomalous IoT Traffic Flow with Locality Sensitive Hashes. *Proceedings of the Global Communications Conference, GLOBECOM, 7–11 December 2020, Taipei, Taiwan*. IEEE; 2020. DOI:10.1109/GLOBECOM.42002.2020.9322559
13. Garlisi D., Martino A., Zouwayhed J., Pourrahim J., Cuomo F. Exploratory approach for network behavior clustering in LoRaWAN. *Journal of Ambient Intelligence and Humanized Computing*. 2021. DOI:10.1007/s12652-021-03121-z
14. Fu C., Zeng Q., Du X. HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes. *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association; 2021. p.4223–4240. Available from: <https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong> [Accessed 21th December 2021]
15. Nicheporuk A., Nicheporuk A., Sachenko A., Sachenko O., Kazantsev A. A System for Detecting Anomalies and Identifying Smart Home Devices Using Collective Communication. *Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, IntellITSIS, 2021, 24–26 March 2021, Khmelnytskyi, Ukraine*. Available from: <http://ceur-ws.org/Vol-2853/paper44.pdf> [Accessed 21th December 2021]
16. Bhatia R., Benno S., Esteban J., Lakshman T.V., Grogan J. Unsupervised machine learning for network-centric anomaly detection in IoT // *Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA '19)*. New York: Association for Computing Machinery, 2019. PP. 42–28. doi:10.1145/3359992.3366641
17. Nömm S., Bahsi H. Unsupervised Anomaly Based Botnet Detection in IoT Networks // *Proceedings of the 17th International Conference on Machine Learning and Applications, ICMLA, 17–20 December 2018, Orlando, USA*. IEEE, 2018. DOI:10.1109/ICMLA.2018.00171

Сведения об авторе:

МУРЕНИН
Иван Николаевич

младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН,
imurenin@gmail.com
 <https://orcid.org/0000-0002-2263-2426>

Экспериментальное исследование влияния схем модуляции-кодирования на размер зоны обслуживания цифрового радиовещания стандарта DRM в диапазоне ОВЧ. Часть 2

С.В. Мышьянов¹✉*

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

*Адрес для переписки: mishyanov@gmail.com

Информация о статье

Поступила в редакцию 26.07.2021

Поступила после рецензирования 06.12.2021

Принята к публикации 06.12.2021

Ссылка для цитирования: Мышьянов С.В. Экспериментальное исследование влияния схем модуляции-кодирования на размер зоны обслуживания цифрового радиовещания стандарта DRM в диапазоне ОВЧ. Часть 2 // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 138–146. DOI:10.31854/1813-324X-2021-7-4-138-146

Аннотация: в статье приведены результаты измерений параметров качества сигнала цифрового радиовещания DRM в опытной зоне Санкт-Петербурга с целью определения влияния режимов передачи, заложенных в стандарт DRM на размер зоны обслуживания.

Ключевые слова: цифровое радиовещание, DRM, зона обслуживания, мобильные измерения.

Данный материал является продолжением статьи [1]. В первой части раскрыта проблематика планирования зон обслуживания передатчиков системы цифрового радиовещания Digital Radio Mondiale (DRM) [2], дана постановка задачи исследований, описание условий измерений, приведены результаты измерений для маршрутов № 1 в северном и № 2 восточном направлениях. Во второй части представлены результаты измерений для маршрутов № 3 в юго-восточном и № 4 западном

направлениях, а также обобщение экспериментальных данных.

№ 3: Юго-восточное направление (трасса Е105 СПб – Москва)

Маршрут в юго-восточном направлении проходил по трассе Е105 СПб – Москва, перечень измерений представлен в таблице 1, качество приема сигнала для разных режимов DRM - на рисунке 1.

ТАБЛИЦА 1. Перечень измерений в юго-восточном направлении

TABLE 1. List of Measurements in the Southeast Direction

№ п/п	Дата измерения	Режим передачи	Мощность передатчика, Вт	Длительность записи, мин	Расстояние до передатчика, км	
					минимальное	максимальное
1	18.11.2020	QAM16 PL3	674	1:25:34	12	70
2	11.05.2021	QAM4 PL0	99	0:50:18	25	86
3		QAM4 PL1		0:42:44	26	78
4		QAM4 PL2		0:37:42	26	78
5		QAM4 PL3		0:39:17	26	78
6		QAM16 PL0		0:40:15	26	78
7		QAM16 PL1		0:34:44	26	78
8		QAM16 PL2		0:34:23	26	78
9		QAM16 PL3		1:13:06	26	78

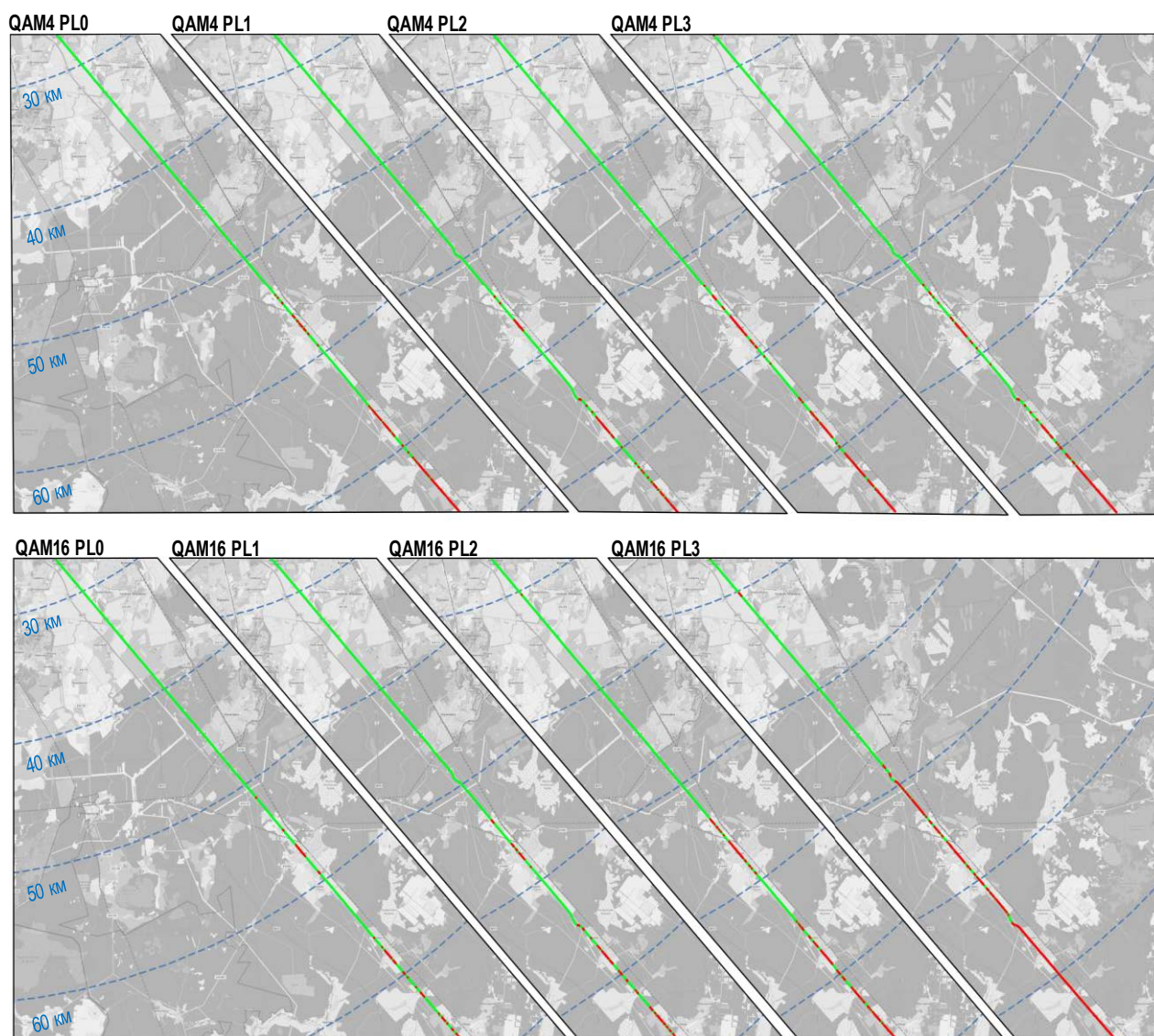


Рис. 1. Качество приема сигнала для разных режимов DRM в юго-восточном направлении

Fig. 1. Signal Reception Quality for Different DRM MODES in the Southeast Direction

На рисунке 2 представлены зависимости измеренной напряженности поля от расстояния до передатчика для соответствующих маршрутов, приведенных на рисунке 1. На рисунке 3 приведены гистограммы качества декодирования сигнала DRM измерительным приемником, сгруппированные по километровым интервалам в зависимости от расстояния до передатчика. В целях сопоставления на рисунках 1-3 проиллюстрирован отрезок с 26 по 78 км маршрута, который представляет собой практически прямую линию под небольшим углом к радиальному направлению удаления от передатчика.

Маршрут проходит по равнинной местности без резких перепадов высот и затенений естественными препятствиями. Минимальная высота над уровнем моря (15 м) наблюдается на начальном отрезке маршрута и возрастает при удалении от СПБ до максимальной в 65 м.

В г. Тосно присутствовали сильные помехи в интервалах 55–60 и 65–70 км, на графиках напряженности поля прослеживается увеличение уровня при одновременном падении отношения сигнал/шум (SNR, аббр. от англ. Signal-to-Noise Ratio). Помеха на 65–70 км представляла собой незарегистрированную УКВ-ЧМ радиостанцию, которая перебивала при прослушивании звуковой сигнал «Comedy Radio» на частоте 95,9 МГц и была стационарной, т.е. фиксировалась на всех итерациях измерений. Очевидно, что проценты некорректно декодированных кадров на гистограммах рисунка 3 в указанных интервалах связаны преимущественно с данными помехами, что затрудняет оценку градации границ зоны обслуживания в зависимости от режима. По всей видимости, граница лежит в 70–72 км для наиболее помехоустойчивого режима QAM4 PL0, а разница при переключении между режимами существенно меньше в сравнении с похожим по ха-

рактору рельефа восточным направлением. Характеристики приема от QAM4 PL0 до QAM16 PL2 очень похожи, и лишь QAM16 PL3 показывает себя существенно хуже, ограничивая зону обслуживания на 48 км еще до участка влияния стационарной помехи (ошибки на 31 км также обусловлены помехой).

Измерения в юго-восточном направлении показывают иллюстрируют проблему наличия в радиозфере большого количества помех, существенно превышающих уровень индустриального

шума, заложенного в критерии планирования зон обслуживания радиостанций. Причем, используемый режим помехоустойчивости передатчика DRM в данной ситуации мало влияет на возможность противостоять подобным помехам ввиду их большой мощности.

Измерение на повышенной мощности (674 Вт) проводилось при QAM16 PL3 с неполным совпадением маршрута относительно основной серии измерений. Соответствующие иллюстрации приведены на рисунках 4 и 5.

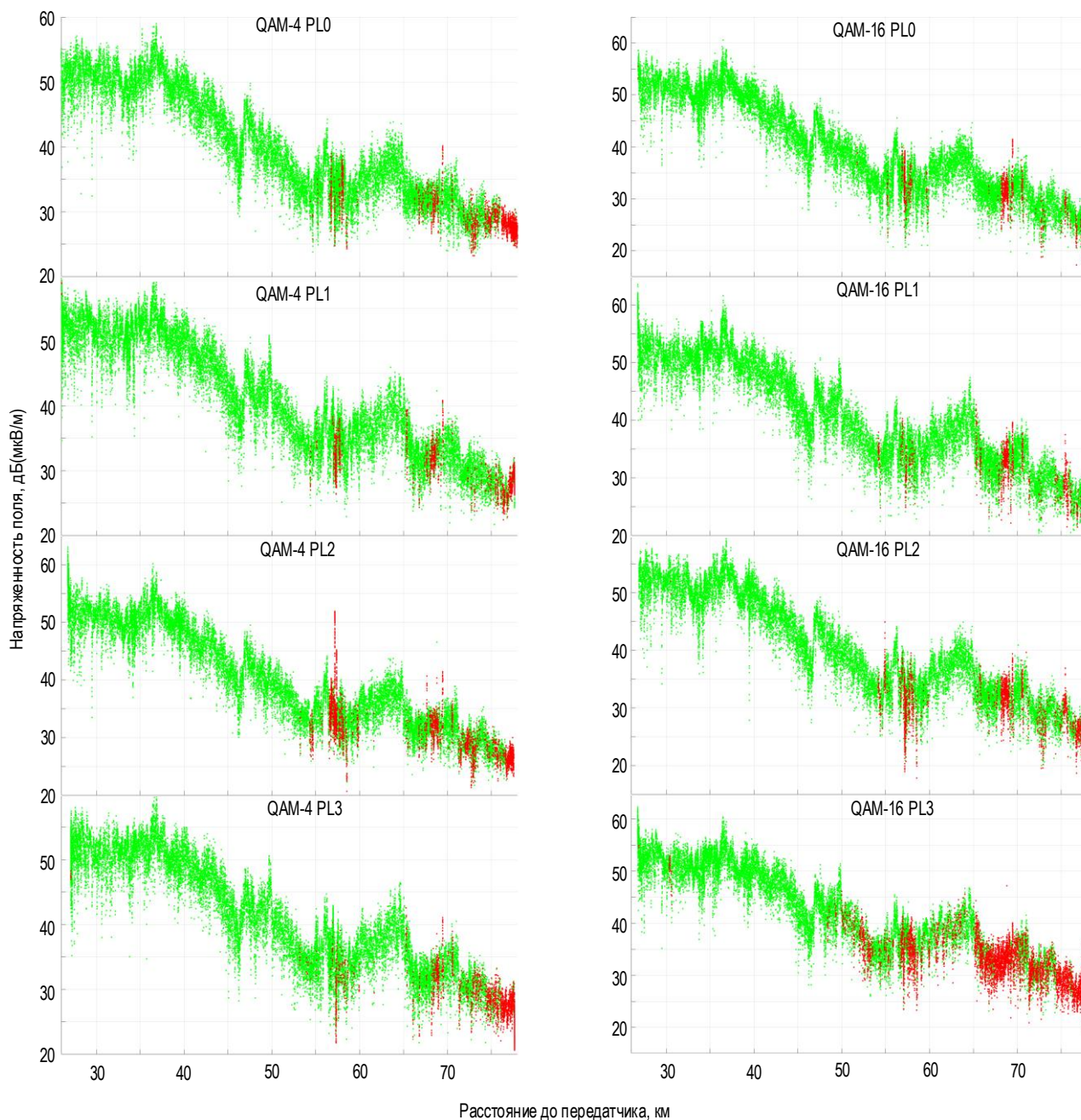


Рис. 2. Зависимости измеренной напряженности поля от расстояния до передатчика для маршрутов в юго-восточном направлении

Fig. 2. Dependences of the Measured Field Strength on the Distance to the Transmitter for Routes in the Southeast Direction

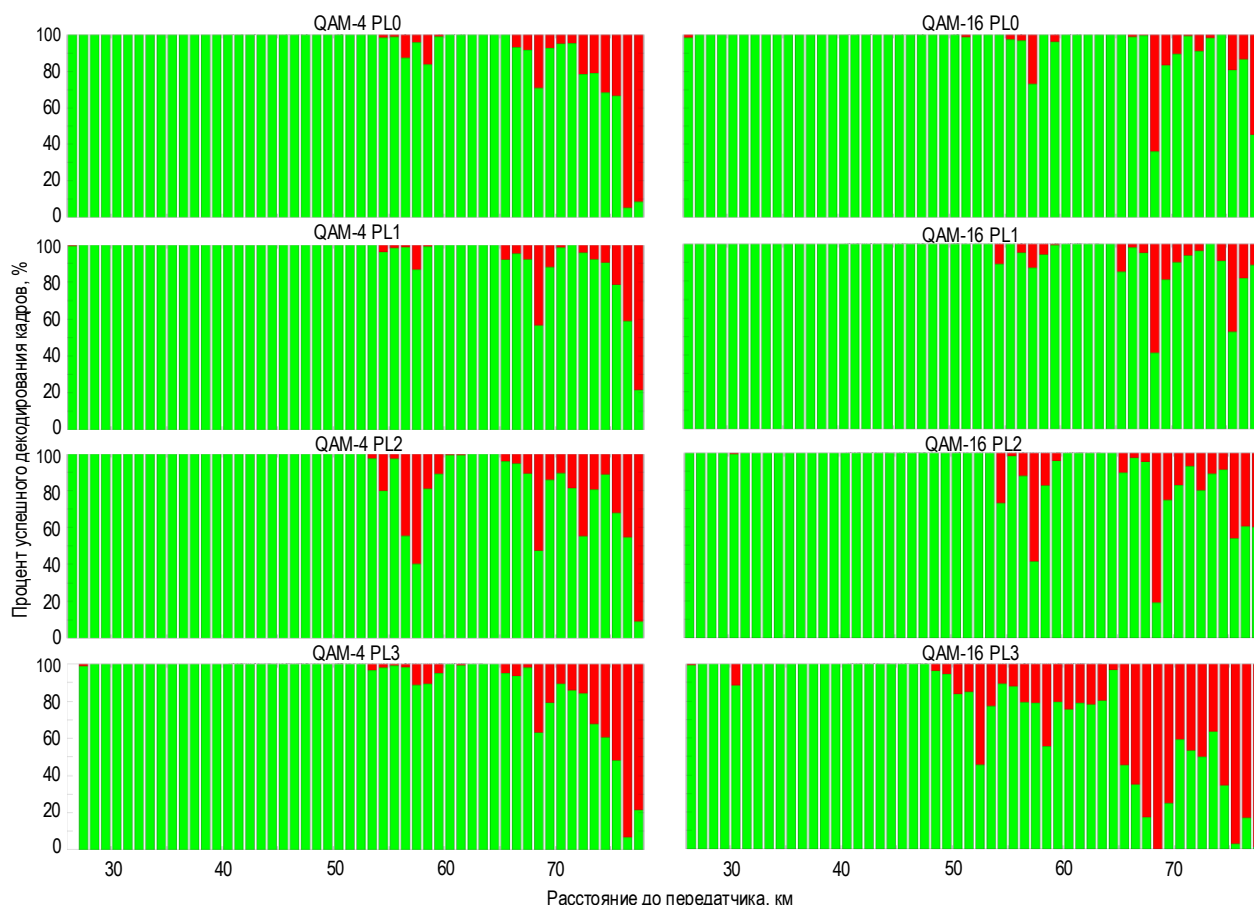


Рис. 3. Нормированные гистограммы качества декодирования сигнала в юго-восточном направлении

Fig. 3. Normalized Histograms of the Decoding Quality of the Signal in the South-Eastern Direction

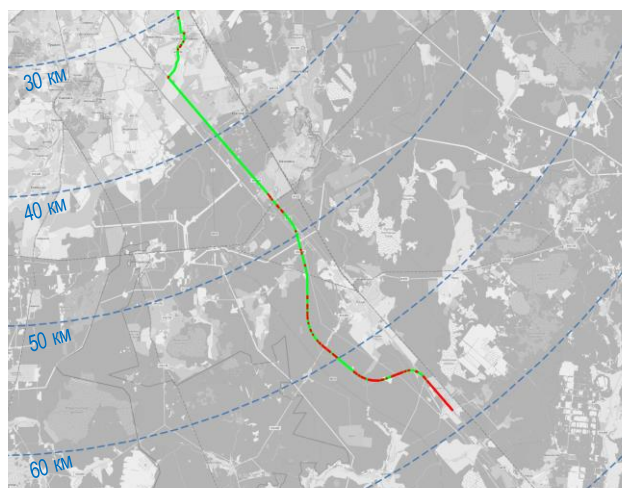


Рис. 4. Качество приема сигнала в юго-восточном направлении при QAM16 PL3 674 Вт

Fig. 4. Signal Reception Quality in the Southeast Direction at QAM16 PL3 674 Wt

Результаты показывают, что повышение мощности передатчика в данном случае, также как и в восточном направлении, позволяет существенно улучшить качество приема и сдвинуть границу зоны обслуживания ближе к геометрическому горизонту распространения радиоволн.

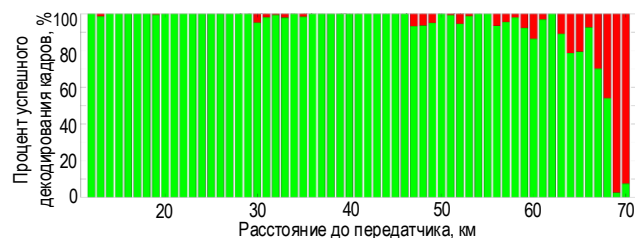


Рис. 5. Нормированная гистограмма качества декодирования сигнала в юго-восточном направлении при QAM16 PL3 674 Вт

Fig. 5. Normalized Histogram of the Decoding Quality of the Signal in the South-Eastern Direction at QAM16 PL3 674 Wt

№ 4: Западное направление (СПб – Сосновый бор)

Маршрут в западном направлении проходил из Санкт-Петербурга в Сосновый Бор, перечень измерений представлен в таблице 2. Измеренные параметры качества в западном направлении представлены на рисунках 6–8. В целях сопоставления проиллюстрирован отрезок с 42 по 68 км маршрута. Маршрут до 57 км проходит вдоль берега Финского залива, в интервале 57–59 км радиальное направление меняется на окружное к передатчику и далее до конца маршрута вновь на радиальное.

ТАБЛИЦА 2. Перечень измерений в западном направлении

TABLE 2. List of Measurements in the Western Direction

№ п/п	Дата измерения	Режим передачи	Мощность передатчика, Вт	Длительность записи, мин	Расстояние до передатчика, км	
					минимальное	максимальное
1	01.12.2020	QAM4 PL0	652	0:51:48	14	70
2	30.11.2020	QAM16 PL3	631	0:37:39	38	75
3	13.05.2021	QAM4 PL0	99	0:46:10	35	77
4		QAM4 PL1		0:24:25	42	68
5		QAM4 PL2		0:22:53	42	68
6		QAM4 PL3		0:21:51	42	68
7		QAM16 PL0		0:33:59	35	68
8		QAM16 PL1		0:31:29	35	68
9		QAM16 PL2		0:37:15	35	69
10		QAM16 PL3		0:39:19	42	77
11		QAM16 PL3		1:14:08	10	69

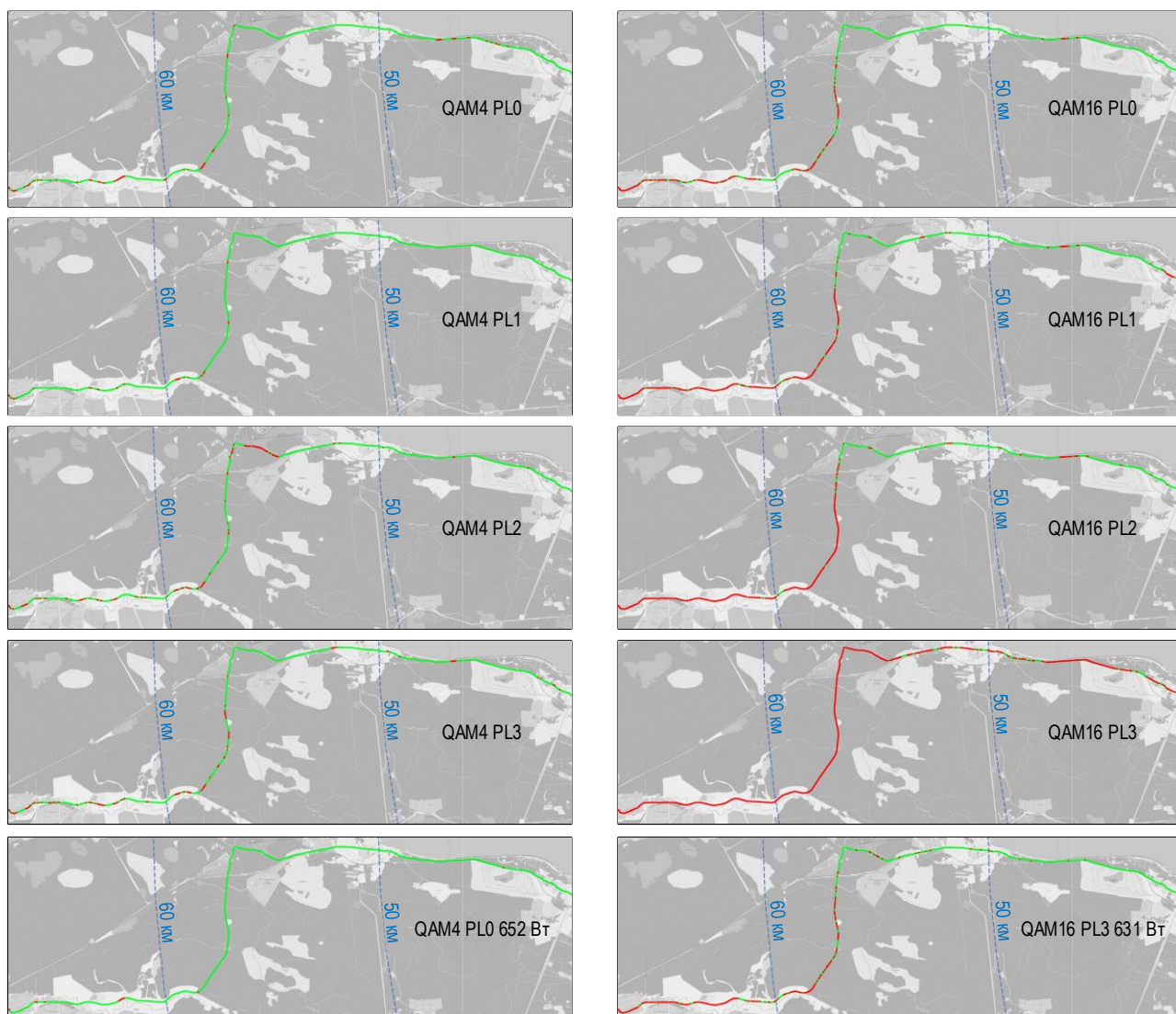


Рис. 6. Качество приема сигнала для разных режимов DRM в западном направлении

Fig. 6. Signal Reception Quality for Different DRM Modes in the Western Direction

До 57 км напряженность поля достаточна для корректного декодирования сигнала в режимах от QAM4 PL0 до QAM16 PL2, возникающие ошибки преимущественно связаны с помехами на маршруте. Напряженность поля резко падает после 57 км, и для режимов с QAM4 оказывается достаточной для приема сигналов вплоть до окончания зоны на 68 км маршрута, а для режимов QAM16 ограничением можно считать 57 км. Начиная с 69 км, при въезде в Сосновый Бор присутствует сильная помеха, не позволяющая декодировать

сигнал. Режим QAM16 PL3 аналогично предыдущим направлениям показывает существенно большее ухудшение характеристик приема, зона обслуживания ограничивается 41 км (гистограмма полного маршрута на рисунке 9). Увеличение мощности для QAM4 PL0 не расширяет зону обслуживания, ввиду ее ограничения сильной помехой, но улучшает качество приема в пределах всей зоны до близкого к безошибочному; для QAM16 PL3 существенно улучшает прием в части маршрута до 57 км до сопоставимого с QAM16 PL1 99Вт качества.

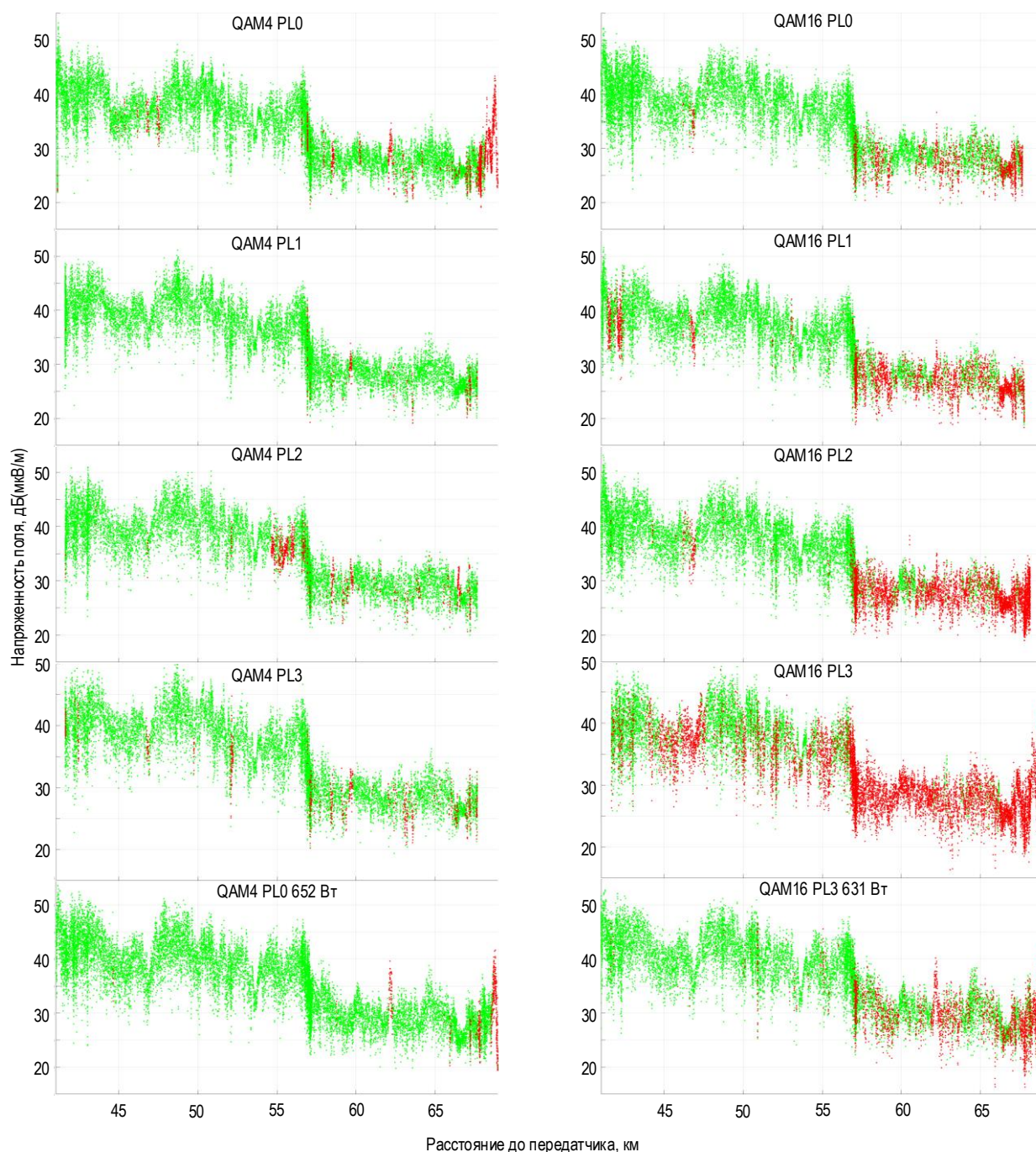


Рис. 7. Зависимости измеренной напряженности поля от расстояния до передатчика для маршрутов в западном направлении
Fig. 7. Dependences of the Measured Field Strength on the Distance to the Transmitter for Routes in the Western Direction

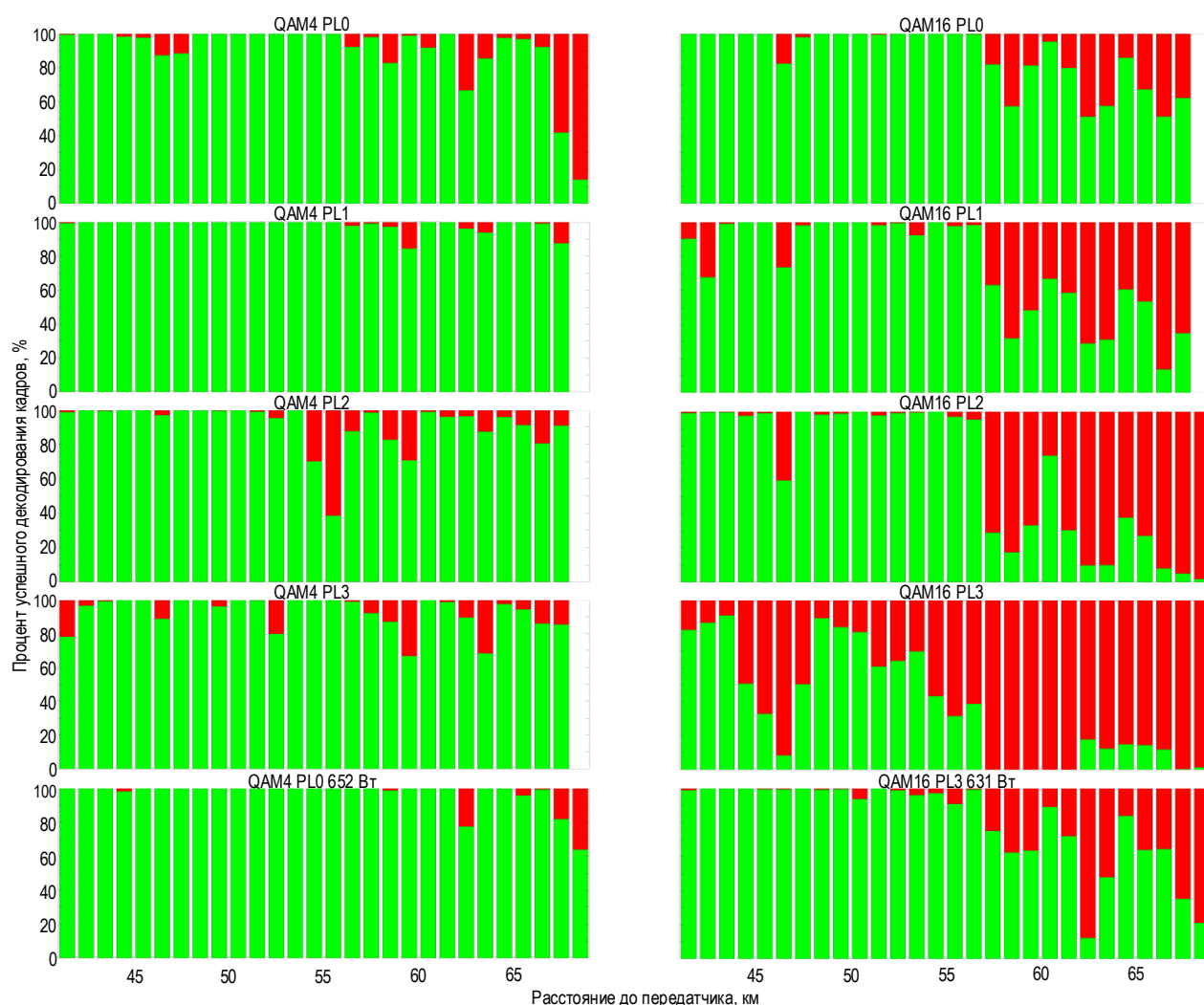


Рис. 8. Нормированные гистограммы качества декодирования сигнала в западном направлении

Fig. 8. Normalized Histograms of the Decoding Quality of the Signal in the Western Direction

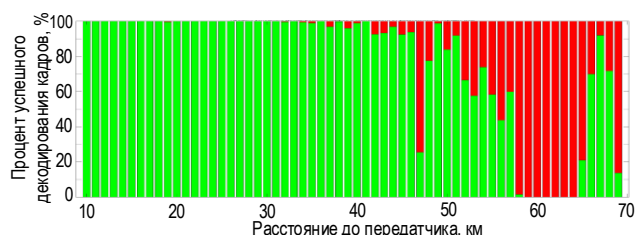


Рис. 9. Нормированная гистограмма качества декодирования сигнала в западном направлении при QAM16 PL3 99 Вт, полный маршрут

Fig. 9. Normalized Histogram of the Decoding Quality of the Signal in the Western Direction at QAM16 PL3 99 W, Full Route

ТАБЛИЦА 3. Интерпретация границ зон обслуживания, полученных в ходе измерений

TABLE 3. Interpretation of the Boundaries of Service Areas Obtained during Measurements

Направление	Граница зоны обслуживания, км			
	при QAM4 PL0		при QAM16 PL3	
	O	P	O	P
северное	64	64	31	49
восточное	72	77	30	64
юго-восточное	72	–	48	54
западное	68	68	41	57

Выводы по результатам исследований

Оценка границ зон обслуживания в основной серии измерений (O) и при повышенной мощности (P) на основании полученных экспериментальных данных в опытной зоне Санкт-Петербурга для наиболее (QAM4 PL0) и наименее (QAM16 PL3) помехоустойчивых режимов передачи DRM представлена в таблице 3.

Результаты измерений показывают следующее.

Во-первых, для маршрутов с ровным рельефом без резких провалов напряженности поля при применении помехоустойчивых режимов передачи увеличение мощности передатчика незначительно увеличивает зону обслуживания, т. к. ее ограничение обусловлено уменьшением напряженности поля до уровня радишумов при достижении гео-

метрического горизонта распространения радиоволн; при применении менее помехоустойчивых режимов передачи эффект увеличения зоны обслуживания более выражен, т. к. на продолжительном отрезке маршрута увеличивается запас на флуктуации радиосигнала до требуемых декодером значений SNR; для наименее помехоустойчивого режима QAM16 PL3 выигрыш в километрах достигает кратной разницы.

Во-вторых, для маршрутов, на которых ограничением является естественное затенение или наличие сильной помехи при применении помехоустойчивых режимов кодирования увеличение мощности передатчика мало влияет на размер зоны обслуживания, т. к. для компенсации эффекта затенения требуется существенно больший запас мощности, при этом в зонах неуверенного приема качество декодирования улучшается; при менее помехоустойчивых схемах кодирования увеличение мощности дает значительный эффект для расширения зоны обслуживания.

В ходе проведения измерений было выявлено большое количество помех выше среднего уровня шумов на всех маршрутах, как в условиях городской застройки, так и в сельской местности. Некоторые помехи были стационарными и проявлялись при разнесенных во времени измерениях. Очевидно, что преодоление данной проблемы методами радиопланирования невозможно и полностью зависимо от качества радиочастотного контрoля.

В целом, на сегодняшний день не разработан систематизированный подход к определению границ зоны обслуживания для системы DRM. При радиопланировании текущая практика апеллирует к граничным значениям напряженности поля, включающим запасы на быстрые и медленные замирания сигнала как для цифровых, так и для аналоговых систем [3–6]. Между тем характеристика ухудшения качества сигнала на границах зоны для цифровых и аналоговых систем существенно отличается. Несмотря на то, что критерий качества приема сигнала DRM является объективным параметром, а прием сигнала DRM носит выраженный пороговый характер: при определении границ зоны обслуживания в процесс неизбежно вовлечена субъективная оценка слушателей, т. е. при въезде в зону неуверенного приема часть слушателей сочтет качество приема неприемлемым и переключит станцию раньше, а часть – позже. Пороговый эффект цифровых систем в зоне неуверенного приема может значительно ухудшить субъективное восприятие звукового сигнала и существенно снизить зону обслуживания.

Учет малых зон с невыполнением критерия качества для цифровых систем является более ответственной задачей в сравнении с аналоговыми, т. е. если даже передатчик способен обеспечить достаточную среднюю напряженность поля вплоть до расстояния геометрического горизонта, но на маршруте движения слушателя будет присутствовать продолжительный участок неуверенного приема, реальная зона обслуживания для многих пользователей будет ограничена этим участком.

Как было отмечено выше, к определению границ зон обслуживания цифровой системы сложно применить объективный критерий ввиду субъективной природы восприятия ухудшения качества звука. В качестве одного из инструментов оценки данного параметра для режима мобильного приема предлагается ввести использование нормированных гистограмм распределения кадров DRM принятых с ошибками и без в дополнение к традиционно используемым формам представления данных мобильных измерений.

Возможности по гибкой настройке параметров мультимплекса DRM в части выбора схем модуляции-кодирования являются преимуществом стандарта. Выбор комбинации схемы модуляции и кодирования при передаче сигнала влияет на помехоустойчивость приема и объем данных, которые можно передать. Выбор параметров при проектировании радиостанции остается за вещателем и всегда является компромиссом между размером зоны обслуживания радиостанции и скоростью цифровых потоков (т. е. количеством программ, которые можно передать в одном мультимплексе). Стандарт позволяет включить в один мультимплекс, транслируемый в полосе частот 100 кГц – до 4 аудиопрограмм, каждая из которых кодируется наиболее эффективным на сегодняшний день кодеком xHE-AAC, а также широкий перечень дополнительных звуковых мультимедийных данных. Однако такая гибкость системы является скорее препятствием для практического внедрения технологии вещателями в условиях отсутствия исчерпывающих рекомендаций, позволяющих установить взаимосвязи между объемом передаваемого контента, требуемыми энергетическими характеристиками передающего оборудования и конечным охватом слушателей цифрового радиовещания.

Полученные в ходе измерений систематизированные статистические данные о распределении значений напряженности поля, SNR и уровня радишумов в дальнейшем будут использованы при разработке методики радиопланирования и радиоконтроля зон обслуживания передатчиков DRM в ОВЧ диапазоне.

Список используемых источников

1. Мышнянов С.В. Экспериментальное исследование влияния схем модуляции-кодирования на размер зоны обслуживания цифрового радиовещания стандарта DRM в диапазоне ОВЧ. Часть 1 // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 101–112. DOI:10.31854/1813-324X-2021-7-3-101-112
2. ETSI ES 201 980 V4.2.1 (2021-01) Digital Radio Mondiale (DRM). System Specification. European Broadcast Union.

3. Рекомендация МСЭ-R BS.1660-8 (06/2019) Техническая основа для планирования наземного цифрового звукового радиовещания в полосе ОВЧ.
4. Рекомендация МСЭ-R P.1546-6 (08/2019) Метод прогнозирования для трасс связи пункта с зоной для наземных служб в диапазоне частот от 30 МГц до 4000 МГц.
5. Рекомендация МСЭ-R P.1812-6 (09/2021) Метод прогнозирования распространения сигнала на конкретной трассе для наземных служб «из пункта в зону» в диапазонах УВЧ и ОВЧ.
6. Ковалгин Ю.А. О применении программы Radio Mobile для расчета зон покрытия передатчиков, работающих в диапазоне ОВЧ // Труды учебных заведений связи. 2021. Т. 7. № 2. С. 24–36. DOI:10.31854/1813-324X-2021-7-2-24-36

* * *

Experimental Research of Modulation-Coding Schemes Influence on Size of the DRM Digital Radio Broadcasting Service Area in the VHF Band. Part 2

S. Myshyanov¹ 

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info

DOI:10.31854/1813-324X-2021-7-4-138-146

Received 26th July 2021

Revised 6th December 2021

Accepted 6th December 2021

For citation: Myshyanov S. Experimental Research of Modulation-Coding Schemes Influence on Size of the DRM Digital Radio Broadcasting Service Area in the VHF Band. Part 2. *Proc. of Telecom. Universities*. 2021;7(4):138–146. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-138-146

Abstract: The article presents the results of measurements of the parameters of the digital radio broadcasting DRM signal quality in the experimental zone of St. Petersburg in order to determine the influence of the transmission modes laid down in the DRM standard on the size of the service area.

Keywords: digital radio broadcasting, DRM, service area, mobile measurements.

References

1. Myshyanov S. Experimental Research of Modulation-Coding Schemes Influence on Size of the DRM Digital Radio Broadcasting Service Area in the VHF Band. Part 1. *Proceedings of Telecommunication Universities*. 2021;7(3):101–112. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-101-112
2. ETSI ES 201 980 V4.2.1 (2021-01) *Digital Radio Mondiale (DRM). System Specification*. European Broadcast Union.
3. Rec. ITU-R BS.1660-8 (06-2019) *Technical basis for planning of terrestrial digital sound broadcasting in the VHF band*.
4. Rec. ITU-R P.1546-6 (08/2019) *Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 4 000 MHz*.
5. Rec. ITU-R P.1812-6 (09/2021) *A path-specific propagation prediction method for point-to-area terrestrial services in the frequency range 30 MHz to 6 000 MHz*.
6. Kovalgin Y. On the Application of the Radio Mobile Software for Calculating the Coverage Zones of Transmitters Broadcasting in the VHF Range. *Proc. of Telecom. Universities*. 2021;7(2):24–36. (in Russ.) DOI:10.31854/1813-324X-2021-7-2-24-36

Сведения об авторе:

МЫШЬЯНОВ
Сергей Васильевич

начальник научно-образовательного центра «Технологии информационных образовательных систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, mishyanov@gmail.com
 <https://orcid.org/0000-0002-7511-012X>

АПИНО
ICAIT

11TH INTERNATIONAL CONFERENCE
ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2022

**XI МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ
И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ
В НАУКЕ И ОБРАЗОВАНИИ»**

15–16
ФЕВРАЛЯ 2022

НАУЧНЫЕ НАПРАВЛЕНИЯ:

- Радиотехнологии связи
- Инфокоммуникационные сети и системы
- Информационные системы и технологии
- Теоретические основы радиоэлектроники и систем связи
- Цифровая экономика, управление и бизнес-информатика
- Гуманитарные проблемы информационного пространства
- Сети связи специального назначения



APINO.SPBGUT.RU

Подробности на сайте конференции

СПбГУТ)))

Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича



Выходные данные

Дизайн обложки – ООО «Комильфо»

План издания научной литературы 2021 г., п. 5

Дата выхода в свет	Усл.-печ. л.	Формат	Тираж	Заказ	Свободная цена
29.12.2021	14	60×84 _{1/8}	1000 экз.	№ 1240	

Ответственный редактор **Татарникова И.М.**
Выпускающий редактор **Яшугин Д.Н.**

Адрес типографии:
193232, Санкт-Петербург, пр. Большевиков, 22/1

Учредитель и издатель:

Федеральное государственное бюджетное образовательное учреждение
высшего образования "Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича"

E-mail: tuzs@spbgut.ru Web: tuzs.sut.ru VK: vk.com/spbtuzs



Подписной индекс в Объединенном каталоге "ПРЕССА РОССИИ" - 59983