Научно-технический журнал

H&ES RESEARCH

Scientific and Technical Journal

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.

Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссиейРоссии (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

Тематика публикуемых статей в соответствии с перечнем группспециальностей научных работников по Номенклатуре специальностей:

- 2.2.15 Системы, сети и устройства телекоммуникаций (техн. науки)
- 2.3.1 Системный анализ, управление и обработка информации (техн. науки)
- 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (техн. науки)
- 2.3.6 Методы и системы защиты информации, информационная безопасность (техн. науки)
- 2.5.13 Проектирование, конструкция и производство летательныхъх аппаратов (техн. науки)
- 2.5.16 Динамика, баллистика, управление движением летательных аппаратов (техн. науки)

H&ES Research is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the specialties:

- 2.2.15 Telecommunication systems, networks and devices
- 2.3.1 System analysis, management and information processing
- 2.3.5 Mathematical and software support for computing systems, complexes and computer networks
- 2.3.6 Methods and systems of information security
- 2.5.13 Design, construction and production of aircraft
- 2.5.16 Dynamics, ballistics, aircraft motion control

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

JOURNAL H&ES RESEARCH INDEXING

• NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Все номера журнала находятся в свободном доступе на сайте журнала **www.hes.ru** и библиотеке **elibrary.ru.**

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: **HT-ESResearch@yandex.ru.**
С требованиями можно ознакомиться на сайте: **www.H-ES.ru.**

Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.
Свидетельство о регистрации СМИ ПИ № ФС 77-60899 от 02.03.2015
Территория распространения: Российская Федерация, зарубежные страны

Тираж 1000 экз. Цена 1000 руб.
Плата с аспирантов за публикацию рукописи не взимается.

All issues of the journal are in a free access on a site of the journal **www.hes.ru** and **elibrary.ru.**

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: **HT-ESResearch@yandex.ru.**
The requirements are available on the website: **www.H-ES.ru.**

Language of publications: Russian, English.
Periodicity – 6 issues per year.
Media Registration Certificate PI No. FS77-60899. Date of issue: March 2, 2015.
Distribution Territory: Russian Federation, foreign countries

Circulation of 1000 copies. Price of 1000 Rur.
Postgraduate students for publication
of the manuscript will not be charged

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU Дата выхода: 20 ноября 2022

6 2022 Т.14

Учредитель:
ООО "ИД Медиа Паблишер"

Издатель:
ДЫМКОВА С.С.

Адрес издателя:
111024, Россия, Москва,
ул. Авиамоторная, д. 8, корп. 1, офис 323.

Адрес редакции:
194044, Россия, Санкт-Петербург,
Лесной Проспект, 34-36, к. 1,
Тел.: +7(911) 194-12-42.

Адрес типографии:
Россия, Москва, ул. Складочная, д. 3, кор. 6.

СОДЕРЖАНИЕ

CONTENTS

Founder:
"Media Publisher", LLC

Publisher:
DYMKOVA S.S.

Editor in chief:
LEGKOV K.E.

Address of publisher:
111024, Russia, Moscow,
st. Aviamotornaya, 8, bild. 1, office 323

Address of edition:
194044, Russia, St. Petersburg,
Lesnoy av., 34-36, h.1,
Phone: +7 (911) 194-12-42.

Address of printing house:
Russia, Moscow, st. Skladochnaya, 3, h. 6

doi: 10.36724/2409-5419-2022-14-6-4-11

ГИБРИДНЫЙ СПОСОБ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПОЛЬЗОВАТЕЛЯ ПРИ РАБОТЕ С ВЕБ-БРАУЗЕРОМ

ШЕЛУХИН
Олег Иванович[1]

ИГУМНОВ
Вадим Олегович[2]

АННОТАЦИЯ

Введение: Одной из распространённых уязвимостей конфиденциальности информации в Интернете является цифровое отслеживание, позволяющее идентифицировать пользователя, включающее cookie файлы и механизмы снятия цифровых отпечатков. Сравнительный анализ существующих современных способов веб-отслеживания показывает, что подходы, полагающиеся на выявление и блокировку веб-трекеров, являются менее эффективными, чем подходы, использующие подмену значений, так как не предоставляют защиту от методов пассивных отпечатков, а также являются легко обнаруживаемыми и, как следствие, подвержены возможности использования для идентификации пользователя. Для устранения этих недостатков должны быть разработаны новые, в общем случае комбинированные, способы и механизмы противодействия цифровому отслеживанию. **Цель исследования:** Анализ основных механизмов и разновидностей цифрового отслеживания, описание принципов их работы и разработка эффективного гибридного способа противодействия снятию цифрового отпечатка устройства пользователя. **Результаты:** Показано, что отслеживание с использованием цифровых отпечатков представляет наибольшую опасность, так как не может быть эффективно заблокировано со стороны браузера. Для решения проблемы предложен гибридный способ подмены передаваемых данных, включающий как рандомизацию, так и унификацию данных.Выбор подхода с подменой данных обусловлен тем, что он обеспечивает защиту от известных методов формирования цифровых отпечатков, а также в нем отсутствует этап выявления трекера, что позволяет обеспечить моментальную защиту. Характеристики, которые обладают более широким набором возможных значений и являются трудно унифицированными (Canvas, WebGL, Audio) предлагается подменять на реальные с добавлением незначительных искажений. Атрибуты, которые должны соблюдать свойство адекватности значений и изменение которых может нарушить работу сайта, будут подвергаться унификации. Унифицировать предлагается HTTP-заголовки и глобальные JavaScript параметры. Программная реализация предложенного алгоритма выполнена на языке программирования JavaScript в спецификации ECMAScript 6 с использованием стандарта кросс-браузерной системы разработки дополнений WebExtensions API.

КЛЮЧЕВЫЕ СЛОВА: *безопасность, конфиденциальность, браузер, цифровой отпечаток, cookie, фингерпринт, веб-трекеры, цифровое отслеживание.*

Сведения об авторах:

[1] д.т.н., профессор, зав. кафедры "Информационная безопасность", Московский Технический Университет Связи и Информатики, Москва, Россия, sheluhin@mail.ru

[2] магистрант, Московский Технический Университет Связи и Информатики, Москва, Россия, vad.igumnov@gmail.com

Для цитирования: Шелухин О.И., Игумнов В.О. Гибридный способ обеспечения конфиденциальности пользователя при работе с веб-браузером // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 4-11. doi: 10.36724/2409-5419-2022-14-6-4-11

Введение

Одной из распространённых уязвимостей конфиденциальности информации в Интернете является цифровое отслеживание – медленное, постоянное и непреклонное накопление данных о пользователе [1]. Составными частями этой уязвимости являются история просмотров, использование приложений, информация об онлайн-покупках и сведения о геолокации. Эти малозначительные отдельные данные могут быть объединены в значительное целое, которое позволяет идентифицировать пользователя. Трекеры собирают данные о кликах, просмотрах, нажатиях и переходах и создают обширные поведенческие профили, например, с целью показа таргетированной рекламы или оптимизации работы сайта. Однако эта информация может выявить политические предпочтения, религиозные убеждения, расу и этнос, уровень образования, ежемесячный доход, потребительские привычки, а также физическое и психическое здоровье и в руках злоумышленников может использоваться для дискриминации, шантажа или пропаганды [2].

По этой причине, вопрос о защите собственной конфиденциальности стоит особо остро. Для повышения конфиденциальности данных пользователя принимаются различные правовые и организационно-технические меры. К последним часто относят использование специального программного обеспечения, которое реализует один из существующих методов по противодействию цифровому отслеживанию. К таким методам относится выявление и блокировка выполнения программного кода веб-трекера, а также подмена передаваемых веб-ресурсу данных, для создания ложного профиля пользователя.

Механизмы цифрового отслеживания

К механизмам веб-трекинга в основном относят два метода отслеживания: использование файлов cookie [3, 4] и создание цифрового отпечатка устройства (браузера). Иногда их могут использовать совместно для увеличения точности идентификации.

Куки – это фрагмент данных, который веб-сайты хранят в браузере пользователя и обрабатывают при каждом подключении к сайту. Они могут хранить любую текстовую информацию размером 4096 байт. После создании файла сервером, cookie передаются в веб-браузер и сохраняются на компьютере пользователя. При каждом последующем подключении к сайту куки пересылаются обратно веб-серверу.

Наиболее часто их используют для хранения определенной информации, к которой относятся: данные для авторизации (логин, пароль, электронная почта), пользовательские настройки сайта и так далее. Однако часто в куки сохраняют уникальный идентификатор пользователя, присвоенный ему веб-ресурсом, который в последствии может быть использован для персональной идентификации пользователя на других веб-ресурсах.

Куки классифицируются по сроку действия: постоянные – такие куки могут храниться от нескольких месяцев до нескольких лет и сессионные, которые удаляются после закрытия браузера. В качестве механизма цифрового отслеживания используются постоянные куки.

Механизм отслеживания на основе куки файлов заключается в том, что на веб-сайте размещается скрипт стороннего сервера путём добавления фрагмента программного кода. Такой скрипт будет вызывать JavaScript код, размещённый на стороннем веб-сервере (рис. 1).

Рис. 1. Принцип отслеживания на основе Cookie файлов [5]

Данный код может выполнять различные функции, например, загружать и отображать рекламный баннер партнёрской рекламной сети или подгружать на сайт специальную программную библиотеку для разработчиков. Также в него может быть встроен код, который позволяет этому серверу устанавливать сторонние файлы cookie в браузер пользователей и отслеживать их, при загрузке данного скрипта.

Таким образом, веб-сервер, занимающийся отслеживанием, может разместить свой трекер на разных веб-сайтах и получать данные об истории посещений пользователя, времени нахождения на определенных страницах и прочие данные, которые предоставляются веб-сайтом со встроенным скриптом отслеживания (рис. 2).

Недостатком такого метода отслеживания является то, что cookie файлы, а соответственно и идентификационная информация о пользователе, хранятся на стороне пользователя. Данная особенность оставляет пользователю возможность удалить cookie файлы, тем самым временно остановить цифровое отслеживание. Поэтому часто в качестве веб-трекеров используют механизм снятия цифрового отпечатка или фингерпринтинг.

Под цифровым отпечатком понимается набор информации о программной и аппаратно-программной конфигурации устройства клиента, подключенного к веб-ресурсу. Основной концепцией снятия цифрового отпечатка является первичная и повторная идентификация пользователя на основе специфичной для устройства информации.

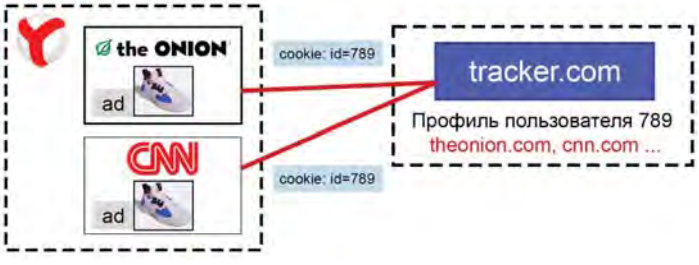

Рис. 2. Принцип отслеживания на основе Cookie [5]

Источниками информации для формирования цифрового отпечатка являются:

- данные о пользовательских настройках;
- характеристики оборудования;
- характеристики операционной системы;
- характеристики браузера;
- пользовательское поведение.

В качестве примера в таблице 1 приведен список информации, которую возможно собрать об устройстве пользователя.

Таблица 1

Информация, которая может быть собрана с помощью цифрового отпечатка

Параметр	Источник	Пример
User Agent	HTTP header, JavaScript	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.160 YaBrowser/22.5.1.985 Yowser/2.5 Safari/537.36
Accept	HTTP header	text/html,application/xhtml+xml,application/xml;q=0.9, image/avif,image/webp,image/apng,*/*;q=0.8, application/signed-exchange;v=b3;q=0.9
Accept-Language	HTTP-header, JavaScript	ru,en;q=0.9,ko;q=0.8
Accept-Encoding	HTTP-header	gzip, deflate, br
Content-Language	HTTP-header, JavaScript	de-DE, en-CA
DNT	HTTP-header, JavaScript	Null
App Version	JavaScript	5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.160 YaBrowser/22.5.1.985 Yowser/2.5 Safari/537.36
Vendor	JavaScript	Google Inc.
Platform	JavaScript	Win32
Screen Height	JavaScript	1920
Screen Width	JavaScript	1080

Цифровые отпечатки классифицируются по источнику и делятся на: пассивные – основанные на информации, автоматически передаваемой браузером в содержимом HTTP-заголовка и активные – собранные при выполнении JavaScript кода на стороне клиента, для получения информации, предоставляемой различными программными интерфейсами веб-браузера (API).

Помимо этого, существуют современные комплексные техники формирования цифровых отпечатков. Они являются наиболее эффективными, так как результат их работы зависит от параметров аппаратной конфигурации устройства, например, от используемого в устройстве графического ускорителя или звуковой карты. К таким техникам относятся Canvas Fingerprint, WebGL Fingerprint и Audio Fingerprint.

Canvas Fingerprint – метод получения характеристики устройства, который использует элемент Canvas веб-технологии HTML5. Этот элемент представляет из себя поверхность с возможностью отображения двумерной графики в браузере с помощью кода, выполняемого на стороне клиента. Суть метода в том, что на скрытом от пользователя canvas элементе рисуются некоторые графические элементы и текст. Результат выполнения отрисовки одинакового кода при этом может отличаться, в зависимости от операционной системы, библиотеки шрифтов, видеокарты, версии драйверов, браузерного движка и так далее. Полученное изображение представляется в виде строки закодированной в Base64 (рис. 3).

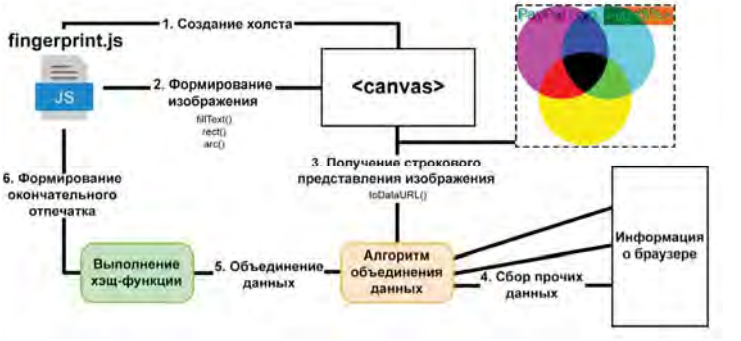

Рис. 3. Принцип Canvas Fingerprint

WebGL Fingerprint является развитием ***Canvas Fingerprint***. В данном случае, код веб-трекера заставляет браузер отрисовывать сцены с использованием технологии 3D графики, на которые также накладываются различные графические эффекты. Полученное изображение переводится в результирующий байтовый массив, который будет иметь отличия в зависимости от аппаратно-программной конфигурации устройства.

Audio Fingerprint заключается в генерации звуковых сигналов. Характеристики таких сигналов также могут отличаться из-за различий в оборудовании или используемом программном обеспечении. Данный метод реализуется за счёт интерфейса веб-браузера Web Audio API. В общем виде, такая техника снятия отпечатка представляет собой последовательную цепочку узлов для работы с аудио в браузере и происходит в три этапа: генерация звукового сигнала, анализ характеристик звукового сигнала, скрытие звукового сигнала. Данный метод включает в себя два разных подхода проиллюстрированных на рисунке 4. Основное их различие заключается в способе маскировки сгенерированного программным путём звука.

В первом случае используется интерфейс доступа к периферийному устройству вывода и для скрытия используется узел усилителя, установленным на 0. Во втором случае аудио сигнал не выводится на аппаратное обеспечение устройства, а сохраняется в специальный узел AudioBuffer, который сохраняет сигнал в памяти устройства. В качестве характеристик для анализа наиболее часто используют информацию о частотной области или результат линейной импульсно-кодовой модуляции.

Цифровой отпечаток в техническом плане представляет собой хэш-функцию от суммы результатов работы функции, где результат функции – это значение некоторой идентифицирующей особенности (характеристики).

Способы противодействия цифровому отслеживанию

Большинство браузеров не обеспечивают конфиденциальность информации пользователей по умолчанию. Это значит, что они позволяют хранить файлы cookie, в том числе полученные от третьих лиц, а также никак не ограничивают существующие интерфейсы, использующиеся при формировании цифровых отпечатков. Большая часть пользователей не оптимизируют безопасность выбранного браузера. Чаще всего такое поведение обосновано отсутствием данного шага при установке программы для работы с ресурсами Интернет, а также недостаточной осведомленностью пользователей.

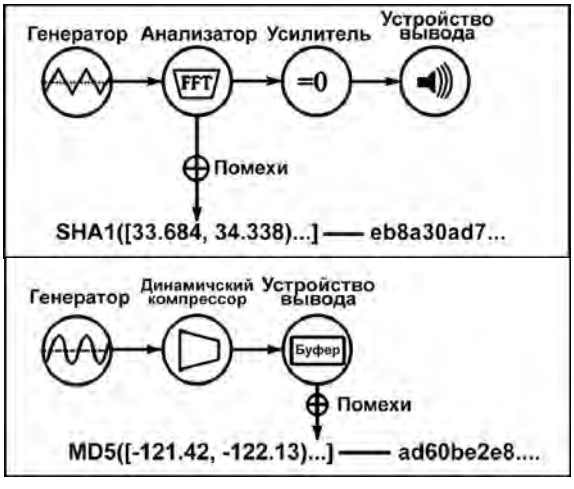

Рис. 4. Механизмы работы Audio Fingerprint

Для предотвращения отслеживания с помощью файлов cookie достаточно установить соответствующие опции в настройках браузера. Как правило, все современные браузеры предоставляют функцию блокировки cookie файлов, при этом часто разделяя куки файлы на основные и сторонние. Блокировка сторонних cookie файлов избавит пользователя от однозначно идентифицирующего отслеживания сторонними сайтами.

Значительно более сложной является задача повышения защищенности пользователя от фингерпринтинга, поскольку в этом случае контрмеры, предоставляемые браузером, очень ограничены и малоэффективны. Так, например, можно применить настройку, блокирующую выполнение любого JavaScript кода, что безусловно повысит защищенность пользователя от большинства современных техник веб-отслеживания, однако частично или полностью нарушит работоспособность почти всех сайтов. К тому же, все равно остаются способы снятия цифровых отпечатков, например, использование пассивных отпечатков.

Вследствие невозможности для современного пользователя отключения JavaScript в браузере, предложены два концептуальных способа по противодействию снятию отпечатков устройства, представленные на рисунке 5.

Первый способ заключается в выявлении и блокировании выполнения кода веб-трекеров. При реализации такого подхода браузер или расширение блокирует выполнение отслеживающих скриптов на основе списка фильтрации, которые включают в себя перечень правил, то есть доменных имён или URL скриптов отслеживания или поведения скрипта.

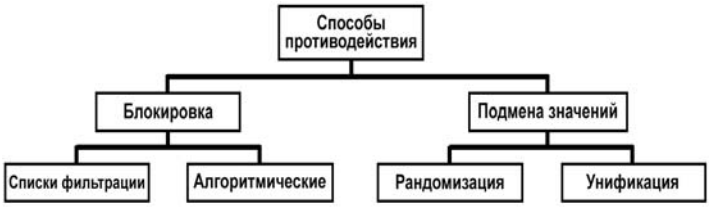

Рис. 5. Способы противодействия фингерпринтингу

Достоинством такого подхода является низкая вероятность нарушения работоспособности веб-сайтов. Однако такой подход не является эффективным по ряду причин:

- Решения, блокирующие трекеры на основе списков фильтрации, могут не учитывать отслеживание на небольших локальных или региональных сайтах. Это доказывают некоторые исследования [5], в которых показано, что при подобном подходе блокируется менее 50% трекеров.
- Необходимо постоянно обновлять список фильтрации, либо полагаться на обновления существующих списков, которые могут производиться с задержкой.
- Необходимо полагаться на честность и добропорядочность разработчиков списков фильтрации, так как они обладают возможностью скрывать или подменять определенный контент для пользователей их списков [6].
- Такие расширения используют проверку запросов браузера на низком уровне, замедляя время отклика.
- Большинство списков фильтрации полагаются на блокировку по домену, тем самым могут происходить ложные срабатывания, когда блокируются ресурсы домена, не относящиеся к трекингу.

Второй способ противодействия цифровому отслеживания заключается в подмене собираемых данных и в свою очередь делится на две разновидности: рандомизация и унификация данных.

Рандомизация заключается в генерации случайных значений полей, передаваемых данных при каждом обновлении страницы так, чтобы каждое взаимодействие между пользователем и сайтом формировало разные отпечатки. Суть метода заключается в том, что третьи стороны полагаются на стабильность цифровых отпечатков чтобы связать их с одним устройством. Отправляя случайные значения вместо реальных, собранные отпечатки становятся настолько разными и нестабильными, что трекер не может идентифицировать устройства в сети. Недостатком является то, что рандомизация неадекватных комбинаций определенных параметров может привести к снижению конфиденциальности пользователя.

Унификация предполагает, что передаваемые данные приводятся к единообразию для каждого пользователя. Проблемой данного способа является отсутствие возможности подмены некоторых атрибутов, например, характеристик аппаратной конфигурации устройства. Наличие неизменных уникальных атрибутов становится серьёзной уязвимостью для безопасности пользователя, особенно если они будут несовместимы с унифицированными данными.

Сравнительный анализ существующих способов приведён в таблице 2. По результатам анализа, можно сделать вывод о том, что подходы, полагающиеся на выявление и блокировку веб-трекеров, являются менее эффективными, чем подходы, использующие подмену значений, так как не предоставляют защиту от методов пассивных отпечатков, а также являются легко обнаруживаемыми и, как следствие, подвержены возможности использования для идентификации пользователя.

Таблица 2

Сравнительный анализ способов противодействия цифровому отслеживания

	Блокировка на основе списка фильтрации	Блокировка на основе поведения	Подмена с использованием рандомизации данных	Подмена с использованием унификации данных
Влияние на корректную работу веб-сайтов	Низкое	Высокое	Высокое	Низкое
Влияние на скорость загрузки веб-страниц	Нет	Нет	Высокое	Низкое
Вероятность ложного срабатывания	Низкая	Высокая	Нет	Нет
Противодействие пассивным отпечаткам	Нет	Нет	Да	Да
Противодействие снятию JavaScript отпечатков	Да	Да	Да	Да
Противодействие отслеживанию третьими лицами	Да	Да	Да	Да
Противодействие отслеживанию первыми лицами	Нет	Да	Да	Да
Вероятность обнаружения и добавление уникальности	Высокая	Высокая	Низкая	Высокая
Область покрытия	30-50%	до 100%	~100%	~100%

Гибридный способ противодействия цифровым отпечаткам

Для решения проблемы противодействия цифровому отслеживания предлагается вариант гибридного подхода подмены передаваемых данных, включающий как рандомизацию, так и унификацию некоторых данных.

Выбор способа с подменой данных обуславливается тем, что он обеспечивает защиту от всех рассмотренных методов формирования цифровых отпечатков, а также в нем отсутствует этап выявления трекера, что позволяет обеспечить моментальную защиту.

При предлагаемом варианте характеристики, которые обладают более широким набором возможных значений и являются трудно унифицированными (Canvas, WebGL, Audio), будут подменяться на реальные с добавлением небольших искажений. В свою очередь, атрибуты, которые должны соблюдать свойство адекватности значений и изменение которых может нарушить работу сайта, будут подвергаться унификации. Их значение будет соответствовать моде частотного распределения возможных вариантов, иными словами, наиболее часто встречаемое [7]. При этом планируется учитывать связность параметров между собой, а также адекватность их значений.

Унифицировать предлагается следующие параметры: HTTP-заголовки (User-Agent, Accept-Language, Content-Language, DNT) и глобальные JavaScript параметры браузера (navigator.userAgent, navigator.appVersion, navigator.userAgentData, navigator.vendor, navigator.platform, navigator.language, navigator.languages, navigator.doNotTrack, screen.height, screen.width, screen.pixelDepth).

В первую очередь, перед отправкой HTTP-запроса с требуемыми заголовками на запрашиваемый веб-сервер, значение описанных заголовков будут заменяться и передаваться уже в измененном виде. Таким образом, будет обеспечена защита от пассивных цифровых отпечатков.

Затем, после начала загрузки страницы, но до загрузки и выполнения каких-либо других скриптов, будет происходить внедрение и выполнение скрипта, осуществляющего подмену значений глобально доступных JavaScript параметров, перечисленных ранее. После этого будут загружаться все прочие скрипты на сайте. Таким образом, все вебтрекеры при попытке получить значения характеристик через API браузера, будут получать уже измененные значения как это показано на рисунке 6.

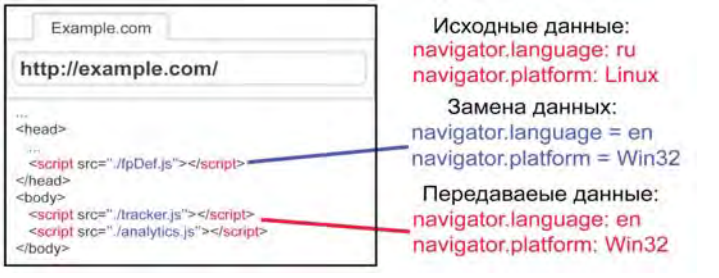

Рис. 6. Принцип подмены значений глобальных параметров JavaScript

Следующим этапом, будет обеспечение защиты от известных техник снятия отпечатков, описанных ранее. Общий принцип работы защиты для каждого способа скрытия одинаковый.

Скрипт защиты будет переопределять программную реализацию JavaScript методов используемых при формировании отпечатков. В дальнейшем, при попытке веб-сайта сгенерировать цифровой отпечаток, при использовании методов будет происходить выполнение переопределенного кода. Суть переопределения заключается в том, что к фактическим цифровым отпечаткам будут добавляться случайные помехи. Данное действие будет совершаться при каждом использовании соответствующих методов в браузере.

Добавление помех на элемент canvas будет проходить в несколько этапов:

1. После того, как на странице создаётся холст, выполнение соответствующего скрипта останавливается до выполнения скрипта защиты.
2. Скрипт защиты копирует данные значений пикселей холста (canvas).
3. Изменяется значение красного, зеленого и синего цвета каждого пикселя на небольшое случайное значение.
4. Подменяется холст (canvas).
5. Скрипт возвращает управление скрипту веб-трекера для дальнейшей обработки.

Алгоритм технологии снятия отпечатков с применением WebGL похож на предыдущий. Однако в этом случае помехи будут добавляться в буфер данных отрисованной сцены, который впоследствии используется для формирования отпечатка. Буфер данных может содержать значения координат вершин, по которым происходит отрисовка, либо значения цветов.

Для Audio Fingerprint предлагается заменить программную реализацию некоторых узлов, получающие характеристики сгенерированных аудиосигналов. В частности, предлагается изменить узел анализатора (AnalyserNode) и узел буфера вывода (AudioBuffer) (рис. 7).

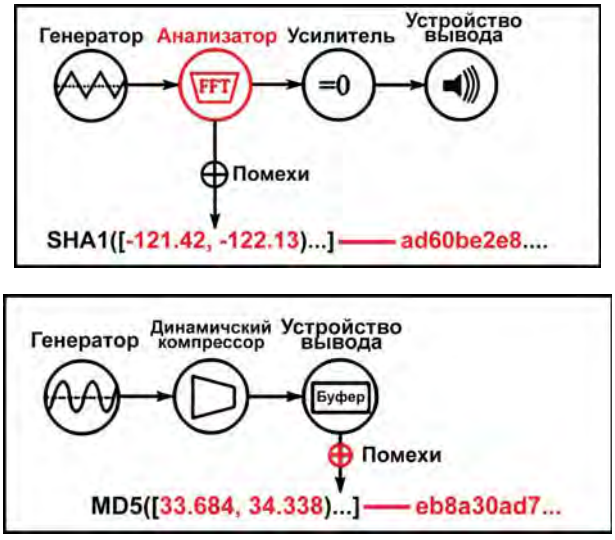

Рис. 7. Принцип защиты от Audio Fingerprint

Программная реализация предложенного алгоритма выполнена на языке программирования JavaScript в спецификации ECMAScript 6 с использованием стандарта кроссбраузерной системы разработки дополнений WebExt. Основными элементами программной реализации являются «Замена значений передаваемых заголовков», «Внедрение скрипта защиты», «Выполнение скрипта защиты», «Замена значений глобальных параметров JavaScript», «Замена реализации методов интерфейсов Canvas, WebGL, AudioContext».

Заключение

Показана возможность нарушения конфиденциальности пользователя при работе с веб-браузером с использованием веб-трекеров.

Рассмотрены основные механизмы цифрового отслеживания, описаны принципы их работы, разновидности и современные реализации. Выявлено, что отслеживание с использованием цифровых отпечатков представляют наибольшую опасность, так как не могут быть эффективно заблокированы со стороны браузера.

Предложен гибридный способ противодействия отслеживания цифровых отпечатков, заключающийся в унификации простых характеристик с соблюдением взаимосвязи и адекватности значений, а также рандомизации комплексных характеристик, зависящих от аппаратной конфигурации устройства и не подвергающихся унификации.

Литература

1. *Sanchez-Rola I., Santos I.* Knockin' on Trackers' Door: Large-Scale Automatic Analysis of Web Tracking. In: Giuffrida, C., Bardin, S., Blanc, G. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2018. Lecture Notes in Computer Science, vol. 10885. Springer, Cham. doi:10.1007/978-3-319-93411-2_13
2. *Gebhart G., Cyphers B.* Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance / Electronic Frontier Foundation. URL: https://www.eff.org/wp/behind-the-one-way-mirror (date of access 31.10.2022)
3. *Гадельшин А.А., Степанов М.М.* Cookie-файлы как объект персональных данных и способ нарушения конфиденциальности персональных данных // Вопросы российской юстиции. 2021. № 16. С. 516-531.
4. *Chen Q., Panagiotis I., Polychronakis M., Karpavelos A.* Cookie Swap Party: Abusing First-Party Cookies for Web Tracking // Материалы Web Conferenct 2021 (WWW '21) (Нью-Йорк, США, апрель 2021). С. 2117-2129. doi:10.1145/3442381.3449837
5. *Castell-Uroz I., Solé-Pareta J.* TrackSign: Guided Web Tracking Discovery // IEEE Instrumentation & Measurement Magazine. 2020. №23(9). С. 50-57. doi: 10.1109/INFOCOM42981.2021.9488842
6. *Колесников А.* uBlock Origin – быть или не быть // Habr – URL: https://habr.com/ru/sandbox/138904/ (дата обращения: 24.09.2022)
7. Most Common User Agents // Tech Blog (wh) URL: https://techblog.willshouse.com/2012/01/03/most-common-user-agents/ (дата обращения: 24.09.2022)
8. *Copland S.* The Top Browser Fingerprinting Techniques Explained // FingerprintJS Pro – Device fingerprinting and fraud detection API. URL: https://fingerprintjs.com/blog/browser-fingerprinting-techniques/ (дата обращения: 24.09.2022)
9. *Laperdrix P., Rudametkin W., Baudry B.* Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints // Материалы 2016 IEEE Symposium on Security and Privacy (SP). С. 878-894, doi:10.1109/SP.2016.57

10. *Iordanou C., Smaragdakis G., Poese I., Laoutaris N.* Tracing Cross Border Web Tracking // Internet Measurement Conference 2018. 2018. doi: https://doi.org/10.1145/3278532.3278561

11. *Englehardt S., Narayanan A.* Online tracking: A 1-million-site measurement and analysis // Материалы 2016 ACM SIGSAC conference on computer and communications security. Октябрь 2016. С. 1388-1401. doi:10.1145/2976749.2978313

12. *Libert T.* Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites // International Journal of Communication. 2015. № 9. С. 3544-3561.

13. *Samarasinghe N.* Towards a global perspective on web tracking // Computers & Security. 2019. doi:10.1016/j.cose.2019.101569

14. *Ermakova T., Fabian B., Bender B., Klimek K.* Web Tracking – A Literature Review on the State of Research // The Hawaii International Conference on System. 2018. doi:10.24251/HICSS.2018.596

15. *Nibbeling N.* Comparing privacy plugins // Radboud University URL:https://www.cs.ru. nl/bachelors-theses/2019/Nick_Nibbeling___4616146 Comparing_privacy_ plugins.pdf (дата обращения: 05.06.2022)

16. *Gómez-Boix A., Laperdrix P., Baudry B.* Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale // Материалы WWW2018 - TheWebConf 2018: 27th International World Wide Web Conference (Лион, Франция, апрель 2018). Лион, 2018. С. 309-31. doi:10.1145/3178876.3186097

17. *Cao Y., Li S., Wijman E.* (Cross-) Browser Fingerprinting via OS and Hardware Level Features // Материалы NDSS Symposium 2017(Сан-Диего, Калифорния, февраль-март, 2017) Сан-Диего, 2017. doi:10.14722/NDSS.2017.23152

18. *Shubham A.* Your digital fingerprint is tracked everywhere online. Brave wants to change that // Digital Trends. URL: https://www.digitaltrends.com/computing/digital-fingerprinting-online-privacy-brave/ (дата обращения: 12.05.2022).

19. *Ильницкий А.С.* О некоторых аспектах преступности в теневом Интернете // Уголовная политика и культура противодействия преступности. Материалы Международной научно-практической конференции. Краснодар. 2019. С. 14-18.

20. *Дубровин О.В., Ковалева И.Ю.* Защита персональных данных в сети Интернет: пользовательское соглашение // Вестник Южно-Уральского государственного университета. Серия: «Право». 2014. №2. С. 64-70.

HYBRID WAY TO ENSURE USER PRIVACY WHEN WORKING WITH A WEB-BROWSER

OLEG I. SHELUHIN
Moscow, Russia, sheluhin@mail.ru

VADIM O. IGUMNOV
Moscow, Russia, vad.igumnov@gmail.com

KEYWORDS: *security, confidentiality, web browser, digital fingerprint; cookie, fingerprint; web tracker, digital tracking.*

ABSTRACT

Intoduction: One of the most common privacy vulnerabilities on the Internet is digital tracking that identifies users, which includes cookies and digital fingerprinting mechanisms. A comparative analysis of existing modern web tracking methods shows that approaches that rely on detecting and blocking web trackers are less effective than ones using value spoofing, since they do not provide passive fingerprinting methods protection, and are also easily detectable and, as a consequence, are susceptible to being used user identification. To eliminate these shortcomings, new, generally combined, methods should be developed. **Purpose** is to analyze the main mechanisms and varieties of digital tracking, describe the principles of their operation and develop an effective hybrid method to counteract the digital fingerprinting of the user's device. **Results:** It is shown that fingerprint tracking is extremely dangerous, as it cannot be effectively blocked by the browser. To solve the problem, a hybrid method of spoofing transmitted data, including both randomization and unification, is proposed. This method is chosen due to the fact that it provides protection against known digital fingerprinting methods. In addition, the method lacks the tracker detection stage, that provides instant protection. Characteristics with a wider range of possible values, that are also difficult to unify (Canvas, WebGL, Audio) are proposed to be replaced with the real ones with the addition of minor distortions. Attributes that must comply with the value adequacy property and changing of which may disrupt the website will be unified. Consequently, it is proposed to unify HTTP headers and global JavaScript browser parameters. The software implementation of the described algorithm is made in the JavaScript programming language in the ECMAScript 6 specification using the standard of the WebExtensions API cross-browser add-on development system.

REFERENCES

1. I. Sanchez-Rola, I. Santos (2018). Knockin' on Trackers' Door: Large-Scale Automatic Analysis of Web Tracking. In: Giuffrida, C., Bardin, S., Blanc, G. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2018. *Lecture Notes in Computer Science*, vol 10885. Springer, Cham. doi:10.1007/978-3-319-93411-2_13

2. G. Gebhart, B. Cyphers (2022). Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance / Electronic Frontier Foundation. https://www.eff.org/wp/behind-the-one-way-mirror (date of access 31.10.2022)

3. A.A. Gadelshin, M.M. Stepanov (2021). Cookies as an object of personal data and a way to violate the confidentiality of personal data. Voprosy rossiyskoy yustitsii [Issues of Russian justice]. No. 16, pp. 516-531 (In Rus).

4. Q. Chen, I. Panagiotis, M. Polychronakis, A. Karpavelos (2021). Cookie Swap Party: Abusing First-Party Cookies for Web Tracking. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, pp. 2117-2129. doi:10.1145/3442381.3449837

5. I. Castell-Uroz, J. Sol-Pareta (2020). TrackSign: Guided Web Tracking Discovery. *IEEE Instrumentation & Measurement Magazine*. No. 23(9), pp. 50-57. doi: 10.1109/INFOCOM42981.2021.9488842

6. A. Kolesnikov (2022). uBlock Origin - byt' ili ne byt' [uBlock Origin - to be or not to be]. https://habr.com/ru/sandbox/138904/ (date of access: 24.09.2022). (In Rus)

7. Most Common User Agents. https://techblog.willshouse.com/2012/01/03/most-common-user-agents/ (date of access: 24.09.2022)

8. S. Copland (2022). The Top Browser Fingerprinting Techniques Explained // FingerprintJS Pro - Device fingerprinting and fraud detection API. URL: https://fingerprintjs.com/blog/browser-fingerprinting-techniques/ (date of access: 24.09.2022)

9. P. Laperdrix, W. Rudametkin, B. Baudry (2016). Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. *In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, pp. 878-894, doi:10.1109/SP.2016.57

10. C. Iordanou, G. Smaragdakis, I. Poese, N. Laoutaris (2018). Tracing Cross Border Web Tracking. *Internet Measurement Conference 2018.* doi: https://doi.org/10.1145/3278532.3278561

11. S. Englehardt, A. Narayanan (2016). Online tracking: A 1-million-site measurement and analysis. *In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. October 2016, pp. 1388-1401. doi:10.1145/2976749.2978313

12. T. Libert (2015). Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication*. No. 9, pp. 3544-3561.

13. N. Samarasinghe (2019). Towards a global perspective on web tracking. *Computers & Security*. doi:10.1016/j.cose.2019.101569

14. T. Ermakova, B. Fabian, B. Bender, K. Klimek (2018). Web Tracking – A Literature Review on the State of Research. *The Hawaii International Conference on System*. doi:10.24251/HICSS.2018.596

15. N. Nibbeling (2019), Comparing privacy plugins. Radboud University. https://www.cs.ru. nl/bachelors-theses/2019/Nick_Nibbeling___4616146___Comparing_privacy_ plugins.pdf (date of access: 05.06.2022)

16. A. Gomez-Boix, P. Laperdrix , B. Baudry (2018). Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale. *In Proceedings of the WWW2018 - TheWebConf 2018: 27th International World Wide Web Conference* (Lyon, France, april 2018), pp. 309-31. doi:10.1145/3178876.3186097

17. Y. Cao, S. Li, E. Wijman (2017). (Cross-) Browser Fingerprinting via OS and Hardware Level Features. *NDSS Symposium 2017* (San-Diego, California, febrary-march, 2017). doi:10.14722/NDSS.2017.23152

18. A. Shubham (2022). Your digital fingerprint is tracked everywhere online. Brave wants to change that, Digital Trends. URL: https://www.digitaltrends.com/computing/digital-fingerprinting-online-privacy-brave/ (date of access: 12.05.2022)

19. A.S. Il'nitskiy (2019). Some aspects of crime on the shadow Internet. *Criminal policy and culture of countering crime. Proceedings of the International Scientific and Practical Conference*. Krasnodar, pp. 14-18.

20. O.V. Dubrovin, I.Yu. Kovaleva (2014). Protection of Personal Data on the Internet: User Agreement. *Bulletin of South Ural State University. Series: Justice*. No. 2, pp. 64-70.

INFORMATION ABOUT AUTHORS:

Oleg I. Sheluhin, Dr.Sc., Professor, Head of the Department of Information security, Moscow Technical University of Communications and Informatics, Moscow, Russia

Vadim O. Igumnov, Student, Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Sheluhin O.I., Igumnov V.O. Hybrid way to ensure user privacy when working with a web-browser. *H&ES Reserch*. 2022. Vol. 14. No 6. P. 4-11. doi: 10.36724/2409-5419-2022-14-6-4-11 (In Rus)

doi: 10.36724/2409-5419-2022-14-6-12-19

О ВОЗМОЖНОСТИ ЧИСЛЕННЫХ МЕТРИК В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ВОВИК
Андрей Геннадьевич[1]

ЛАРИН
Александр Иванович[2]

АННОТАЦИЯ

Введение. Существующий аппарат управления информационной безопасностью в информационных системах представляет собой совокупность неформализованных вербальных моделей. Они позволяют определять комплекс мероприятий, но лишены возможности проводить численные оценки – сравнивать альтернативные стратегии по введенному критерию, численно фиксировать изменения в состоянии защищенности информации, выполнять математически обоснованную оптимизацию управляющих воздействий. Отдельные попытки формализовать модели носят частный, специфический характер и не выходят за рамки аналитических или статистических представлений. При этом аналитические методы предполагают искусственное игнорирование неопределенности. Применение статистических методов ограничено с одной стороны невозможностью достоверной оценки вероятностных характеристик переменных модели, а с другой стороны с существенными сложностями доказательства репрезентативности используемых выборок. **Цель исследования:** Целью исследования является обоснование возможности использования численных оценок в управлении информационной безопасностью. **Методы:** Поиск альтернативных методов моделирования процессов управления ИБ начинается с классификации объекта моделирования. Объект моделирования – процесс управления информационной безопасностью – рассматривается как сложная система с неустранимой неопределенностью. В качестве используемого метода моделирования выбран метод с применением нечетких алгоритмов на основании алгоритмов вывода на правилах Мамдани, а также принцип вложенности моделей для построения модели системы управления информационной безопасностью информационной системы. **Результаты:** Обоснована чувствительность, непрерывность и качественная адекватность описанной модели, показана возможность оперативного отслеживания влияния дестабилизирующих воздействий на уровень защищенности информации в информационной системе с помощью численной метрики. **Практическая значимость:** Использование предложенных методов открывает возможности построения автоматической системы управления безопасностью информационной системы.

Сведения об авторах:

[1] ассистент каф. ИСУиА, Московский технический университет связи и информатики, Москва, Россия, a.g.vovik@mtuci.ru

[2] к.т.н., доцент каф. ИСУиА, Московский технический университет связи и информатики, Москва, Россия, a.i.larin@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: *управление информационной безопасностью, численная метрика, нечеткая логика, алгоритм Мамдани*

Для цитирования: Вовик А.Г., Ларин А.И. О возможности численных метрик в управлении информационной безопасностью // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 12-19. doi: 10.36724/2409-5419-2022-14-6-12-19

Введение

Под системой защиты информации (СЗИ) в информационной системе понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности [1].

Современные СЗИ используют большой спектр известных на сегодня методов и способов защиты информации от различный угроз информационной безопасности на основе организационных, программных, аппаратных и программно-аппаратных мер. Совокупность применяемых мер объединяются в такие группы как организационно-правовые меры, техническая защита, криптографическая защита, физическая защита. Основным назначением СЗИ можно считать снижение уровня уязвимости информационной системы к воздействию разнообразных угроз информационной безопасности и, как следствие, снижение информационных рисков до приемлемого уровня. При этом уровень приемлемого риска определяется владельцем информации, который выступает как лицо принимающее решение (ЛПР) исходя в том числе из предпочтений ЛПР.

Совокупность взаимосвязанных мер защиты информации формируют структуру СЗИ, которая в свою очередь, характеризуется способностью эффективно противостоять объективно существующим угрозам. Из всего множества угроз чаще всего в практической деятельности используют термин «актуальные угрозы». Критерии для отнесения той или иной угрозы к актуальным – наличие хотя бы одного сценария угрозы безопасности информации. Под сценарием понимается способ реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

Вместе с тем, сама структура СЗИ не является стабильной, предполагается, что она изменяется во времени [2]. Основными причинами необходимости изменения СЗИ являются:

- идентификация ранее не учитываемых угроз информационной безопасности, что обусловлено развитием информационных технологий, появление у злоумышленников новых программно-аппаратных средств, повышение их квалификации и проч.;
- выявление ранее неизвестных уязвимостей в защищаемой системе, например, о выявлении новых уязвимостей в программном обеспечении вендоры регулярно оповещают потребителей;
- изменение структуры или конфигурации самой защищаемой системы, что может быть вызвано ее расширением или изменением основных бизнес-процессов;
- изменение стоимости информации в защищаемой информационной системе;
- и рядом других причин.

Своевременное реагирование на снижение эффективности СЗИ, вызванное в том числе перечисленными выше причинами, и заключающееся в изменении структуры СЗИ с целью недопущения повышения информационных рисков в защищаемой системе является одной из функций системы управления информационной безопасностью (СУИБ).

Требования к системе управления информационной безопасностью

Можно сказать, что система управления информационной безопасностью в совокупности с системой защиты информации и формируют понятие «информационная безопасность».

Основные вопросы содержания понятия «управление информационной безопасностью», стандартизация основных мероприятий, формирующих процесс управления, отражены в различных нормативных документах: серии стандартов ГОСТ Р ИСО/МЭК 27000-27004 «Менеджмент информационной безопасности, в РД ФСТЭК в части защиты информации от несанкционированного доступа. Отдельные вопросы регламентируются также в ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель». В основе современных представлений об управлении информационной безопасностью лежат процессный и риск-ориентированный подходы.

Существующий аппарат управления информационной безопасностью в информационных системах представляет собой совокупность неформализованных вербальных моделей. Они позволяют определять комплекс необходимых мероприятий, но лишены возможности проводить численные оценки – сравнивать альтернативные стратегии по введенному критерию, численно фиксировать изменения в состоянии защищенности информации, выполнять математически обоснованную оптимизацию управляющих воздействий.

Так, например, одним из обязательных требований к СУИБ является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты. Также в ряде руководящих документов, приводятся требования к показателям эффективности и наименования этих показателей. Однако, предлагаемые показатели носят качественный характер и часто не охватывают всей предметной области. В РД ФСТЭК приведены показатели отдельно для автоматизированных систем и отдельно для средств защиты, кроме того, все они имеют отношение к подсистеме защиты от несанкционированного доступа (НСД) и не учитывают другие виды угроз. В ГОСТ Р ИСО/МЭК 27004-2021 так же указаны только требования, предъявляемые к показателям эффективности.

Разработанные ФСТЭК Методические указания, призванные конкретизировать положения и требования существующих стандартов для практического применения, так же лишены метрик. Оценку угроз безопасности информации предлагается проводить с использованием экспертного метода. Возможные негативные последствия от реализации угроз безопасности информации так же предложено определять как на основе экспертной оценки специалистов, проводящих оценку угроз безопасности информации, так и на основе информации, представляемой профильными подразделениями или специалистами обладателя информации. При этом в Приложении 2 к Методике «Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации» указано, что экспертная группа должна включать не менее трех человек, а итоговое

среднее значение оцениваемого параметра определяется как среднее значение оцениваемого параметра. Экспертную оценку рекомендуется проводить в отношении следующих параметров:

а) негативного последствия от реализации угроз безопасности информации;

б) целей нарушителей по реализации угроз безопасности информации;

в) сценария действий нарушителей при реализации угроз безопасности информации.

В качестве шкалы измерений предполагается использовать «низкий», «средний», «высокий» или «да», «нет» или иные шкалы.

Предложенный способ проведения экспертной оценки вызывает вопросы относительно корректности обработки полученных от экспертов оценок, так как не проводится оценка коэффициента согласованности (или непротиворечивости) и не учитываются веса, приписываемые к оценке каждого эксперта, так как даже в группе из 3 человек ситуация идентичности компетенции всех членов группы маловероятна [3].

Кроме того, одним из требований к СУИБ является периодичность контроля эффективности СЗИ. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами. Так как оценка эффективности предполагает также и оценку угроз, то такую экспертную группу необходимо собирать также периодически или она должна быть постояннодействующей. Учитывая необходимость обеспечения соответствия экспертов предъявляемым требованиям и особенности формирования экспертной группы становится очевидным, что обеспечить необходимую периодичность такой оценки на практике весьма проблематично.

И, наконец, такой подход к оцениванию предполагаемых параметров модели не дает представление о структуре самой модели процесса управления информационной безопасностью, а переход от последовательности вербальных моделей, описанных в рассмотренных нормативных документах, к формальной модели, в том числе и из-за недостатка информации, существенно затруднен или невозможен.

Отдельные попытки формализовать модели носят частный, специфический характер и не выходят за рамки аналитических или статистических представлений.

Например, известны формальные модели в области кибербезопасности (уязвимости программного обеспечения), основанные на применении весовых коэффициентов к различным показателям [4]. Однако назначение таких коэффициентов, как правило, носит непрозрачный и необоснованный характер. На рисунке 1 представлен фрагмент формальной аналитической модели – определение текущего количества уязвимостей кибербезопасности в ИТ инфраструктуре. Модель была представлена как Доклад на II школе-семинаре «Современные тенденции развития методов и технологий защиты информации» в МТУСИ в октябре 2022 года. Попытка применить аналитические методы моделирования привела к «выявлению» более 1 млн. уязвимостей, что в принципе, ставит под сомнение эффективное управление информационной безопасностью [5].

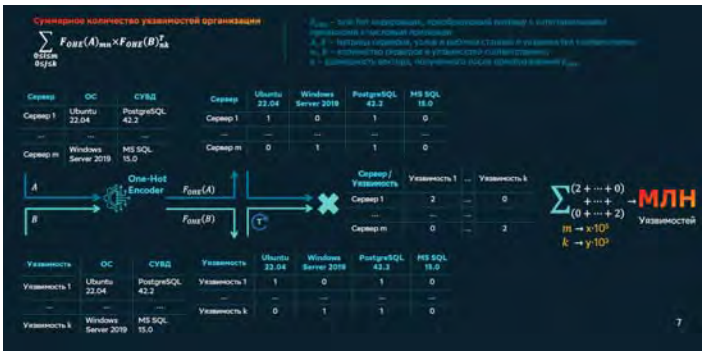

Рис. 1. Определение текущего количества уязвимостей кибербезопасности в ИТ инфраструктуре

При этом аналитические методы предполагают искусственное игнорирование неопределенности. Применение статистических методов ограничено с одной стороны невозможностью достоверной оценки вероятностных характеристик переменных модели, а с другой стороны с существенными сложностями доказательства репрезентативности используемых выборок.

Модель процесса управления ИБ

Поиск альтернативных методов моделирования процессов управления ИБ необходимо начать с классификации объекта моделирования.

Объектом моделирования в данном случае является процесс управления информационной безопасностью, который может быть рассмотрен как система, представленная на рисунке 2.

В качестве выходной переменной модели может быть рассмотрен обобщенный показатель эффективности **P**, который характеризует уровень защищенности информации в системе. Рассматривая информацию как совокупность базовых свойств информации как объекта защиты, введенный коэффициент может быть представлен в виде:

$$P = F(P_c, P_i, P_a), P = [0..1] \quad (1)$$

где P_c – показатель защищенности конфиденциальности информации в системе; P_i – показатель защищенности целостности информации в системе; P_a – показатель защищенности доступности информации в системе.

Учитывая, где к свойствам информации как объекта защиты отнесены также и свойства «неотказуемости, подотчетности, аутентичности и достоверности», обобщенный показатель защищенности информации в системе примет вид

$$P = F(x_1, x_2, ...x_i, ..x_n) \quad (2)$$

где x_i – показатель защищенности *i*-го свойства информации как объекта защиты; *n* – количество свойств информации.

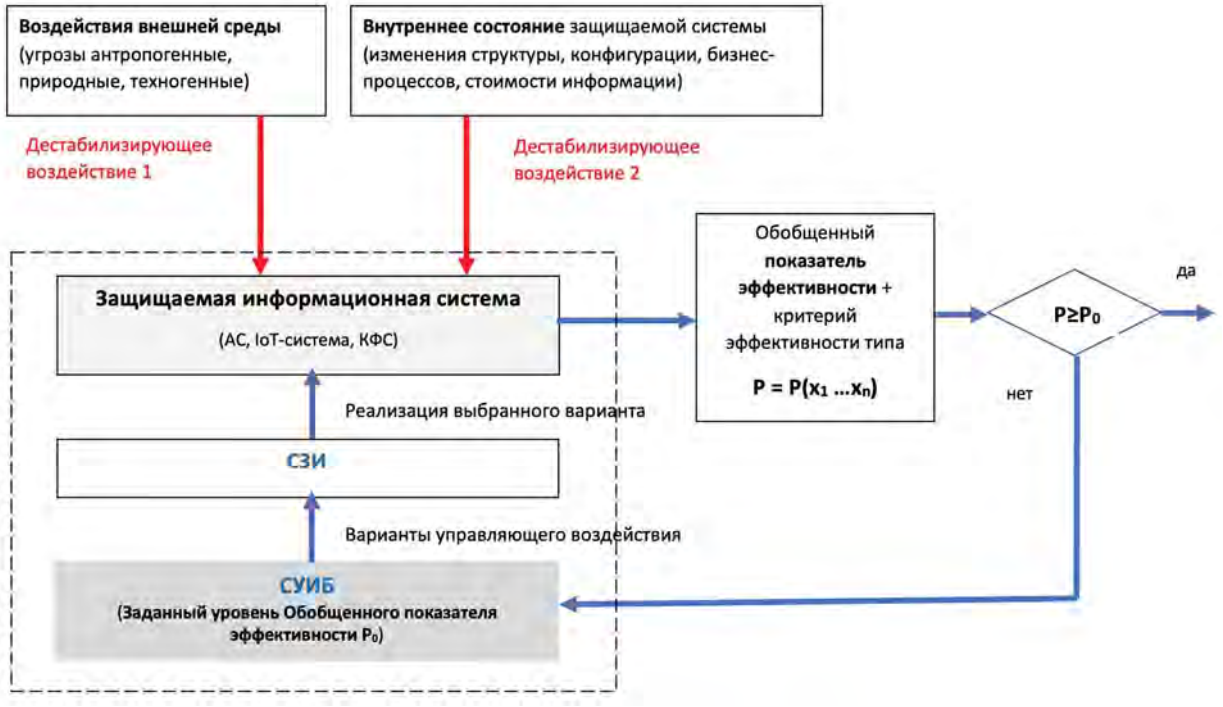

Рис. 2. Обобщенная структура процесса управления информационной безопасностью

На первый взгляд, структура системы определена и взаимосвязи между элементами системы также могут быть описаны (хотя бы вербально). Вместе с тем каждый элемент системы (рис. 2) может быть рассмотрен как подсистема с большой неустранимой неопределенностью.

Основные причины неопределенности моделируемого объекта.

1. Неизвестен полный перечень угроз, действующих на защищаемую систему. Для анализа и учета актуальных угроз возможно использование так называемых нормативных угроз, упоминаемых в различных нормативных документах. Например, угроза несанкционированного доступа или угроза утечки информации по техническим каналам. Однако формулировка угроз в нормативных документах чаще всего требует конкретизации применительно к конкретному защищаемому объекту (информационной системе). Кроме того, при формировании перечня угроз рекомендуется использование Банка данных угроз безопасности информации ФСТЭК России. Содержащиеся там вербальные формулировки угроз и их описания достаточно конкретны, однако они имеют отношение только к области кибербезопасности и криптографической защите, что не охватывает все возможные угрозы. Значительную долю неопределенности вносят так называемые случайные угрозы - такие угрозы, которые могут или случиться, или не случиться. К таким угрозам относятся угрозы хакеров дестабилизировать информационные системы субъектов из хулиганских побуждений, случайные непредсказуемые действия пользователей и т.д.

2. Состояние технической исправности программно-аппаратных средств подсистемы технической защиты информации в конкретный момент времени, полнота реализации функций защиты подсистемами СЗИ, а также состояние выполнения всех организационных мер, действующих в защищаемой системе и проч.

Кроме того, необходимо учитывать, что сама структура защищаемой системы может изменяться при изменении основных целей ее функционирования (изменение или появление новых бизнес-целей), может так же изменяться и структура СЗИ для осуществления управляющих воздействий.

Таким образом, по классификации систем В.В.Налимова [6], которая предполагает разделение по степени организованности на

- хорошо организованные системы;
- плохо организованные (или диффузные) системы;
- самоорганизующиеся или развивающиеся системы.

Систему управления информационной безопасностью можно отнести к последнему классу.

Такие системы характеризуются

- неоднозначность использования понятий;
- нестационарность (изменчивость, нестабильность) параметров;
- стохастичность поведения;
- уникальность и непредсказуемость поведения системы в конкретных условиях.

Одним из возможных методов моделирования подобных объектов может быть рассмотрен метод с применением нечетких алгоритмов.

Нечеткая логика для моделирования системы управления информационной безопасностью

В основе нечеткого моделирования лежит концепция нечетких множеств (НМ), введенная в середине 1960-х гг. Лотфи Заде. Решающую роль в становлении концепции НМ как основы для альтернативных методов моделирования стало появление устройств, основанных на использовании нечеткой логики, применявшихся для решения задач управления поездами метрополитена, подъемными кранами, лифтами и т. д.

Основы метода заложили такие исследователи, как Мамдани, Сугено, Такаги и др.

Задачи нечеткого управления в настоящее время играют роль эталонных тестовых проблем для нечетких множеств, а многими эти задачи и вообще воспринимаются как синоним приложений нечетких множеств [7]. Вместе с тем, потенциальные возможности моделирования на основе нечетких алгоритмов значительно превосходят построение алгоритмов управления техническими устройствами или системами.

Определим структуру нечеткой модели управления информационной безопасностью. Выходной переменной модели является уровень защищенности информации в защищаемой системе. Исходя из структуры моделируемого объекта, выходная переменная будет зависеть от уровня дестабилизирующих факторов и состояния системы защиты информации.

Уровень дестабилизирующих факторов определяется из совокупности двух переменных:

- дестабилизирующие воздействия 1 (угрозы информационной безопасности);
- дестабилизирующие воздействия 2 (главным образом это изменения структуры защищаемой системы и изменения характера информационного процесса.

Что касается дестабилизирующих воздействий 2, то в данном примере будем считать, что такие воздействия отсутствуют и защищаемая система находится в стабильном состоянии.

Что касается угроз информационной безопасности, то уровень воздействия угроз определяется наличием уязвимостей в системе [8], [9], поэтому данный фактор будем определять через «Уровень уязвимости защищаемой информационной системы». Эта переменная модели является комплексной и должна учитывать все пары «элементарная угроза-уязвимость».

Другим действующим фактором модели определим «Состояние СЗИ». Эта переменная также является комплексной и должна учитывать:

1) полноту реализации функций защиты информации всех применяемых способов и методов защиты в системе (например, надежность идентификации и аутентификации пользователей, реализацию мер разграничения доступа, класс межсетевого экрана, достаточность мер физической защиты и т.д.);

2) техническую исправность всех защитных механизмов, поддержка правильных параметров настройки программно-аппаратных средств и т.д.

Таким образом, структура нечеткой модели управления информационной безопасностью в данном контексте может быть сведена к модели с двумя входами и одном выходом (рис.3).

Реализация модели нечеткой логики выполнена в среде инженерных вычислений MATLAB [10] с инструментами Fuzzy Logic Toolbox [11].

В качестве оператора модели применим нечеткий вывод на правилах Мамдани.

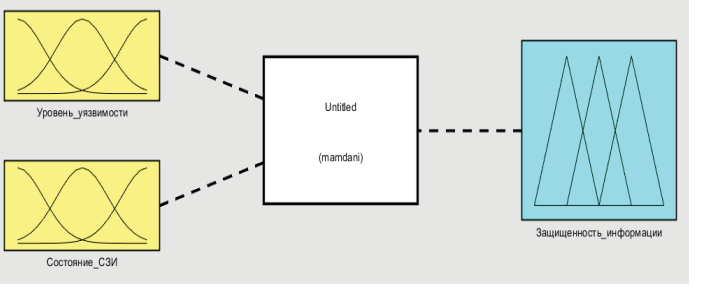

Рис. 3. Возможная структура нечеткой модели процесса управления информационной безопасностью в информационной системе

Выходные переменные модели представлены в виде лингвистических переменных с 4 нечеткими множествами на непрерывной области определения [0 …1] (рис. 4 и 5). При отсутствии информации об особенностях конкретной информационной системы область определения разбита на термы равномерно [12].

Лингвистическое терм-множество переменной «Уровень уязвимости защищаемой информационной системы» A_L = {низкий, средний, высокий, критический}.

Лингвистическое терм-множество переменной «Состояние системы защиты информации (СЗИ)» B_L = {слабый, средний, сильный, высший}.

В качестве функции принадлежности нечетким множествам использована функция pimf, как одна из функций, позволяющий получить более сглаженный отклик на выходе модели: функция вычисляет нечеткие значения членства с помощью основанной на сплайне функции принадлежности, имеющей пи-образную форму (*y = pimf (x,params)* возвращает вычисленное использование значений нечеткого членства основанной на сплайне функции принадлежности).

$$f(x,a,b,c,d)=\begin{cases} 0, x \le a \\ 2*(\frac{x-a}{b-a})^2, a \le x \le \frac{a+b}{2} \\ 1-2*(\frac{x-b}{b-a})^2, \frac{a+b}{2} \le x \le b \\ 1, b \le x \le c \\ 1-2*(\frac{x-c}{d-c})^2, c \le x \le \frac{c+d}{2} \\ 2*(\frac{x-d}{d-c})^2, \frac{c+d}{2} \le x \le d \\ 0, x \ge d \end{cases} \quad (3)$$

Задать a, b, c и параметры d возможно с помощью params пакета fuzzy в MatLab.

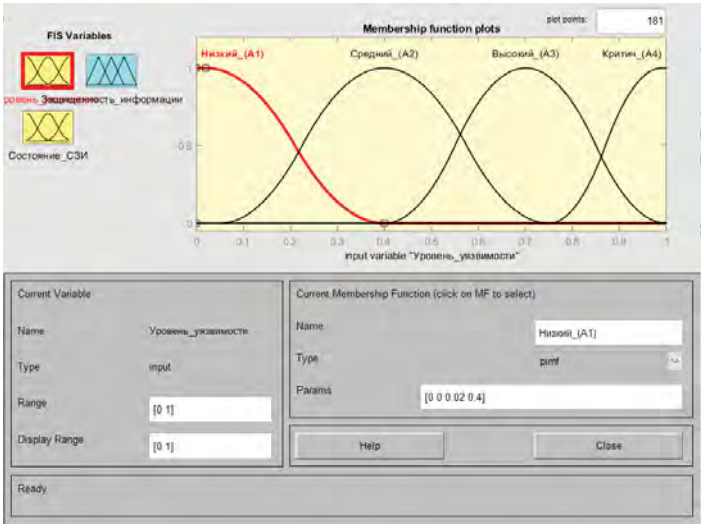

Рис. 4. Представление входной переменной **A** «Уровень уязвимости защищаемой информационной системы» в виде лингвистической переменной средствами MatLab Fuzzy

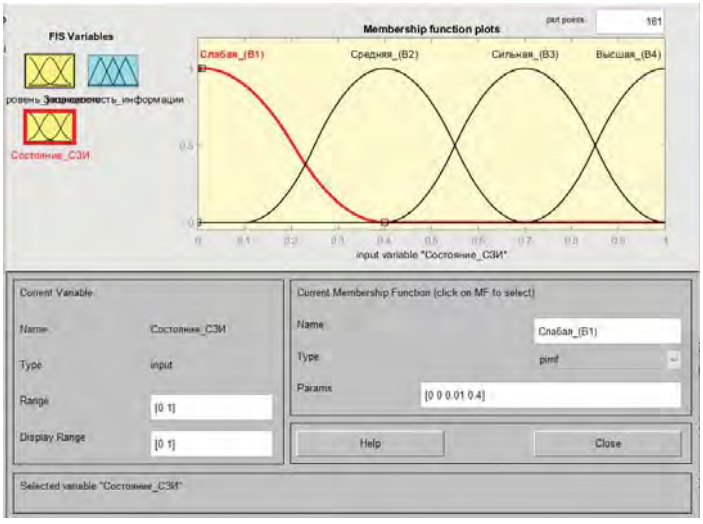

Рис. 5. Представление входной переменной **B** «Состояние СЗИ» в виде лингвистической переменной средствами MatLab Fuzzy

Выходная переменная «Состояние защищенности информации в системе» так же представлена с помощью четырех нечетких множеств на непрерывной области определения [0 …1] с помощью кусочно-линейной функции принадлежности (trimf) [13] (рис. 6.). Эта функция вычисляет нечеткие значения членства с помощью треугольной функции принадлежности (*y = trimf(x,params*) возвращает вычисленное использование значений нечеткого членства следующей треугольной функции принадлежности:

$$f(x,a,b,c,d) = \max(\min(\frac{x-a}{b-a}, \frac{c-x}{c-b}, 0)) \quad (4)$$

Чтобы задать параметры, a, b и c, используют *params*.

Лингвистическое терм-множество выходной переменной «Состояние защищенности информации в системе» CL = {критическая, слабая, средняя, высшая}.

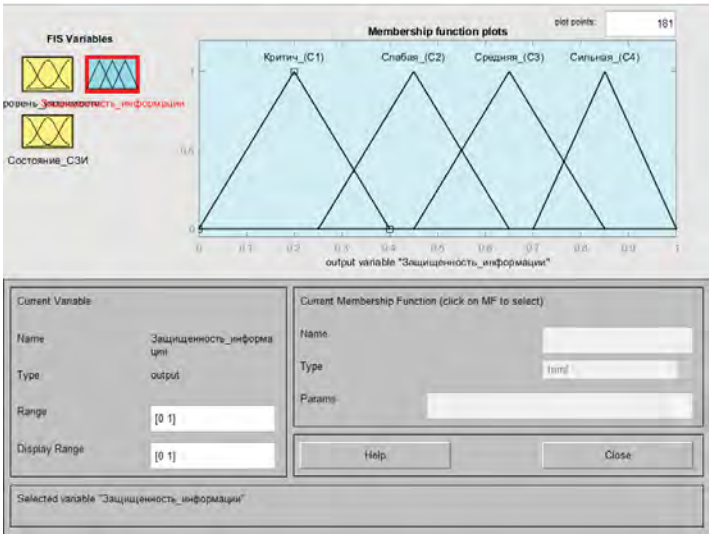

Рис. 6. Представление выходной переменной модели в виде лингвистической переменной «Состояние защищенности информации в системе» средствами MatLab Fuzzy

База правил нечеткой модели Мамдани представлена в таблице 1 и содержит 16 правил. Каждое правило в базе содержит условие и заключение и имеет вид:

R_1: ЕСЛИ (A = A_1) И (B = B_1) ТО (C = C_2)

R_{16}: ЕСЛИ (A = A_4) И (B = B_4) ТО (C = C_3)

Таблица 1

База правил нечеткой модели

Уровень уязвимости (**A**) / Состояние СЗИ (**B**)	A1 (низкий)	A2 (средний)	A3 (высокий)	A4 (критич)
B1 (слабая)	C2	C2	C1	C1
B2 (средняя)	C3	C2	C2	C1
B3 (сильная)	C4	C3	C3	C2
B4 (высшая)	C4	C4	C3	C3

Параметры модели представлены на рисунке 7.

Рис. 7. Параметры нечеткой модели управления информационной безопасностью

Вид трехмерной поверхности решения модели для заданной структуры представлен на рисунке 8.

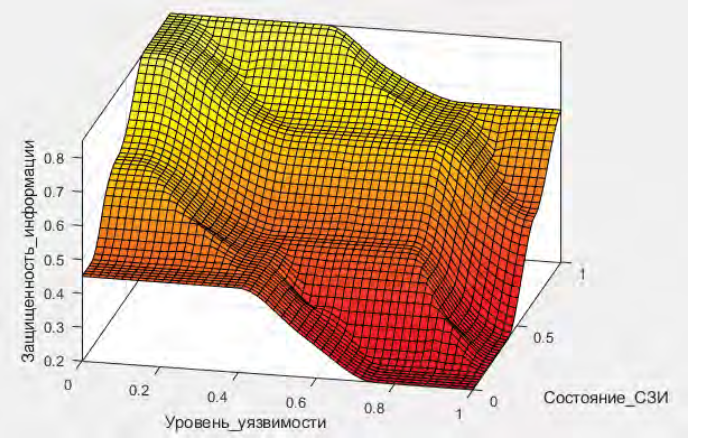

Рис. 8. Графическая интерпретация поверхности нечеткой модели

В результате анализа полученного результата возможны следующие утверждения:

- применение нечетких методов моделирования (алгоритм Мамдани) позволяет получить неразрывную и чувствительную поверхность модели управления информационной безопасностью (изменение любой входной переменной в области определения приводит к изменению значения выходной переменной);
- наличие гибких инструментов настройки нечеткой модели (как грубой – с изменением структуры модели, так и тонкой) позволит добиваться заданной точности;
- полученная нечеткая модель качественно адекватна моделируемому процессу управления информационной безопасностью информационной системы;
- применение на практике полученной модели позволяет оперативно отслеживать изменения показателя защищенности информации в системе при любых изменениях входных переменных. Эти изменения выражаются численно.

Заключение

Показана возможность построения модели системы управления информационной безопасности методами нечеткого моделирования. Модель позволяет вводить численную метрику.

Полученный прототип модели имеет дескриптивный характер. На базе этой модели может быть построена оптимизационная модель с введением критерия оптимизации. В настоящей статье вопросы оптимизации не рассматривались.

Не рассмотрены также численные оценки входных переменных модели, однако продемонстрированный метод моделирования показывает, что такая оценка возможна в полученной метрике посредством создания последовательности нескольких двухвходовых нечетких моделей.

Сказанное выше открывает возможности построения автоматизированной и даже автоматической системы управления информационной безопасностью информационной системы. Основной проблемой здесь может быть мониторинг уровня угроз, действующих на систему. Одним из методов решения такой проблемы может быть организация нескольких разнородных каналов получения информации о возможных угрозах. Таким каналом может стать постоянный анализ неструктурированной текстовой информации, содержащейся в открытых периодических источниках, например новостные ленты информационных агентств. Для формализации такой информации могут быть использованы методы векторного анализа слов в тексте [14], [15].

Литература

1. *Saleem K. et al*. An intelligent information security mechanism for the network layer of WSN: BIOSARP //Computational intelligence in security for information systems. Springer, Berlin, Heidelberg, 2011. С. 118-126.
2. *Chuiko G. P., Dvornyk O. V., Yaremchuk O. M*. Mathematical Modeling of Systems and Processes // Publ. House of Petro Mohyla Black Sea State University, Mykolaiv. 2015.
3. *Bogdanov Yu. M., Ogarok A. L., Selivanov S. A.* Monitoring of cybersecurity of complex information and control systems of critical infrastructure // Informatization and communications. 2021. No. 1, pp. 142-150.
4. Spring J., Hatleback E., Householder A., Manion A., Shick D. Time to Change the CVSS? // IEEE Security & Privacy, vol. 19, no. 2, pp. 74-78, March-April 2021, doi: 10.1109/MSEC.2020.3044475
5. *Пегат А*. Нечеткое моделирование и управление. Пер. с англ. 2-е изд. М.: БИНОМ. Лаборатория знаний, 2017. 798 с. (Адаптивные и интеллектуальные системы). ISBN 978-5-9963-1495-9.
6. *Влэдуц Г. Э., Налимов В. В., Стяжкин Н. И*. Научная и техническая информация как одна из задач кибернетики // Успехи физических наук. 1959. Т. 69. №. 9. С. 13-56.
7. *Гродзенский Я.С*. Информационная безопасность: учебное пособие. М.: РГ-Пресс, 2020. ISBN 978-5-9988-0845-6
8. *Зима В. М., Крюков Р. О., Кравчук А. В*. Методика оценивания информационных рисков на основе анализа уязвимостей // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. №. 11-12. С. 36-46.
9. *Дроботун Е. Б., Цветков О. В*. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя //Программные продукты и системы. 2016. №. 3 (115). С. 42-50.
10. *Kaur E. K., Mutenja V., Gill I. S.* Fuzzy logic based image edge detection algorithm in MATLAB // International Journal of Computer Applications. 2010. Т. 1. №. 22. С. 55-58.
11. *Sivanandam S. N.* et al. Introduction to fuzzy logic using MATLAB. Berlin: Springer, 2007. Т. 1.
12. *Hrehova S., Mizakova J.* Evaluation a process using fuzzy principles and tools of Matlab // International Journal of Applied Mathematics, Computational Science and Systems Engineering. 2019. Т. 1.
13. *Daniel-Petru G. et al.* Analysis of sustainable development using fuzzy logic prediction models and artifical neural networks // Management Strategies Journal. 2016. Т. 31. №. 1. С. 204-218.
14. *Ларин А. И., Вовик А. Г., Тряпицын А. Д*. Формализация неструктурированной текстовой информации на основе векторного представления слов // Инновационное развитие: потенциал науки и современного образования. 2021. С. 212-223.
15. *Triapitsyn A. D., Larin A. I.* Designing of a Classifier for the Unstructured Text Formalization Model Based on Word Embedding // 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH), 2020, pp. 1-5, doi: 10.1109/EMCTECH49634.2020.9261546

EXPLORING POSSIBILITY OF USING NUMERICAL METRICS IN INFORMATION SECURITY MANAGEMENT

ANDREY G. VOVIK
Moscow, Russia, a.g.vovik@mtuci.ru

ALEXANDER I. LARIN
Moscow, Russia, a.i.larin@mtuci.ru

KEYWORDS: *information security management, numerical metrics, fuzzy logic, mamdani's algorithm.*

ABSTRACT

Introduction. The existing information security management in information systems is a set of informal verbal models. They make it possible to determine a variety of measures but cannot conduct numerical assessments – to compare alternative strategies according to the introduced criterion, to numerically record changes in the level of information security, to perform mathematically justified optimization of control actions. **Purpose:** The purpose of the study is to substantiate the possibility of using numerical estimates in information security management. **Methods:** The search for alternative methods of modeling information security management processes begins with the modeling object classification. The modeling object (the information security management process) is considered as a complex system having irremediable uncertainty. A method using fuzzy algorithms can be classified as one of the possible methods in modeling such objects. Fuzzy algorithms are most widely used when modeling technical control systems, but this method potential allows us to hope for positive results when modeling more complex processes. The article offers an example of using fuzzy modeling algorithms based on Mamdani rules of inference algorithms for creating an information security management system model of an information system. **Results:** The sensitivity, continuity and qualitative adequacy of the described model are substantiated, the possibility of operational tracking of the influence of destabilizing influences on the level of information security in the information system using a numerical metric is shown. **Practical relevance:** The use of the proposed methods opens up the possibility of building an automatic information security management system of an information system.

REFERENCES

1. K. Saleem et al. (2011). An intelligent information security mechanism for the network layer of WSN: BIOSARP. *Computational intelligence in security for information systems*. Springer, Berlin, Heidelberg, pp. 118-126.

2. G.P. Chuiko, O.V. Dvornyk, O.M. Yaremchuk (2015). Mathematical Modeling of Systems and Processes. Publ. House of Petro Mohyla Black Sea State University, Mykolaiv.

3. Yu.M. Bogdanov, A.L. Ogarok, S.A. Selivanov (2021). Monitoring of cybersecurity of complex information and control systems of critical infrastructure. *Informatization and communications*. No. 1, pp. 142-150.

4. J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick (2021). Time to Change the CVSS? *IEEE Security & Privacy*, vol. 19, no. 2, pp. 74-78, March-April 2021, doi: 10.1109/MSEC.2020.3044475.

5. A. Pegat (2012). Nechetkoe modelirovanie i upravlenie (Fuzzy Simulation and Control), Moscow: BINOM. Laboratoriya Znanii. (In Rus)

6. G.Je.Vljeduc, V.V. Nalimov, N.I. Stjazhkin (1959). Nauchnaja i tehnicheskaja informacija kak odna iz zadach kibernetiki. *Uspehi fizicheskih nauk*. Vol. 69. No. 9, pp. 13-56.

7. Ja.S. Grodzenskij (2020). Informacionnaja bezopasnost': uchebnoe posobie. Moscow: RG-Press. ISBN 978-5-9988-0845-6 (In Rus)

8. V.M. Zima, R.O. Krjukov, A.V. Kravchuk (2019). Methodology for information risk assessment based on analysis of vulnerabilities. Voprosy oboronnoj tehniki. Series 16: Tehnicheskie sredstva protivodejstvija terrorizmu. No. 11-12, pp. 36-46. (In Rus)

9. E.B. Drobotun, O.V. Tsvetkov (2016). Modeling Information Security Threats in the Automated Control System for Crucial Objects on the Basis of Attack Scenarios. *Software & Systems*. No. 3, pp. 42-50. DOI:10.15827/0236-235X.115.042-050 (in Rus.)

10. E.K. Kaur , V. Mutenja, S.I. Gill (2010). Fuzzy logic based image edge detection algorithm in MATLAB. *International Journal of Computer Applications*. Vol. 1. No. 22, pp. 55-58.

11. S.N.Sivanandam et al. (2007). Introduction to fuzzy logic using MATLAB. Berlin: Springer. Vol. 1.

12. S. Hrehova, J. Mizakova (2019). Evaluation a process using fuzzy principles and tools of Matlab. *International Journal of Applied Mathematics, Computational Science and Systems Engineering*. Vol. 1.

13. G. Daniel-Petru et al. (2016). Analysis of sustainable development using fuzzy logic prediction models and artifical neural networks. *Management Strategies Journal*. Vol. 31. No. 1, pp. 204-218.

14. A.I. Larin, A.G. Vovik, A.D. Trjapicyn (2021). Formalization of unstructured text information based on vector representation of words. *Innovacionnoe razvitie: potencial nauki i sovremennogo obrazovanija*, pp. 212-223.

15. A.D. Triapitsyn and A.I. Larin (2020). Designing of a Classifier for the Unstructured Text Formalization Model Based on Word Embedding. *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, pp. 1-5, doi: 10.1109/EMCTECH49634.2020.9261546.

INFORMATION ABOUT AUTHORS:

Andrey G. Vovik, Lecturer at the Department ISUiA, Moscow Technical University of Communications and Informatics, Moscow, Russia

Alexander I. Larin, PhD, Associate Professor at the Department ISUiA, Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Vovik A.G, Burlov V.G., Larin A.I. Exploring possibility of using numerical metrics in information security management. H&ES Reserch. 2022. Vol. 14. No. 6. P. 12-19. doi: 10.36724/2409-5419-2022-14-6-12-19 (In Rus)

doi: 10.36724/2409-5419-2022-14-6-20-26

МАРКИРОВКА НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНОГО ГАУССОВСКОГО ШУМА И ДВУМЕРНОГО ДИСКРЕТНОГО ВЕЙВЛЕТ ПРЕОБРАЗОВАНИЯ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ

МАГОМЕДОВА
Дженнет Исламутдиновна[1]

АННОТАЦИЯ

Введение. актуальность защиты авторских прав на мультимедиа контент определяется повсеместностью использования цифровых объектов во всех областях жизни. Непрерывно растет число и квалификация злоумышленников, нацеленных на использование чужого интеллектуального труда. Проблема защиты авторских прав может быть решена путем использования методов стеганографии. Несмотря на широкую разработанность темы, есть ряд проблем, ограничивающих возможности использования классических методов стеганографии. Устойчивость многих известных методов к несанкционированному доступу основывается на знании алгоритма без использования дополнительных ключей. Это делает методы уязвимыми к модификации и удалению встроенной метки нарушителем. **Целью исследования** является повышение устойчивости алгоритмов защиты авторских прав от несанкционированного доступа. Предлагается встраивать водяные знаки в два этапа: на первом этапе значения цифрового водяного знака заменяются последовательностями фрактального гауссовского шума, затем полученный фрактальный ключ встраивается в защищаемое изображение путем замены коэффициентов вейвлет разложения. **Методы:** для генерации фрактального гауссовского шума использовался алгоритм быстрого преобразования Фурье. Показатель Хёрста шумовых последовательностей оценивался с помощью R/S анализа. **Результаты:** предложен новый алгоритм встраивания цифровых водяных знаков в изображения на основе фрактального гауссовского шума и дискретного вейвлет преобразования. Определены значения рациональных параметров алгоритма таких, как уровень разложения, масштабирующий коэффициент, длина шумовой последовательности, значения показателя Хёрста для единичной последовательности и пороговое значение, позволяющие достичь наилучшего баланса между качеством встраивания и извлечения.

Сведения об авторе:

[1] старший преподаватель кафедры "Информационная безопасность" Московского Технического университета связи и информатики, Москва, Россия, d.i.magomedova@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: *защита авторских прав, дискретное вейвлет преобразование, фрактальный гауссовский шум, стеганография, показатель Хёрста.*

Для цитирования: Магомедова Д.И. Маркировка неподвижных изображений с использованием фрактального гауссовского шума и двумерного дискретного вейвлет преобразования для защиты авторских прав // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 20-26. doi: 10.36724/2409-5419-2022-14-6-20-26

Введение

Одним из направлений цифровой стеганографии является защита авторских прав на мультимедиа контент. Добавление невидимых для человека меток – цифровых водяных знаков (ЦВЗ) – позволяет сохранить качество оригинального объекта и в тоже время способствовать защите интеллектуальной собственности от неправомерного использования.

Классические алгоритмы цифровой стеганографии обладают низкой устойчивостью к несанкционированному доступу, поскольку для доступа к встроенному ЦВЗ в большинстве случаев необходимо только знание алгоритмов [1-2]. Для решения этой проблемы активно разрабатываются алгоритмы, требующие наличия дополнительных ключей.

Фрактальная геометрия может быть использована для встраивания больших объемов информации в одномерные (звуковые сигналы) или двумерные (изображения) контейнеры, не влияя на их качество и сделать скрытую информацию устойчивой и достаточно эффективной к несанкционированному доступу.

Фрактальная геометрия широко используется при разработке новых стеганографических методов встраивания информации [3-7]. Но существующие методы не могут быть использованы для решения задачи защиты авторских прав.

Основная часть алгоритмов встраивания цифровых водяных знаков (ЦВЗ) позволяет использовать только фрактальные контейнеры, что ограничивает их область применения только задачами скрытой передачи данных [8-10].

Целью статьи является исследование и разработка алгоритма встраивания ЦВЗ в виде псевдослучайной последовательности с использованием фрактального гауссовского шума для защиты авторских прав.

Алгоритм встраивания водяных знаков в изображения с использованием фрактального гауссовского шума и 2D ДВП

Алгоритм встраивания состоит из следующих шагов:

Шаг 1. Генерация цифрового водяного знака в виде псевдослучайной последовательности (ПСП).

Шаг 2. Вычисление матрицы яркости Y(x,y) из оригинального контейнера S(x,y) путем перехода из пространства RGB в YCbCr.

Шаг 3. Дискретное вейвлет преобразование матрицы яркости, вычисление коэффициентов вейвлет разложения $W_\varphi(j_0,m,n)$ и $W_\psi^i(j,m,n)(i=H,V,D)$ по формулам (1-2). Использование данного вида преобразования в процессе встраивания обусловлено высокими результатами, полученными при разработке алгоритмов стеганографии с использованием вейвлетов [11-14].

$$W_\varphi(j_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}Y(x,y)\varphi_{j_0,m,n}(x,y), \qquad (1)$$

$$W_\psi^i(j,m,n)=\frac{1}{\sqrt{M_jN_j}}\sum_{x=0}^{M_j}\sum_{y=0}^{M_j}Y(x,y)\psi_{j.m,n}^j(x,y), \qquad i=H,V,D. \qquad (2)$$

Шаг 4. Генерация фрактального гауссовского шума (ФГШ) $X^H(j)$. Производится генерация двух последовательностей ФГШ с заданным значением показателя Хёрста H_0 и H_1, которые соответствуют битам ПСП. Для встраивания «0» генерируется ФГШ с фрактальной размерностью, характеризуемым показателем Хёрста H_0, для встраивания «1» - ФГШ с показателем Хёрста H_1.

Шаг 5. Формирование новой матрицы диагональных коэффициентов путем замены элементов матрицы $Y(x,y)$ последовательностью ФГШ $X^H(j)$ по формуле (3). Каждая последовательность ФГШ полностью заполняет одну строку матрицы. Для сохранения встроенных значений в процессе обратного преобразования шумовые последовательности умножаются на коэффициент α.

Размеры контейнера и длина ПСП подбираются таким образом, чтобы новая матрица полностью совпадала по размерам с матрицей коэффициентов вейвлет разложения.

$$W_\psi^{i=D}(j=2,m_2,n_2)= =\frac{1}{M_2N_2}\alpha\sum_{x=0}^{M_2}\sum_{y=0}^{N_2}X^H_{j,m_2,n_2}(x,y)\psi^D_{j,m_2,n_2}(x,y). \qquad (3)$$

Шаг 6. Вычисление новой матрицы яркости Y*(x,y) путем обратного вейвлет преобразования с использованием фрактального контейнера $F_{j,m,n}(x,y)$ по формуле (4):

$$\begin{aligned}Y^*(x,y)=&\frac{1}{\sqrt{MN}}\sum_m^M\sum_n^N W_\varphi(j_0,m,n)\varphi_{j_0,m,n}+\\&+\sum_{i=H,V,D}\sum_{j_0}[\sum_{m_1}^{M_1}\sum_{n_1}^{N_1}W_\psi^i(j=1,m_1,n_1)\psi^i_{j=1,m_1,n_1}(x,y)+\\&+\sum_{m_2}^{M_2}\sum_{n_2}^{N_2}W_\psi^i(j=2,m_2,n_2)\psi^i_{j=2,m_2,n_2}(x,y)+\\&+\sum_{m_3}^{M_3}\sum_{n_3}^{N_3}W_\psi^i(j=3,m_3,n_3)\psi^i_{j=3,m_3,n_3}(x,y)].\end{aligned} \qquad (4)$$

Шаг 7. Получение стегоконтейнера S*(x,y) путем вычисления цветовых компонент на основе измененной матрицы яркости Y*(x,y).

Алгоритм извлечения

Алгоритм извлечения состоит из следующих шагов:

Шаг 1. Вычисление матрицы яркости $Y^*(x,y)$ из стегоконтейнера $S^*(x,y)$ путем перехода из пространства RGB в YCbCr.

Шаг 2. Дискретное вейвлет преобразование матрицы яркости, вычисление коэффициентов вейвлет разложения $W_\varphi(j_0,m,n)$ и $W_\psi^i(j,m,n)(i=H,V,D)$.

Шаг 3. Выделение последовательностей ФГШ из матрицы коэффициентов вейвлет разложения.

Шаг 4. Оценка показателя Хёрста полученных сегментов $\hat{H}(p)$.

Шаг 5. Сравнение оценок показателя Хёрста $\hat{H}(p)$ с пороговым значением $H_{пор}$ и извлечение элементов ПСП ПСП*(p) согласно формуле (5):

$$ПСП^*(p) = \begin{cases} 1, \text{если } \widehat{H}(p) \geq H_{пор} \\ 0, \text{если } \widehat{H}(p) < H_{пор} \end{cases} \quad (5)$$

Шаг 6. Генерация «опорной» ПСП $\widehat{ПСП}$ (p).

Шаг 7. Вычисление корреляции «опорной» и извлеченной ПСП по формуле (6) для последующей оценки достоверности извлечения и сравнение с порогом.

$$B_{ПСП}(i) = \frac{1}{P}\sum_{p=1}^{P} ПСП_p^* \widehat{ПСП}_{p+i} \quad (6)$$

Выбор параметров алгоритма

Для определения параметров контейнера, позволяющих достичь баланса между качеством встраивания и качеством извлечения были исследованы такие параметры алгоритма, как уровень вейвлет-разложения, значение масштабирующего коэффициента alpha, длина последовательности ФГШ, значение показателя Хёрста единичной последовательности, пороговое значение.

При проведении экспериментов было использовано 20000 изображений из двух баз изображений, используемых для тестирования алгоритмов стеганографии [15, 16].

Качество встраивания оценивалось с использованием усредненного по всем экспериментам значения пикового соотношения сигнал/шум PSNR [17]. В качестве порога было установлено значение 40 дБ.

Для оценки качества извлечения вычислялось усредненное значение корреляции $B_{ПСП}$(i=0) [18]. Порог качества извлечения был задан как $B_{ПСП}(i=0) \geq 0.95$.

Рассматривалось 4 типа вейвлетов: Хаар, Добеши 4, Симлет 4 и Койфлет 4.

Уровень вейвлет-разложения влияет на максимально возможный объем встраивания: при увеличении уровня происходит уменьшение числа доступных для замены коэффициентов. С другой стороны, замена коэффициентов на первых уровнях может привести к искажению контейнера. Зависимости качества встраивания и извлечения от уровня вейвлет-разложения показаны на рисунках 1-2.

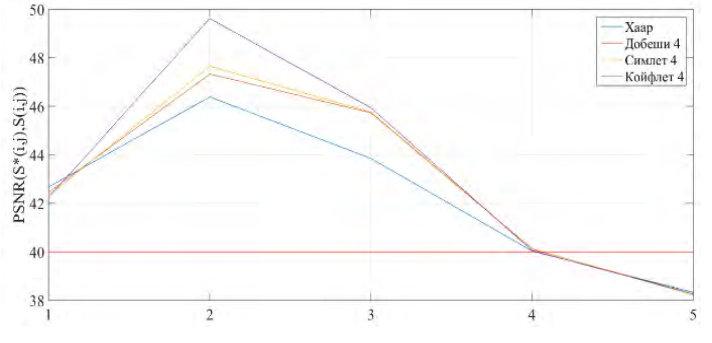

Рис. 1. Зависимость PSNR стегоконтейнера от уровня вейвлет-разложения

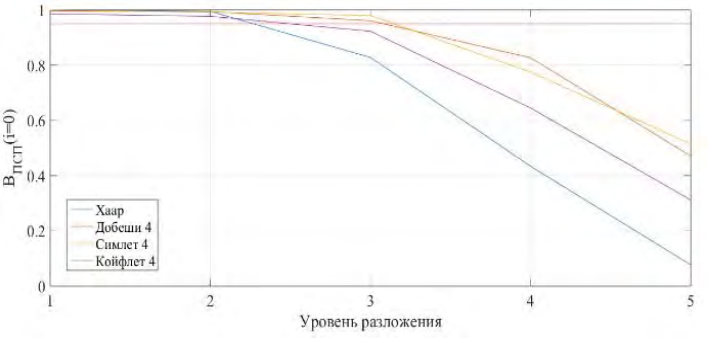

Рис. 2. Зависимость $B_{ПСП}$ (i=0) от уровня вейвлет-разложения

Полученные результаты иллюстрируют, что наилучшие результаты при встраивании и извлечении достигаются при встраивании в 1 и 2 уровни вейвлет разложения.

Значение масштабирующего коэффициента α выбирается исходя из требований незаметности встраивания ЦВЗ в изображение. Правильно подобранная величина α позволяет уменьшить влияние добавляемого ФГШ на качество стегоконтейнера и избежать изменений, заметных для глаза человека. При этом стоит учитывать, что слишком маленькое значение масштабирующего коэффициента может привести к искажению встроенной шумовой последовательности при вейвлет реконструкции маркированного изображения, что способствует недостоверному извлечению на приемной стороне.

На рисунке 3 представлена зависимость пикового соотношения сигнал/шум PSNR стегоконтейнера от значения параметра alpha.

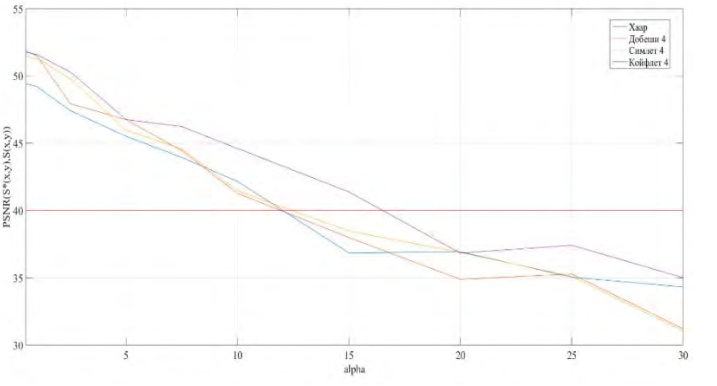

Рис. 3. Зависимость PSNR стегоконтейнера от параметра alpha

При анализе полученных зависимостей можно отметить, что допустимый уровень PSNR≥40 дБ достигается при alpha≤12.5 для всех вейвлетов Хаара, Добеши 4 и Симлет 4. Для вейвлета Койфлет 4 значение PSNR=40 дБ достигается при alpha>15. Наибольшие искажения в контейнере появляются при использовании вейвлета Хаара, наименьшие – при использовании вейвлета Койфлет 4.

На рисунке 4 представлена зависимость $B_{ПСП}$ (i=0) от значения alpha.

Для достижения баланса между качеством встраивания и извлечения рекомендуется использовать alpha ∈ [2.5;12.5].

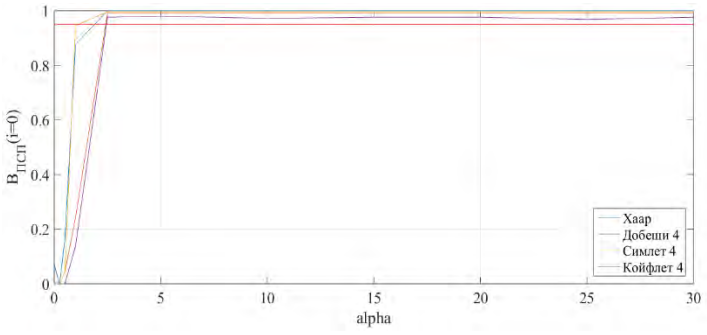

Рис. 4. Зависимость $B_{ПСП}(i=0)$ от параметра alpha

Длина последовательности ФГШ влияет на максимально допустимый размер ПСП: чем выше длина фрактальной последовательности, тем меньше значений ПСП можно встроить. Но недостаточно длинная шумовая последовательность может привести к ошибкам при извлечении.

На рисунке 5 представлена зависимость PSNR стегоконтейнера от длины последовательности ФГШ.

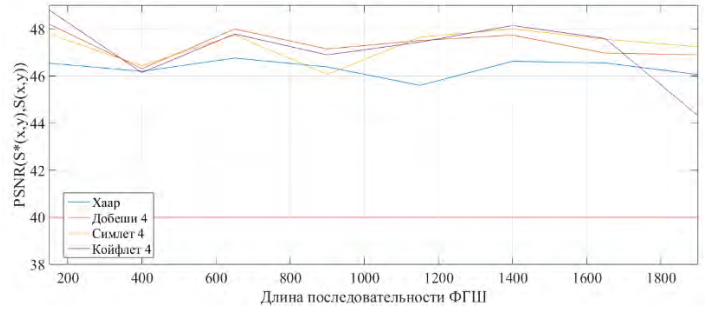

Рис. 5. Зависимость PSNR стегоконтейнера от длины последовательности ФГШ

На рисунке 6 представлена зависимость $B_{ПСП}$ (i=0) от длины ФГШ.

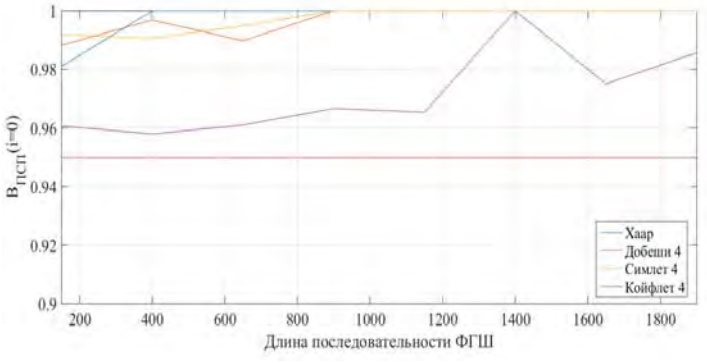

Рис. 6. Зависимость $B_{ПСП}(i=0)$ от длины последовательности ФГШ

Из полученных значений можно сделать вывод о том, что длина последовательности ФГШ незначительно влияет на качество извлечения.

В процессе вейвлет реконструкции маркированного изображения на передающей стороне и вейвлет разложения на приемной стороне неизбежно возникают искажения в добавленных шумовых последовательностях, что ведёт к погрешностям при оценке показателя Хёрста. Для того чтобы данные погрешности не влияли на достоверность извлечения ПСП, необходимо задавать показатели Хёрста для нулевой и единичной последовательности значительно отличались.

Как известно, что отличие показателя Хёрста от 0,5 является своеобразным отражением фрактальных свойств процессов, порождающих временные ряды: по аналогии с обобщенным броуновским движением при H > 0, 5 поддерживается наблюдающаяся тенденция (свойство персистентности), а при H < 0, 5 тенденция сменяется на противоположную (антиперсистентности), т. е. рост наблюдаемой величины сменяется убыванием и наоборот [19-20].

Исходя из вышеизложенного, было решено использовать для встраивания нулевого бита ПСП последовательность ФГШ с показателем Хёрста 0.5, что является нижней границей трендоустойчивого самоподобного процесса. Результаты исследования влияния значения показателя Хёрста единичной последовательности на качество встраивания и извлечения показаны на рисунке 7-8.

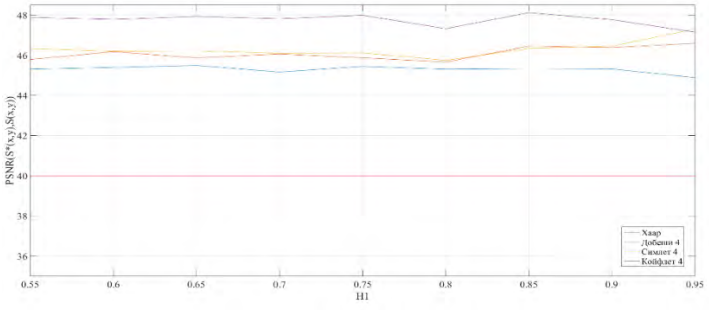

Рис. 7. Зависимость PSNR стегоконтейнера от значения показателя Хёрста единичной последовательности H_1

На рисунке видно, что нет прямой зависимости между значением показателя Хёрста H_1 и степенью искажения контейнера. Все полученные значения превышают предельный уровень PSNR=40 дБ.

На рисунке 8 представлена зависимость $B_{ПСП}(i=0)$ от значения показателя Хёрста единичной последовательности H_1.

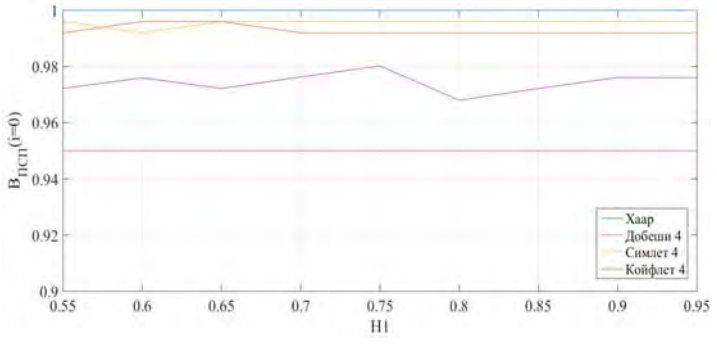

Рис. 8. Зависимость $B_{ПСП}(i=0)$ от значения показателя Хёрста единичной последовательности H_1

Как говорилось выше, при оценке показателя Хёрста на приемной стороне могут возникать погрешности. Возможные

погрешности необходимо учитывать при выборе порога $H_{пор}$, на основе которого производится восстановление ПСП.

На рисунке 9 представлена зависимость $B_{ПСП}$ (i=0) от порогового значения $H_{пор}$

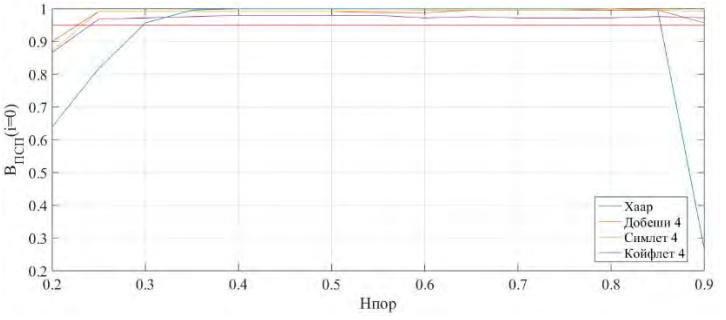

Рис. 9. Зависимость $B_{ПСП}$ (i=0) от порога $H_{пор}$

На основе анализа полученных результатов можно сделать вывод, что при использовании вейвлета Хаара рекомендуется использовать значение порога Hthr∈[0.35;0.75], для вейвлетов Добеши 4 и Симлет 4 рекомендуется Hthr∈[0.4;0.75], для Койфлет 4 - Hthr∈[0.3;0.55].

Заключение

Проведенные исследования показали, что использование фрактального гауссовского шума позволяет осуществить встраивание цифровых водяных знаков в целях защиты авторских прав с сохранением высокого качества встраивания и извлечения.

Проведенные исследования параметров алгоритма позволили сформулировать следующие рекомендации:

– наилучший баланс между качеством контейнера и качеством извлечения достигается при замене коэффициентов первого и второго уровня вейвлет-разложения;

– рекомендуется использовать alpha∈ [2.5;12.5];

– значения длины последовательности ФГШ и показателя Хёрста единичной последовательности не оказывают значительного влияния на вероятность ошибки извлечения;

– при использовании вейвлета Хаара рекомендуется использовать значение порога Hthr∈[0.35;0.75], для вейвлетов Добеши 4 и Симлет 4 рекомендуется Hthr∈[0.4;0.75], для Койфлет 4 - Hthr∈[0.3;0.55];

– наибольшие ошибки извлечения возникают при использовании вейвлета Койфлет 4, наименьшие – при использовании вейвлета Хаара.

Литература

1. *Sowmya S., Karanth S., Kumar S.* Protection of data using image watermarking technique // Global Transitions Proceedings, 2021, no. 2, pp.386-391.

2. *Wadhera S., Kamrac D., Rajpal A., Jain A., Jain V.* A Comprehensive Review on Digital Image Watermarking // Workshop on Computer Networks & Communications, 2021, pp.126-143.

3. *Sheluhin O.I., Magomedova D. I., Rybakov S. Y., Simonyan A. G.* Marking audio signals using fractal gaussian noise // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 – Conference Proceedings, 30 июня – 02 июля 2021 года. Svetlogorsk, Kaliningrad Region, 2021. P. 9488381. doi10.1109/SYNCHROINFO51390.2021.9488381

4. *Awarayi N. S., Appiah O., Weyori B.A., Ninfaakang C.B.* A Digital Image Watermarking Using Dwt and Lshaped Tromino Fractal Encryption // I.J. Image, Graphics and Signal Processing, 2021, pp. 33-43.

5. *Kiani K., Mousavi A., Shamshirband S.* A new fractal watermarking method for images of text // International Journal of Advanced Intelligence Paradigms, 2019, pp. 207-219.

6. *Sun T, Wang X, Lin D.* Medical image security authentication method based on wavelet reconstruction and fractal dimension // International Journal of Distributed Sensor Networks, 2021, no.17(4), pp. 1-10.

7. *Caballero-Hernandez H., Muñoz-Jimenez V., Ramos M.A.* Steganographic Method to Data Hiding in RGB Images Using Pixels Redistribution Combining Fractal-Based Coding and DWT // Intelligent Computing. Lecture Notes in Networks and Systems, 2021, pp. 1-18.

8. *Ali A.H., George L.E., Zaidan A.A., Mokhtar M.R.* High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain // Multimed Tools Appl, no. 77, 2018, pp. 31487-31516.

9. *Zhang X., Peng F., Lin Z.* A Coverless Image Information Hiding Algorithm Based on Fractal Theory // International Journal of Bifurcation and Chaos, 2020, pp. 1-20.

10. *Alia M., Suwais K.* Improved Steganography Scheme based on Fractal Set // The International Arab Journal of Information Technology, 2020, pp. 128-136.

11. *Abbasi M.* Color Image Steganography using Dual Wavelet Transforms // International Journal of Computer Applications, 2019, pp. 32-38.

12. *Pan P., Wu Z., Yang C., Zhao B.* Double-Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi-Region Coverage // Entropy. 2022, pp. 1-21.

13. *Sharma V.* A Daubechies DWT Based Image Steganography Using Smoothing Operation // The International Arab Journal of Information Technology, 2020, pp.154-161.

14. *Fakhredanesh M., Rahmati M., Safabakhsh R.* Steganography in discrete wavelet transform based on human visual system and cover model // Multimedia Tools and Applications. 2019, pp. 18475-18502.

15. *Bas P., Filler T. & Pevn´y T.* Break our steganographic system // The ins and outs of organizing BOSS. LNCS. 6958, 2011, pp. 59-70. Available from: doi:10.1007/978-3-642-24178-9_5.

16. PPG-LIRMM-COLOR database. Available at: http://www.lirmm.fr/~chaumont/PPG-LIRMM-COLOR.html.

17. *Onur K., Yilmaz A., Tekalp M.* On the Computation of PSNR for a Set of Images or Video // arXiv, 2021, pp. 1-5.

18. *Samithamby S.* Usefulness of Correlation Analysis // SSRN Electronic Journal, 2021, pp. 1-10.

19. *Ceballos R.F., Largo F.F.* On The Estimation of the Hurst Exponent Using Adjusted Rescaled Range Analysis, Detrended Fluctuation Analysis and Variance Time Plot: A Case of Exponential Distribution // Imperial Journal of Interdisciplinary Research, 2017, vol-3, pp. 424-434.

20. *Gomez-Aguila A.* Improvement in Hurst exponent estimation and its application to financial markets // Financial Innovation, 2022, pp. 1-21.

LABELING STILL IMAGES USING FRACTAL GAUSSIAN NOISE AND 2D DISCRETE WAVELET TRANSFORM FOR COPYRIGHT PROTECTION

DZHENNET I. MAGOMEDOVA
Moscow, Russia

KEYWORDS: *copyright protection, discrete wavelet transform, fractal Gaussian noise, steganography, Hurst exponent.*

ABSTRACT

Introduction. The relevance of copyright protection for multimedia content is determined by the using digital objects in all areas of life. The number and qualification of malefactors aimed at using someone else's intellectual work is constantly growing. The problem of copyright protection can be solved by using steganography methods. Despite the wide development of the topic, there are a number of problems that limit the use of classical steganography methods. The resistance of many well-known methods to unauthorized access is based on knowledge of the algorithm without the use of additional keys. This leaves the methods vulnerable to modification and removal of the embedded label by an intruder. **The aim of the study** is to increase the stability of copyright protection algorithms from unauthorized access. It is proposed to embed watermarks in two stages: at the first stage, the digital watermark values are replaced by sequences of fractal Gaussian noise, then the resulting fractal key is embedded in the protected image by replacing the wavelet decomposition coefficients. **Methods:** The fast Fourier transform algorithm was used to generate fractal Gaussian noise. The Hurst exponent of noise sequences was estimated using R/S analysis. **Results:** A new algorithm for embedding digital watermarks into images based on fractal Gaussian noise and discrete wavelet transform is proposed. The values of rational parameters of the algorithm, such as the decomposition level, the scaling factor, the length of the noise sequence, the values of the Hurst exponent for a single sequence, and the threshold value, are determined to achieve the best balance between the quality of embedding and extraction.

REFERENCES

1. S. Sowmya, S. Karanth, S. Kumar (2021). Protection of data using image watermarking technique. *Global Transitions Proceedings,* no. 2, pp.386-391.

2. S. Wadhera, D. Kamrac, A. Rajpal, A. Jain, V. Jain (2021). A Comprehensive Review on Digital Image Watermarking. *Workshop on Computer Networks & Communications*, pp.126-143.

3. O.I. Sheluhin, D.I. Magomedova, S.Y. Rybakov, A.G. Simonyan (2021). Marking audio signals using fractal gaussian noise. *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO*. Conference Proceedings, Svetlogorsk, Kaliningrad Region, Svetlogorsk, Kaliningrad Region, P. 9488381. doi10.1109/SYNCHROINFO51390.2021.9488381.

4. N.S. Awarayi, O. Appiah, B.A. Weyori, C.B. Ninfaakang (2021). A Digital Image Watermarking Using Dwt and Lshaped Tromino Fractal Encryption. *I.J. Image, Graphics and Signal Processing*, pp. 33-43.

5. K. Kiani, A. Mousavi, S. Shamshirband (2019). A new fractal watermarking method for images of text. *International Journal of Advanced Intelligence Paradigms*, pp. 207-219.

6. T. Sun, X. Wang, D. Lin (2021). Medical image security authentication method based on wavelet reconstruction and fractal dimension. *International Journal of Distributed Sensor Networks*, no.17(4), pp. 1-10.

7. H.Caballero-Hernandez, V. Muoz-Jimenez, M.A Ramos (2021). Steganographic Method to Data Hiding in RGB Images Using Pixels Redistribution Combining Fractal-Based Coding and DWT. *Intelligent Computing. Lecture Notes in Networks and Systems*, pp. 1-18.

8. A.H Ali, L.E George, A.A. Zaidan, M.R. Mokhtar (2018). High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. *Multimed Tools Appl. No.* 77, pp. 31487-31516.

9. X. Zhang, F. Peng, Z. Lin (2020). A Coverless Image Information Hiding Algorithm Based on Fractal Theory. *International Journal of Bifurcation and Chaos*, pp.1-20.

10. M. Alia, K. Suwais (2020). Improved Steganography Scheme based on Fractal Set. *The International Arab Journal of Information Technology*, pp. 128-136.

11. M. Abbasi (2019). Color Image Steganography using Dual Wavelet Transforms. *International Journal of Computer Applications*, pp. 32-38.

12. P. Pan, Z. Wu, C. Yang, B. Zhao (2022). Double-Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi-Region Coverage. *Entropy*, pp. 1-21.

13. V. Sharma (2020). A Daubechies DWT Based Image Steganography Using Smoothing Operation. *The International Arab Journal of Information Technology*, pp.154-161.

14. M. Fakhredanesh, M. Rahmati, R. Safabakhsh (2019). Steganography in discrete wavelet transform based on human visual system and cover model. *Multimedia Tools and Applications*, pp. 18475-18502.

15. P. Bas, T. Filler, T. Pevny (2011). "Break our steganographic system" the ins and outs of organizing BOSS. LNCS. no. 6958, pp, 59-70. doi:10.1007/978-3-642-24178-9_5.

16. PPG-LIRMM-COLOR database. Available at: http://www.lirmm.fr/~chaumont/PPG-LIRMM-COLOR.html.

17. K. Onur, A. Yilmaz, M.Tekalp (2021). On the Computation of PSNR for a Set of Images or Video. *arXiv*, pp. 1-5.

18. S. Samithamby (2021). Usefulness of Correlation Analysis. *SSRN Electronic Journal*, pp. 1-10.

19. R.F. Ceballos, F.F. Largo (2017). On The Estimation of the Hurst Exponent Using Adjusted Rescaled Range Analysis, Detrended Fluctuation Analysis and Variance Time Plot: A Case of Exponential Distribution. *Imperial Journal of Interdisciplinary Research*, vol-3, pp. 424-434.

20. A. Gomez-Aguila (2022). Improvement in Hurst exponent estimation and its application to financial markets //. *Financial Innovation*, pp. 1-21.

INFORMATION ABOUT AUTHOR:

Magomedova D. I., Senior Lecturer at the Department of Information Security of the Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Magomedova D. I. Labeling still images using fractal Gaussian noise and 2D discrete wavelet transform for copyright protection. H&ES Reserch. 2022. Vol. 14. No 6. P. 20-26. doi: 10.36724/2409-5419-2022-14-6-20-26 (In Rus)

doi: 10.36724/2409-5419-2022-14-6-27-34

АНАЛИЗ ТЕОРИИ И ПРАКТИКИ СУЩЕСТВУЮЩИХ ИНВАРИАНТНЫХ СИСТЕМ СВЯЗИ

ПАВЛОВ
Иван Иванович[1]

АННОТАЦИЯ

Введение: РЕжегодное увеличение передаваемой информации по каналам связи, приводит к усложнению решения задач по помехоустойчивости. Для облегчения решения данных задач, необходимо произвести анализ понятий "инварианта". Данное понятие встречается во всех областях науки и поэтому необходимо рассмотреть различные понятия "инварианта" и авторов, занимающихся изучением данной проблемы. Произвести анализ различий понятий инвариантности в системах связи и других областях науки. И рассмотрен вопрос различия между понятиями "тензор" и "матрица". Матричное описание характеризует фиксированное значение объекта для выбранного момента времени, а тензорное – позволяет получить описание объекта для всех моментов времени и, следовательно, является более общим. Если мы рассмотрим матрицу, которая описывает объект, то данная матрица не будет являться инвариантным объектом. Но зачастую на практике нам необходимо производить большое количество вычислений, и часто они являются однотипными. Для этого применяют тензорные методы вычислений, что приводит к более краткой и наглядной форме представления. **Методы и результаты исследования:** Для решения проблем помехоустойчивости системы связи необходимо чтобы на приемной стороне вероятность ошибок не превышала допустимых значений. В системах связи информация, проходящая через канал связи, может быть передана в канал связи с постоянными характеристиками или в канал связи с переменными характеристиками. Если канал связи организован с постоянными характеристиками, то вероятность ошибки в данном канале является величиной постоянной. И для того, чтобы организовать помехоустойчивость системы связи, необходимо спроектировать её, чтобы все элементы данной системы связи были подобраны, организованы и синхронизированы так, чтобы параметры системы связи удовлетворяли заданным требованиям. Для обеспечения заданных требований система связи может быть абсолютной инвариантной или относительной инвариантной к аддитивной или неаддитивной помехе. Рассмотрена классификация инвариантных систем связи по работе Ю.Б. Окунева.

Сведения об авторе:

[1] Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет телекоммуникации и информатики" (СибГУТИ), доцент кафедры радиотехнических устройств и техносферной безопасности, доцент, к.т.н., Академик МАС, г. Новосибирск, Россия, iipavlov02@mail.ru

КЛЮЧЕВЫЕ СЛОВА: *инвариант, инвариантность, абсолютная инвариантность, относительная инвариантность, флуктуационная помеха, сосредоточенная по спектру помеха, системы связи, постоянные параметры, переменные параметры, аддитивная помеха, неаддитивная помеха.*

Для цитирования: Павлов И.И. Анализ теории и практики существующих инвариантных систем связи // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 27-34. doi: 10.36724/2409-5419-2022-14-6-27-34

Введение

В настоящее время с каждым годом существенно возрастают информационные потоки, передаваемые по каналам связи. Это обстоятельство требует увеличения скорости передачи информации и достоверности.

Эта сложная задача решается комплексом мер, таких как устранение избыточности, помехоустойчивого кодирования, скоростных методов модуляции и т.д. С учетом того что реальные каналы являются каналами с переменными параметрами, в современных системах связи, как правило, используются адаптивные методы передачи и приема. Ввиду изменения параметров канала связи в процессе сеанса связи данные методы обладают серьезными их недостатками:

– требуется большое количество операций умножения и сложения, выполняемых за интервал дискретизации;

– необходим большой объем памяти, для хранения всех возможных ранее вычисленных вариантов сигналов.

Отсюда видно, что алгоритмы, данного метода, требуют осуществления многочисленных операций свертки, которые достаточно сложны, а устройства, их реализующие, характеризуются большим уровнем собственных помех. Также не полностью решены и вопросы воздействия помех в канале связи. шума среды распространения.

Указанные недостатки стимулировали поиск новых методов в построении систем связи. Одним из таких методов является метод использующий новый математический аппарат для описания преобразований сигналов каналом связи – теорию групп преобразования.

Согласно этой теории, преобразование входных сигналов в выходные можно рассматривать как преобразование системы координат пространства представления сигналов, когда входные сигналы отображаются точками в одной системе координат, а выходные – теми же точками в другой, преобразованной системе координат. Операции преобразований систем координат обладают свойствами группы.

Важнейшим моментом для передачи сообщений является то, что группа преобразований обладает инвариантами – особыми соотношениями между параметрами сигналов, которые остаются неизменными, несмотря на искажение самих сигналов каналом связи. В частности, инвариантом аффинной группы преобразований является сохраняющейся каналом отношение длин векторов сигналов, лежащих на одной прямой.

Использование инвариантной методологии позволяет:

– улучшить качественные характеристики систем передачи информации при воздействии мультипликативных помех;

– ороться с искажениями среды распространения;

– бороться с доплеровским смещением частотного спектра;

– бороться с эхосигналами с помощью линейных алгоритмов;

– бороться с эхосигналами с помощью нелинейных алгоритмов.

Указанные выше направления работ могут быть реализованы в виде алгоритмов и устройств во временной и частотной областях передачи информации.

Для решения поставленных задач необходимо провести анализ существующих инвариантных систем связи, а также найти пути к устранению выявленных недостатков и дополнению новых методов в общую теорию инвариантных систем передачи сигналов по каналам с переменными параметрами.

Анализ понятия инварианта и различие понятий инвариантности в системах автоматики и системах связи

В последнее время вырос интерес к тензорным методам расчета сложных систем, в том числе и к расчетам систем связи. Для того чтобы использовать тензорные методы необходимо обратиться к инвариантным свойствам объектов и сетей связи. Если рассматривать инвариантность в геометрии, теории управления и в теории систем связи, то на первый взгляд может показаться, что понятие инвариантности понимается по-разному. Например, понятие инвариантности в геометрии основано на свойствах геометрических объектов, которые связаны с действиями групп и при этом при преобразованиях в свойствах геометрических объектов данные группы остаются неизменными [1].

В Эрлангенской программе [1, 2] Феликс Клейн предложил единый подход к описанию различных геометрий [1]. Изучив Эрлангенскую программу Феликса Клейна, можем выделить одну из основных задач геометрии. Данная задача описывает построение инвариантов геометрических объектов относительно действия группы, которая и определяет эту геометрию. Данный подход решения этой задачи основывается на идеи Софуса Ли, который и ввел в геометрию непрерывные группы преобразований, в настоящее время известные во всем мире как группы Ли [1, 3, 4].

В частности, при рассмотрении классификационных задач и проблем эквивалентности в дифференциальной геометрии следует рассматривать дифференциальные инварианты относительно действия псевдогрупп Ли. При этом проблема эквивалентности геометрических объектов сводится к нахождению полной системы скалярных дифференциальных инвариантов [1]. Рассмотренный подход на многие годы положил ход развития математики. Благодаря этому подходу позволили развить геометрическую теорию дифференциальных уравнений [1, 5, 6], и получить новые методы их интегрирования [1, 7, 8]. В работах [1, 9, 10, 11, 12] были рассмотрены проблемы классификации нелинейных дифференциальных уравнений относительно псевдогруппы Ли контактных преобразований. Чтобы найти решения в поставленных задачах были применены дифференциальные инварианты.

В теории управления под инвариантностью понимается независимость какой-либо системы автоматического регулирования от приложенных к ней внешних воздействий [1]. Одним из первых кто обратил внимание на это свойство, был Г.В. Щипанов, опубликовавший свою первую работу в 1939 году в журнале «Автоматика и телемеханика», в которой выдвинул теорию инвариантности автоматических систем [1, 13]. Впоследствии идея Г.В. Щипанова была развита Б.Н. Петровым [1, 14], который сформулировал принцип инвариантности систем автоматического регулирования, известный сейчас как принцип инвариантности Петрова.

Основной задачей теории инвариантности систем автоматического регулирования является создание систем, не чувствительных, то есть инвариантных, по отношению к возмущениям [1].

В работе Ю.Б. Окунева [15] под инвариантностью понимается способность системы связи автоматического регулирования противостоять мешающим воздействиям. В качестве инварианта рассматривается величина управляющего воздействия по одной из координат. Система автоматического регулирования будет инвариантной тогда, когда из-за влияния мешающего воздействия не будет зависеть управление по некоторой координате.

Если же рассматривать понятие инвариантности в общем случае, то автор Мироновский Л.А. в своей работе [16] дал следующее определение: «инвариантность – неизменность и независимость чего-то от происходящих изменений другого чего-то, влияющего на наш объект рассмотрения» [17]. Из выше сказанного можно сделать вывод, что инвариант – это какая та величина, которая должна характеризовать параметр объекта рассмотрения, и при этом данная величина остается неизменной при любых изменениях не только внешней среды объекта рассмотрения, но и внутренней среды данного объекта. Если заглянуть в большую советскую энциклопедию [18], то там мы найдем следующее определение: «инварианты – числа, алгебраические выражения и т. п., связанные с каким-либо математическим объектом и остающиеся неизменными при определенных преобразованиях этого объекта или системы отсчёта, в которой описывается объект. Чтобы охарактеризовать какую-либо геометрическую фигуру и её положение с помощью чисел, обычно приходится вводить некоторую вспомогательную систему отсчёта или систему координат. Полученные в такой системе числа $x_1, x_2, ..., x_n$ характеризуют не только изучаемую геометрическую фигуру, но и её отношение к системе отсчёта, и при изменении этой системы фигуре будут отвечать другие числа $x'_1, x'_2, ..., x'_n$. Поэтому если значение какого-либо выражения $f(x_1, x_2, ..., x_n)$ характерно для фигуры самой по себе, то оно не должно зависеть от системы отсчёта, т. е. должно выполняться соотношение $f(x_1, x_2, ..., x_n) = f(x'_1, x'_2, ..., x'_n)$».

В работе американских ученных Дэниела Брюса Энниса и Гордона Киндлманна [19] можно найти следующее определение тензорных инвариантов: «инварианты – скалярные функции тензорных переменных, независимые от выбора координатной системы».

Еще лауреат Нобелевской премии по физике, немецкий ученый Альберт Эйнштейн в своих работах все инвариантные величины назвал «тензорами», а нидерландский математик Ян Арнольдус Схоутен объединил понятием «геометрическими объектами». В дальнейшем А.Е. Петров в своей работе [20] рассмотрел все три понятия – тензор, геометрический объект и инвариант, как синонимы. Также А.Е. Петров в своей работе [20] дал описание одного и того же объекта, как с помощью понятия «тензора», так и с помощью понятия «матрица», где можно увидеть различия. Матричное описание характеризует фиксированное значение объекта для выбранного момента времени, а тензорное – позволяет получить описание объекта для всех моментов времени и, следовательно, является более общим [17, 20].

Если мы рассмотрим матрицу, которая описывает объект, то данная матрица не будет являться инвариантным объектом. Но зачастую на практике нам необходимо производить большое количество вычислений, и часто они являются однотипными. Для этого применяют тензорные методы вычислений, что приводит к более краткой и наглядной форме представления.

В системах связи матричные методы применяются для исследования структурных свойств, тензорные методы же используются для исследования структурных и функциональных свойств систем связи.

В работе [17] авторы подчеркнули, что: «Инварианты могут быть строгими и нестрогими, т. е. инвариантами с неточностью, когда изменение соответствующей величины не превышает заданного допуска на ее номинальное значение. Инварианты могут быть простыми параметрами, а могут определяться из формулы, связывающей функциональной зависимостью несколько переменных. Так как параметры объектов в реальном мире не могут постоянно оставаться неизменными, то для реальных объектов интервал времени сохранения инвариантных свойств объекта должен быть не менее времени его эксплуатации, т. е. объект – это носитель своих свойств, для которого некоторые параметры могут быть инвариантами».

Понятие «инвариант» и «инвариантность» можно использовать в различных областях техники и науки. Например, в биологии нормальное артериальное давление у человека в зависимости от возраста будет являться инвариантом; в юриспруденции инвариантом можно считать то, что все равны перед законом; закон сохранения энергии будет инвариантом в физике и так далее. Что касается систем связи, то в роли инварианта можно использовать математическое ожидание. Например, вероятность ошибки, которая является математическим ожиданием частости ошибок [15].

В работе [15] Ю.Б. Окунев дал следующее определение: «Система связи, количественная характеристика помехоустойчивости которой является инвариантом определенного класса помех, будет называться инвариантной по отношению к данным помехам». Для представления в математической форме обозначим количественную характеристику помехоустойчивости системы связи через P (вероятность ошибки при приеме сигнала), а Ξ – реализацию помехи в канале связи.

$$P = \text{invar}\ \Xi. \qquad (1)$$

В выражении (1) в левой части всегда должна стоять числовая характеристика помехоустойчивости системы связи, а в правой части – помеха канала связи. Инвариантом будет считаться числовая характеристика помехоустойчивости системы связи по отношению к помехе [15, 21, 22].

Необходимо выделить отличие в решении проблем инвариантных систем автоматизированного регулирования и в решении проблем инвариантности систем связи. Для этого обратимся к известной работе Ю.Б. Окунева [15], посвященной системам связи с инвариантными характеристиками помехоустойчивости.

Для решения проблемы инвариантности в системах автоматического регулирования обычно применяют пространственное разделение управляющих сигналов и мешающих воздействии. Данный способ нам позволит измерить любое мешающее воздействие и соответственно найти необходимые компенсационные методы для выполнения инвариантности [15]. Например, использование глубокой отрицательной обратной связи или использование второго искусственного

канала для компенсации мешающих воздействий на первом канале.

В системах связи данный способ невозможно реализовать так как полезный сигнал и помеха существуют в канале связи в одно и тоже время (точке). Если бы была возможность разделения сигнала и помехи на входе приемника, то проблема борьбы с помехой была бы не актуальна. В связи с чем, смешанный сигнал с помехой всегда имеет место на входе приемника. Компенсационные методы подавления помех, которые используются в решении проблем инвариантности систем автоматизированного регулирования, не могут быть реализованы в решении проблем инвариантности систем связи.

Еще одной особенностью решения проблем инвариантности систем связи является не мгновенное значение выходной величины, а статическая характеристика выходной величины, например, как уже говорилось выше, математическое ожидание [15].

Для решения проблем инвариантности систем связи необходимо, чтобы на приемной стороне вероятность ошибок не превышала допустимых значений. Это позволит получателю сообщений принимать информацию без искажений и с более высоким качеством. Но если вероятность ошибок превысит допустимый предел значений, то принимаемое сообщение невозможно будет правильно распознать, что приведет к низкому качеству принимаемой информации и соответственно ошибочному приему.

В системах связи информация, проходящая через канал связи, может быть передана в канал связи с постоянными характеристиками или в канал связи с переменными характеристиками. Если канал связи организован с постоянными характеристиками, то вероятность ошибки в данном канале является величиной постоянной. Для организации помехоустойчивости системы связи, необходимо спроектировать её так, чтобы все элементы данной системы были подобраны, организованы и синхронизированы, а параметры системы связи удовлетворяли заданным требованиям.

Соответственно в каналах связи с переменными характеристиками вероятность ошибки будет переменной величиной. Для организации помехоустойчивости в данной системе связи необходимо обеспечить среднее значение заданной допустимой вероятности ошибки. Данная проблема будет считаться выполненной, если независимо от помех в канале связи вероятность ошибки остается неизменной и ниже заданной, или, независимо от изменения характеристик канала связи, вероятность ошибки может изменяться случайно в диапазоне, не превышающем допустимые значения.

Востребованность качественного обеспечения передачи информации в канале связи с переменными характеристиками приводит к потребности в инвариантных системах связи.

Понятие абсолютной и относительной инвариантности

Изменения характеристик канала связи вызываются разными по своей природе помехами – аддитивными и неаддитивными [15]. Аддитивная помеха в канале связи является случайным процессом, который складывается с полезным сигналом и тем самым искажает сигнал. Неаддитивная помеха в канале связи воздействует на отдельные параметры сигнала и канала, что приводит к изменению. Например, в сигнале может измениться амплитуда, фаза или частота сигнала под воздействием на сигнал неаддитивной помехи.

Одним из видов аддитивной помехи является помеха, сосредоточенная по спектру или как её, еще называют гармоническая помеха. Этот вид помех представляет собой узкополосный гармонический сигнал. Источниками таких помех могут быть переходные затухания между цепями кабеля, влияние посторонних радиостанций и т. п. Такую помеху приблизительно можно представить в виде гармонического сигнала со случайной амплитудой, частотой и фазой [15]:

$$\xi(t) = a_n \cos(\omega_n t + \varphi_n)$$

В канале связи от передатчика к приемнику посылается полезный сигнал $S(t)$, под воздействием сосредоточенной по спектру помехи $\xi(t)$ на входе приемника мы получим искаженный сигнал:

$$S_{иск}(t) = S(t) + \xi(t)$$

Если на приемной стороне сосредоточенную по спектру помеху $\xi(t)$ возможно описать детерминированной функцией, то тогда соответственно все параметры данной помехи будут известны. При согласованной работе приемного устройства можно сосредоточенную по спектру помеху $\xi(t)$ полностью компенсировать и получить полезный сигнал $S(t)$. Такая система связи будет абсолютно инвариантной к сосредоточенной по спектру помехе.

Но в реальности в канале связи присутствует флуктуационная (случайная) помеха, которая имеет широкий спектр и максимальной энтропией, и, следовательно, воздействие данной помехи на полезный сигнал оказывается больше. Математической моделью флуктуационной помехи является гауссовский случайный процесс с нулевым средним значением и постоянной спектральной плотностью мощности [15].

«Помехоустойчивость системы по отношению к флуктуационной помехе определяется отношением энергии сигнала Q к спектральной плотности мощности шума σ_0^2, т.е. величиной

$$h^2 = \frac{Q}{\sigma_0^2} = \frac{P_c T}{\sigma_0^2} = \frac{P_c}{P_n}\Delta f T$$

где P_c – мощность сигнала; P_n – средняя мощность помехи; T – длительность посылки сигнала; Δf – ширина полосы пропускания канала» [15].

В канале связи на полезный сигнал действует флуктуационная помеха, а так как данная помеха целиком ориентируется на величину h, то система связи будет инвариантной к помехе ξ тогда, когда действие данной помехи на зависимость вероятности ошибки от h будет оставаться неизменным. Если в случае, когда в канале связи была сосредоточенная по спектру помеха, то инвариантом по отношению к данной помехе являлось число. Когда в канале связи на полезный сигнал воздействует флуктуационная помеха, инвариантом к данной помехе выступает функция $p(h)$.

Ю.Б. Окунев доказал, что «при большой избыточности составного сигнала функция $p(h, \xi)$ мало отличается от функции $p(h, 0)$ и, следовательно, можно говорить о частичной компенсации помехи» [15]. Такая система связи будет относительно инвариантной к флуктуационной помехе.

В каналах связи существует множество различных помех соответственно наиболее распространенными будут системы связи с относительно инвариантными характеристиками помехоустойчивости. Но это не исключает возможности нахождения условий для создания абсолютно инвариантных систем к определенного вида помех.

Классификация инвариантных систем связи Окунева

Ранее были рассмотрены вопросы понятия инварианта и инвариантности в системах связи, а также определились с абсолютной и относительной инвариантностью в системах связи. В работе Ю.Б. Окунева [15] была предложена классификация систем связи с инвариантными характеристиками помехоустойчивости, представленная на рисунке 1.

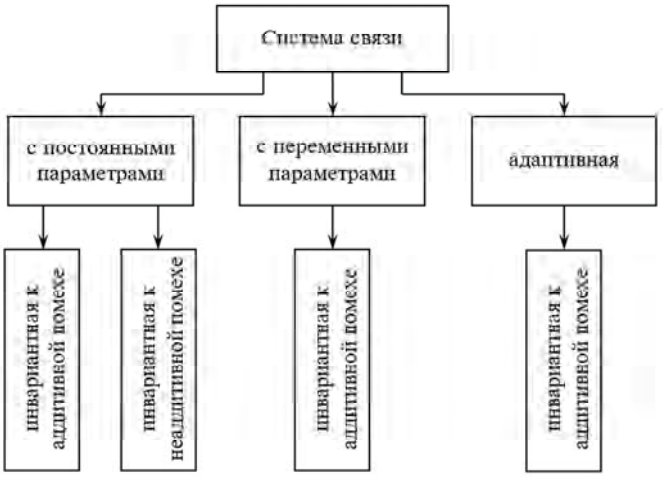

Рис. 1. Классификация инвариантных систем связи, предложенная Ю.Б. Окуневым

Система связи с постоянными параметрами инвариантная к аддитивной помехе.

Данная система представляет собой, рассмотренные выше, систему абсолютной инвариантности к сосредоточенной помехе, основным недостатком которой является то, что увеличение избыточности сигнала прямо пропорционально влияет на расширение спектра сигнала, но это не всегда можно реализовать в системах связи.

Система с относительной инвариантностью к флуктуационной помехе.

В данной системе инвариантность достигается за счет усложнения сигнала, которое обеспечивается увеличением базы сигнала ΔfT, на базу сигнала в реальности нельзя увеличивать без конца [15].

Система связи с постоянными параметрами инвариантная к неаддитивной помехе.

В данной системе неаддитивная помеха в канале связи вызывает изменения любого из параметров полезного сигнала. В работе Ю.Б. Окунева [15] рассматривался пример, когда в полезном сигнале изменялась частота. Автор доказал, что можно создать систему связи с постоянными параметрами инвариантной к неаддитивной помехе, но необходимо использовать автокорреляционный прием. Подобрав нужный алгоритм работы автокорреляционного приема сигнала, добиваемся абсолютной инвариантности системы связи к частоте сигнала (но и любой другой параметр сигнала). Недостатком данной системы связи является то, что происходит снижение помехоустойчивости по отношению к аддитивным помехам.

Система связи с переменными параметрами инвариантная к аддитивной помехе.

Данная система представляет собой, широкополосную систему через которую будет передаваться составной сигнал, а на приемной стороне сигнал поступает на адаптивный приемник. Принцип работы данной системы состоит в следующем, из передатчика в канал связи передается составной сигнал, который является суммой n гармонических колебаний с разными частотами. В канале связи на эти гармонические сигналы будет действовать сосредоточенная по спектру помеха. В приемном устройстве количества ветвей должно быть равно количеству гармонических колебаний в составном сигнале. Гармонические колебания, которые несут одну и ту же информацию, поступают параллельно на входы этих ветвей, далее происходит работа адаптивного приемника, детали работы которой мы рассматривать не будем. Переданную информацию определяют так сказать «методом голосования», простым большинством. И так как сосредоточенная по спектру помеха может воздействовать только на одно гармоническое колебание и данная ветвь будет недостоверной, соответственно в адаптивном приемнике эту ветвь можно исключить в дальнейшей обработке и система будет абсолютно инвариантна к данной помехе канала связи. Если происходит изменение сосредоточенной по спектру помехи, то происходит обучение приемника, определяется ветвь с пораженным гармоническим сигналом и данная ветвь удаляется из приема [15].

При наличии в системе связи флуктуационной помехи, система связи с переменными параметрами инвариантная к аддитивной помехе может быть только относительно инвариантной. Это достигается за счет использования более сложного сигнала с большой базой, и наличием адаптивного приемника со сложной структурой и принципом работы.

Адаптивная система инвариантная к аддитивной помехе.

Данная система является модификацией системы связи с переменными параметрами инвариантной к аддитивной помехе. Кроме адаптивного приемного устройства, используется адаптивный передатчик, а также канал с обратной связью. По каналу связи передаются информационные и проверочные элементы. На адаптивном приемнике происходит прием данных элементов и по каналу обратной связи к адаптивному передатчику отправляются проверочные элементы. Если прием был без ошибок продолжается передача элементов, если же будет обнаружена ошибка, то происходит повторная передача ранее переданных элементов. Адаптивная система будет абсолютно инвариантной к вероятности необнаруженной ошибки при влиянии сосредоточенной по спектру помехи, но приходиться платить временем для передачи элементов, так как возникает потребность повторной передачи информационных и проверочных элементов.

Если в канале связи будет присутствовать флуктуационная помеха, то вероятность не обнаружения ошибки увеличивается и тогда вводиться понятие допустимая вероятность

необнаруженной ошибки. Ю.Б. Окунев доказал, что адаптивная система инвариантна к флуктуационной помехе если выполняется условие:

$$2^{k-n} \le p_{н\ о\ доп}$$

где n – длина переданной кодовой комбинации; k – количество информационных элементов; $p_{н\ о\ доп}$ – допустимая вероятность необнаруженной ошибки [15].

Основными недостатками данной системы является снижение скорости передачи данных. Чем больше мощность помехи, тем скорость передачи данных меньше, за счет частых перезапросов. Необходим код с избыточностью для формирования информационных и проверочных элементов.

Заключение

В статье произведен анализ понятия инварианта и различие понятий инвариантности в системах автоматики и систем связи. На первый взгляд, при рассмотрении понятия инвариантность в геометрии, теории управления и в теории систем связи понимается по-разному. В каждой области науки и техники вопросом инвариантности занимались известные ученые, которые доказали, что «инвариант» – величина неизменная. В области систем связи большой вклад в изучение инвариантности внес Ю.Б Окунев. Он доказал, что для решения проблемы инвариантности системы связи является не мгновенное значение выходной величины, а статическая характеристика выходной величины.

Также можно отметить, что на полезный сигнал, проходящий через канал связи, действует разная помеха. Это может быть сосредоточенная по спектру помеха или флуктуационная помеха. И если на приемной стороне сосредоточенную по спектру помеху возможно определить детерминированной функцией, то тогда все параметры данной сосредоточенной по спектру помехи будут известны. В данном случае система связи будет считаться абсолютно инвариантной к сосредоточенной по спектру помехе. Если на приемной стороне определяются не все параметры помехи, такая помеха считается флуктуационной, компенсировать помеху полностью невозможно. Соответственно система связи будет считаться относительно инвариантной к флуктуационной помехе.

В заключении статьи рассмотрена классификация инвариантных систем связи по Ю.Б. Окуневу. Она состоит из систем связи с постоянными параметрами инвариантными к аддитивной помехе, систем связи с постоянными параметрами инвариантными к неаддитивной помехе, систем связи с переменными параметрами инвариантными к аддитивной помехе и адаптивных систем инвариантных к аддитивной помехе.

Литература

1. *Кушнер А.Г., Лычагин В.В.* Инвариантность Петрова и идентификация гамильтоновых систем с управляющим параметром // труды IX международной конференции «Идентификация систем и задачи управления» SICPRO. 2012. С. 75-81.

2. *Клейн Ф.* Сравнительное обозрение новейших геометрических исследований («Эрлангенская программа») // В кн.: Норден А.П. Об основах геометрии. 1872. С. 399-434.

3. *Lie S.* Ueber einige partielle Differential-Gleichunger zweiter Orduung // Math. Ann. 1872. Vol. 5, pp. 209-256.

4. *Lie S.* Begrundung einer Invarianten-Theorie der Beruhrungs-Transformationen // Math. Ann. Vol. 8, pp. 215-303.

5. *Виноградов А.М., Красильщиков И.С., Лычагин В.В.* Введение в геометрию нелинейных дифференциальных уравнений // Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления». М.: ВИНИТИ, 1988. Т. 28. С. 297.

6. *Vinogradov A.M., Krasil'shchik I.S., Lychagin V.V.* Geometry of jet spaces and nonlinear partial differential equations // Advanced Studies in Contemporary Mathematics. New York: Gordon and Breach Science Publishers. 1986. P. 441.

7. Овсянников Л.В. Групповой анализ дифференциальных уравнений. М.: Наука, 1978. С. 399.

8. *Kushner A.G., Lychagin V.V., Rubtsov V.N.* Contact geometry and nonlinear differential equations // Encyclopedia of Mathematics and Its Applications. Cambridge: Cambridge University Press. 2007. P. 496.

9. *Кушнер А.Г.* Уравнения Монжа-Ампера и е-структуры // ДАН. 1998. Т. 361. № 5. С. 595-596.

10. *Kushner A.G.* A contact linearization problem for Monge-Amp`ere equations and Laplace invariants // Acta Appl. Math. 2008. Vol. 101. No. 1-3, pp. 177-189.

11. *Kushner A.G.* On contact equivalence of Monge-Amp`ere equations to linear equations with constant coefficients // Acta Appl. Math. 2010. Vol. 109. No. 1, pp. 197-210.

12. *Lychagin V.V., Rubtsov V.N., Chekalov I.V.* A classification of Monge-Amp`ere equations // Ann. Sci. Ecole Norm. Sup. 4e s. 1993. Vol. 26, no. 3, pp. 281-308.

13. *Щипанов Г.В.* Теория и методы проектирования автоматических регуляторов // Автоматика и телемеханика. 1939. № 1. С. 49-66.

14. *Петров Б.Н.* Избранные труды. Т. 1. Теория автоматического управления. М.: Наука, 1983.

15. *Окунев Ю.Б.* Системы связи с инвариантными характеристиками помехоустойчивости. М.: Связь, 1973. С. 80.

16. *Мироновский Л. А.* Инварианты математических моделей : Текст лекций // ЛИАП. Л., 1991. С. 32.

17. *Богданов В.С., Богданов С.В.* Инварианты и тензорные инварианты сетей // Известия Волгоградского государственного технического университета. 2013. № 22 (125). С. 21-25.

18. Большая советская энциклопедия. 2013. Режим доступа: https://dic.academic.ru/dic.nsf/bse/90347/Инварианты. Дата обращения: 15.11.2022.

19. *Daniel B.* Ennis and Gordon Kindlmann. Orthogonal Tensor Invariants and the Analysis of Diffusion Tensor Magnetic Resonance Images. Magnetic Resonance in Medicine 55, pp. 136-146. 2006.

20. *Петров А. Е.* Тензорный метод двойственных сетей. М.: Центр информационных технологий в природопользовании. 2007. С. 496.

21. *Абрамов С.С., Абрамова Е.С., Павлов И.И., Павлова М.С.* Обзор основных понятий инвариантности в системах передачи данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб.: СПбГУТ, 2021. Т. 1. С. 29-34.

22. *Лебедянцев В.В., Павлов И.И.* Общая методология синтеза систем, инвариантных к неаддитивной помехе // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; СПб.: СПбГУТ, 2022. Т. 1. С. 654-657.

ANALYSIS OF THE THEORY AND PRACTICE OF EXISTING INVARIANT COMMUNICATION SYSTEMS

IVAN I. PAVLOV
Novosibirsk, Russia, iipavlov02@mail.ru

KEYWORDS: *invariant, invariance, absolute invariance, relative invariance, fluctuation interference, spectrum-centered interference, communication systems, constant parameters, variable parameters, additive interference, non-additive interference.*

ABSTRACT

Introduction: The annual increase in the transmitted information through communication channels leads to a complication in solving problems of noise immunity. To facilitate the solution of these problems, it is necessary to analyze the concepts of "invariant". This concept is found in all fields of science and therefore it is necessary to consider the various concepts of "invariant" and the authors involved in the study of this problem. To analyze the differences between the concepts of invariance in communication systems and other fields of science. And the question of the difference between the concepts of "tensor" and "matrix" is considered. The matrix description characterizes the fixed value of the object for the selected moment of time, and the tensor description allows you to get a description of the object for all moments of time and, therefore, is more general. If we consider a matrix that describes an object, then this matrix will not be an invariant object. However, often in practice, we need to make a large number of calculations, and often they are of the same type. Tensor methods of calculations are used for this, which leads to a more concise and visual form of representation. **Methods and Results:** To solve the problems of noise immunity of the communication system, it is necessary that the probability of errors on the receiving side does not exceed acceptable values. In communication systems, information passing through a communication channel can be transmitted to a communication channel with constant characteristics or to a communication channel with variable characteristics. If the communication channel is organized with constant characteristics, then the probability of error in this channel is a constant value. And in order to organize the noise immunity of the communication system, it is necessary to design it so that all elements of this communication system are selected, organized and synchronized so that the parameters of the communication system meet the specified requirements. To meet the specified requirements, the communication system can be absolute invariant or relative invariant to additive or non-additive interference. In conclusion, the classification of invariant communication systems according to the work of Yu. B. Okunev is considered.

REFERENCES

1. A.G. Kushner, V.V. Lychagin (2012). Petrov invariance and identification of Hamiltonian systems with a control parameter. *Proceedings of the IX International Conference "Identification of systems and management tasks" SICPRO*, pp. 75-81.

2. F. Klein (1872). Comparative review of the latest geometric studies ("Erlangen Program") in book.: Norden A.P. About the basics of geometry, pp. 399-434.

3. S. Lie (1872). Ueber einige partielle Differential-Gleichunger zweiter Orduung. *Math. Ann*. Vol. 5, pp. 209-256.

4. S. Lie. Begrundung einer Invarianten-Theorie der Beruhrungs-Transformationen. Math. Ann. Vol. 8, pp. 215-303.

5. A.M. Vinogradov, I.S. Krasilshchikov, V.V. Lychagin (1988). Introduction to the geometry of nonlinear differential equations. *Results of science and technology. Series "Modern problems of mathematics. Fundamental directions"*. Moscow: VINITI. Vol. 28. P. 297.

6. A.M. Vinogradov, I.S. Krasil'shchik, V.V. Lychagin (1986). Geometry of jet spaces and nonlinear partial differential equations. *Advanced Studies in Contemporary Mathematics*. New York: Gordon and Breach Science Publishers. P. 441.

7. L.V. Ovsyannikov (1978). Group analysis of differential equations. Moscow: The science. P. 399.

8. A.G. Kushner, V.V. Lychagin, V.N. Rubtsov (2007). Contact geometry and nonlinear differential equations. *Encyclopedia of Mathematics and Its Applications*. Cambridge: Cambridge University Press. P. 496.

9. A.G. Kushner (1998). The Monge-Ampere and e-structure equations. *DAN*. -Vol. 361. No. 5, pp. 595-596.

10. A.G. Kushner (2008). A contact linearization problem for Monge-Amp`ere equations and Laplace invariants. *Acta Appl. Math*. Vol. 101. No. 1-3, pp. 177-189.

11. A.G. Kushner (2010). On contact equivalence of Monge-Amp`ere equations to linear equations with constant coefficients. *Acta Appl. Math*. Vol. 109. No. 1, pp. 197-210.

12. V.V. Lychagin, V.N. Rubtsov, I.V. Chekalov (1993). A classification of Monge-Amp`ere equations. *Ann. Sci. Ecole Norm*. Sup. 4e s. Vol. 26. No. 3, pp. 281-308.

13. G.V. Shchipanov (1939). Теория и методы проектирования автоматических регуляторов. *Automation and telemechanics*. No. 1, pp. 49-66.

14. B.N. Petrov (1983). Selected works. Vol. 1. Theory of automatic control. Moscow: The science.

15. Yu.B. Okunev (1973). Communication systems with invariant noise immunity characteristics. Moscow: Svyaz. 80 p.

16. L.A. Mironovskiy (1991). Invariants of mathematical models : Text of lectures. LIAP. L. P. 32.

17.V.S. Bogdanov, S.V. Bogdanov (2013). Invariants and tensor invariants of networks. *Proceedings of the Volgograd State Technical University*. No. 22 (125), pp. 21-25.

23. The Great Soviet Encyclopedia. (2013) : https://dic.academic.ru/dic.nsf/bse/90347. Date of application: 15.11.2022.

18. B. Daniel (2006). Ennis and Gordon Kindlmann. Orthogonal Tensor Invariants and the Analysis of Diffusion Tensor Magnetic Resonance Images. *Magnetic Resonance in Medicine.* No. 55, pp.136-146.

19. A.E. Petrov (2007). Tensor method of dual networks. Moscow: Center for Information Technologies in Nature Management. P. 496.

20. S.S. Abramov, E.S. Abramova, I.I. Pavlov, M.S. Pavlova (2021). Overview of the basic concepts of invariance in data transmission systems. *Actual problems of infotelecommunications in science and education. X International Scientific-technical and scientific-methodical conference;* collection of scientific articles in 4 vol.; SPb.: SPbGUT. Vol. 1, pp. 29-34.

21. V.V. Lebedyantsev, I.I. Pavlov (2022). Общая методология синтеза систем, инвариантных к неаддитивной помехе. *Actual problems of infotelecommunications in science and education. XI International Scientific-technical and scientific-methodical conference*; collection of scientific articles in 4 vol. SPb.: SPbGUT, 2022. Vol. 1, pp. 654-657.

INFORMATION ABOUT AUTHOR:

Pavlov I. I., Federal state budgetary educational institution of higher education "Siberian state university of telecommunications and informatics" (SibSUTIS), Associate professor of the department of radio engineering devices and technosphere security, associate professor, candidate of technical sciences, Academician of the IAC, Novosibirsk, Russia

For citation: Pavlov I. I. Analysis of the theory and practice of existing invariant communication systems. H&ES Reserch. 2022. Vol. 14. No 6. P. 27-34. doi: 10.36724/2409-5419-2022-14-6-27-34 (In Rus)

doi: 10.36724/2409-5419-2022-14-6-35-39

МЕТОДЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ РАДИОЭЛЕКТРОННЫХ УСТРОЙСТВ

СТОЛБИНСКИЙ Денис Владимирович[1]

БЕМ Павел Петрович[2]

АНДРЕЕВ Вадим Алексеевич[3]

АННОТАЦИЯ

Введение. Современное общество сильно зависит от радиоэлектронных устройств. Они охватывают, как бытовую, так и промышленные сферы жизни общества. Радиоэлектронные устройства (РЭУ) входит в состав современных технологических систем в различных отраслях производства электронного и электротехнического оборудования. Значение и относительный объем РЭУ в технических системах постоянно увеличивается. Это требует создания эффективной контрольно-диагностической аппаратуры, применяемой на этапах испытаний и эксплуатации. Отечественные и зарубежные исследователи изучают методы обеспечения безопасности и надежности работы радиоэлектронных устройств, чем и обусловлена актуальность рассматриваемой темы. **Цель работы** заключается в рассмотрении представлений отечественных и зарубежных исследователях о методах и подходах к обеспечению надежности радиоэлектронных устройств. **Используемые методы:** метод диалектического материализма, метод сравнения и аналогии, а также анализ и синтез собранной информации. Эти методы позволят раскрыть вопросы методологии с позиции отечественных и зарубежных исследователей, а также определить оптимальные подходы, для современных условий распространения радиоэлектроники. Новизна работы заключается в систематизации взглядов отечественных и зарубежных исследователей по проблеме контроля деятельности РЭУ. **Результат:** в статье сделаны выводы о перспективности существующих методов и необходимости дальнейшего изучения данного вопроса. **Практическая значимость:** представленный анализ может быть использован, как основа для прикладных исследований, а также как руководство для предприятий, устанавливающих радиоэлектронные устройства. Использование методологии для оценки требований к надежности РЭУ может предвидеть решения, касающиеся топологии, критичности устройств, уровней избыточности и надежности сети, которые можно использовать для принятия решений в рамках жизненного цикла системы, и в частности, на ранних этапах планирования и проектирования.

Сведения об авторах:

[1] аспирант, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия

[2] аспирант, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия

[3] аспирант, Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Россия

КЛЮЧЕВЫЕ СЛОВА: *радиоэлектронные устройства, надежность аппаратуры, методы контроля.*

Для цитирования: Столбинский Д.В., Бем П.П., Андреев В.А. Методы обеспечения надежности радиоэлектронных устройств // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 35-39. doi: 10.36724/2409-5419-2022-14-6-35-39

Введение

Радиоэлектронные устройства (РЭУ) входит в состав современных технологических систем в различных отраслях производства электронного и электротехнического оборудования. Значение и относительный объем РЭУ в технических системах постоянно увеличивается. Это требует создания эффективной контрольно-диагностической аппаратуры, применяемой на этапах испытаний и эксплуатации. Поэтому, сегодня успешно развивается методология диагностирования и обеспечения надежности РЭУ [1, с.32-41].

Актуальность темы обусловлена рядом факторов. Во-первых, развитие инновационных технологий делает приборы все сложнее, а реализация их функций должна регулироваться постоянно и не всегда это возможно и нужно делать на местах, так как существуют дистанционные методы контроля. Во-вторых, современные методы диагностики и обеспечения безопасности изучаются и дополняются исследователями, как в нашей стране, так и во всем мире. В-третьих, надежность работы РЭУ – залог успешной деятельности во многих отраслях современной жизни, потому интерес к ней постоянно поддерживается.

Целью работы является изучение методов обеспечения надежности РЭУ, с точки зрения отечественных и зарубежных исследователей.

Новизна работы заключается в систематизации взглядов отечественных и зарубежных исследователей по проблеме контроля деятельности РЭУ.

Основными методами исследования, которые были использованы для написания работы, являются:

– метод диалектического материализма (предполагает изучение, исследование категорий (понятий) от простейших к более сложным, базируясь на работах отечественных и зарубежных специалистов, выявили, что обеспечения работы РЭУ являются значимыми и обсуждаются по всему миру);

– метод сравнения и аналогии (опираясь на мнения специалистов можно предположить, какие оптимальные методы необходимо применять при работе с радиоэлектронными устройствами);

– анализ и синтез собранной информации (в рамках исследования были проанализированы работы отечественных и зарубежных авторов, сделаны выводы и приведены результаты анализа собранной информации в форме общих характеристик и умозаключений).

Анализ отечественной литературы

Использование методологии для оценки требований к надежности РЭУ может предвидеть решения, касающиеся топологии, критичности устройств, уровней избыточности и надежности сети, которые можно использовать для принятия решений в течение жизненного цикла системы, и в частности, на ранние этапы планирования и проектирования. Например, в зависимости от топологии могут быть созданы альтернативные пути к приемнику, повышающие общую надежность сети. Таким же образом, если поддерживается анализ чувствительности, могут быть идентифицированы критические устройства и приняты решения о различных подходах к резервированию [2, с.221-228].

Анализ работ отечественных исследователей, показывает, что для обеспечения эффективного функционирования РЭУ при снижении стоимости их жизненного цикла необходимо внедрение средств и методов автоматизированного контроля и диагностики ТК. Также необходимо использовать эффективные методы и средства обеспечения безопасности и надежности эксплуатации устройств [3, с.5-12].

В работе Будько П.А., Виноградено А.М., Меженов А.В. и Заремба В.Е. отмечается, что наряду с известными методами оценивания, необходимо так же опираться на методы мониторинга устройств, статистической классификации, теории нейронных сетей, интеллектуальных агентов. Альтернативой вышеперечисленным методам является сбор и обработка СИ, реализованная в многоуровневых системах мониторинга ТС РЭУ, в которых сбор и обработка МИ осуществляется на основе ее комплексной оценки. Этап сбора СИ представлен в виде передачи и обработки данных о выходе параметров объекта за пределы заданных допусков. Этот этап способствует снижению избыточности СИ, за счет интеграции РСС и ТМС. Такая интеграция в комплексе с классификацией аварий и ошибок проверкой ФПР и ФНР способствует повышению производительности (эффективности) в системе управления. В целом, по мнению авторов, проводимые исследования в области управления ТС РЭУ, распознавания видов отказов и их прогнозирования характеризуются достаточно широким спектром подходов в данной предметной области [4, с.59-70].

Ю. Рыжов, Л. Сакович, Ю. Небесная приводят другие аргументы. Они отмечают, что повышение точности количественного определения показателей надежности РЭУ, возможно за счет использования новой модели, учитывающей время работы отдельных подмножеств элементов объекта в возможных режимах его работы [5]. Как показали исследования Максакова С.А. и Симакова А.Н., это позволяет повысить оценку реального значения комплексного показателя надежности – коэффициента готовности, и, как следствие, снижение значения коэффициента готовности. Использование предложенной модели количественной оценки значений показателей надежности радиоэлектронных устройств с переменной структурой позволяет снизить себестоимость продукции при обеспечении требуемых значений наработки на отказ и среднего времени восстановления за счет снижения требований к надежности базовые элементы [6. С.83-91].

Другой коллектив исследователей рассматривая варианты математических методов расчета надежности РЭУ, указывает на необходимость перехода к автоматизации процесса, а не его удешевление. И.С. Урюпин, А.С. Шалумов, М.В. Тихомиров и Е.О. Першин отмечают, что применение РЭУ необходимо расширять не только на промышленные и бытовые нужды, но также и внедрять оборудование в строительные системы. По мнению авторов такой подход позволит ускорить процесс строительства на этапе возведения несущих конструкций. В то же время исследователи отмечают необходимость организации проверочных работ и методов проверки работы радиоэлектронной аппаратуры [7]. Для этого, как отмечают Куатов Б. Ж., Рыбаков И. М. и Юрков Н. К., можно использовать специализированные программы по расчету

надежности системы АСРН и АСОНИКА-Б, которые предназначены непосредственно для анализа показателей безотказности РЭУ [8. С.9-20].

Следовательно, отечественные специалисты уверены, что на сегодняшний день, методы обеспечения надежности РЭУ не могут концентрироваться на обычных проверках и тестировании. В век инновационных технологий необходимо моделирование, прогнозирование, использование автоматизированных и дистанционных систем проверки и мониторинга [9, 10].

Зарубежные исследователи о методах контроля работы радиоэлектронных устройств

Зарубежные авторы также рассматривают автоматизацию контроля надежности РЭУ, но уверены, что этого недостаточно.

Б. Волочьий, Б. Мандзий, Л. Озирковский в своей работе помимо автоматизации системы контроля расписывают плюсы метода логически-вероятного моделирования, а также метод пути и составление блок-схем при анализе и контроллинге деятельности РЭУ. Основная идея состоит в том, чтобы представить сеть в виде графа и измерить надежность на основе количества функциональных связующих звеньев. Если имеется хотя бы одно функциональное остовное звено, то сеть считается надежной. Предложение простое и очень хорошо работает для анализа механизма управления РЭУ. Однако невозможно использовать и проверять физическую избыточность, а также вычислять критичность устройств. Гибкие условия отказа также очень трудно представить из-за зависимостей отказов для состояния связующего звена [11].

Сильва И., Гедес Л.А., Васкес Ф. предложили еще одну систему проверки. Основная идея состоит в том, чтобы вычислить новый параметр надежности, называемый производительностью, который измеряет вероятность того, что сенсорный узел находится в активном состоянии и способен связаться с приемником в момент времени t . Эта новая мера сочетает в себе надежность сенсорного узла с уровнем заряда батареи. Условия отказа сети связаны с наличием минимального количества сенсорных узлов (k-out-n), способных отправлять данные в приемник. Также авторы предлагают альтернативный подход, основанный на численном подходе. Он предназначен для ослабления некоторых допущений, связанных с аналитическим методом. В той же работе они предлагают использовать звенья отказов для вычисления состояния отказа сети. Условия отказа сети определяются очень строгим образом (k-out-n устройств), что не подходит для промышленных сценариев, где важно идентифицировать неисправное устройство, а не только количество отказавших устройств [12].

К. Ли и Х. Ли говорят о том, что радиоэлектронные устройства, на сегодняшний день, устаревшая система, которая получает новую жизнь в процессе организации работы беспроводных сетей Интернет. Исследователи отмечают, что частота сбоев работы в беспроводных сетях может быть минимизирована за счет правленого использования РЭУ. Важно обслуживать узлы в неисправных ячейках без ухудшения качества обслуживания узлов, включенных в нормальные ячейки. Авторы предлагают практический алгоритм самовосстановления для повышения надежности беспроводной сети с учетом удовлетворенности всех узлов в системах за счет надежной работы РЭУ. Задача оптимизации, целью которой является максимизация пропускной способности системы, может быть сформулирована следующим образом: $I_{m,s}^{[n]} nsm\delta$

$$\max_{\vec{p}\geq 0,\vec{p}} \sum \sum \sum_{n\in N} P^{[n]} \quad {}^{[n]}_{m,n}$$

Следовательно,

$$\text{C1:} \sum \quad P^{[n]} \quad {}^{[n]}_{m,n} \geq r_{min},$$

что применимо к случаю равенства всех узлов;

$$\text{C2: } P_{m,n}^{[n]} \in \{0,1\},$$

устройство будет работать при руководстве одного узла связи;

$$\text{C3:} \sum_{s\in S} P_{m,n}^{[n]} = 1\ ,$$

многоканальная система предполагает наличие узлов под каждый канал радиопередачи;

$$\text{C4: } \sum_{n\in N} P_{m,n}^{[n]} \geq \mathrm{P}_{max},$$

при таких данных необходимо контролировать мощность подачи сигнала.

Здесь, все элементы больше или равны. В приведенном выше уравнении, узлы связи, а также обычные узлы рассматриваются для поддержания надежности, когда РЭУ выполняют распределение ресурсов. Ограничение C1 гарантирует, что все узлы, должны обслуживаться по крайней мере с требуемой скоростью передачи данных. В ограничении C2, если РЭУ назначает подканал узлу. Ограничение C3 указывает, что каждый подканал назначается только одному узлу. Ограничение C4 ограничивает доступную мощность передачи.

Таким образом, авторы, чтобы добиться надежной поддержки узлов как в неисправных, так и в нормальных внутренних ячейках, предложили алгоритм, использующий совместную задачу оптимизации. В результате можно максимизировать пропускную способность системы, гарантируя требуемую скорость узла [13].

Из предыдущего обсуждения становится ясно, что эти работы дают лишь частичное решение проблемы. Поскольку большинство из них сосредоточено на конкретных сценариях, они очень ограничены в отношении определения условий отказа сети, показателей надежности, топологии, реконфигурации сети и аспектов резервирования, а также применимости к промышленным сценариям.

Перспективы обеспечения безопасного функционирования радиоэлектронных устройств

Важно отметить, что РЭУ – это широко распространенная технология, нацеленная на связь между сенсорными узлами в различных средах. Его инфраструктура обычно состоит из большого количества сенсорных узлов небольшого физического размера, работающих на относительно недорогих вычислительных процессах.

Узлы датчиков измеряют локальные условия окружающей среды и передают полученные значения в набор центральных точек, называемых узлами-приемниками, для соответствующей обработки. Узлы связи могут воспринимать

окружающую среду, обмениваться данными с соседними узлами и выполнять базовые вычисления на основе собранных данных. Гибкость установки и простота настройки обеспечивают лучшее удобство использования и обслуживания по сравнению с традиционными коммуникационными технологиями. Эти характеристики позволяют использовать РЭУ в широком диапазоне.

В настоящее время работа и надежность РЭУ основаны на стандартизированных или проприетарных протоколах.

В настоящем, методы обеспечения безопасного функционирования РЭУ должны опираться на дистанционную диагностику. Которая, возможно, может претендовать на роль самого актуального метода обеспечения и контроля надежности РЭУ. Дистанционные методы применяются при пуске, монтаже, тестировании, эксплуатации и обслуживании РЭУ и ТС. Бескабельная система должна быть простой в проектировании, установке и эксплуатации, а ее техническое обслуживание в течение всего срока службы должно быть минимальным. Применяемые «бескабельные» устройства или системы напрямую интегрируются в критически важные системы автоматизации и безопасности. Многие компании из списка Fortune 500 и Fortune 100, а также их производители оригинального оборудования (OEM) начинают устанавливать эти устройства по всему миру [14. С.46-52].

Причина реализации усилий по контролю надежность РЭУ заключается в том, что радиоэлектронные устройства заполняют окружающую среду все чаще и регулярно занимают новые частоты. В какой-то момент, неуправляемые, они могут стать проблемой. Потому, производители все чаще говорят о том, что перед началом эксплуатации, необходимо проводить настройку оборудования. Начинать управление потенциальными помехами от радиоэлектронных устройств или систем, необходимо с проверки среды предприятия на наличие всех источников радиочастот. Далее следует контрольный список элементов для контроля РЭУ, а также то, что необходимо задокументировать при установке оборудования, передатчика/приемника на месте. Рекомендуется учитывать стандартные проектные соображения относительно электромагнитных помех или радиочастотных помех. Недорогие анализаторы радиочастотного спектра доступны у большинства поставщиков РЭУ [15].

При этом, необходимо иметь в виду, что приложения для технологии управления, обеспечения надежности и безопасности РЭУ, являются частью нашей повседневной жизни. Устранение неисправности в цепи передач уже является обыденным и повседневным. А потому, оценка рисков, проведенная сертифицированными специалистами по безопасности, определит ценность дистанционного контроля по сравнению с другими решениями.

Заключение

Подводя итог, можно обобщить мнения зарубежных и отечественных исследователей и выделить дистанционные методы контроля надежности РЭУ. Во-первых, это обусловлено автоматизацией всех сфер жизни общества. Во-вторых, дистанционное регулирование упрощает и удешевляет систему надзора. В-третьих, РЭУ не всегда находятся в легкодоступных местах и потому их обслуживание и контроль надежности их работы может и должен осуществляться дистанционно.

Безусловно, данные статьи не коснулись минусов предлагаемых методов обеспечения надежности РЭУ, что предполагает дальнейшее более глубокое изучение вопроса.

Литература

1. *Мищенко В.И., Демин А.П., Корбут В.А*. Исследование и классификация эксплуатационных факторов, влияющих на обеспечение надежности радиоэлектронных средств вооружения и военной техники // НиКСС. 2021. №3 (35). С. 32-41.

2. *Голубцов С.Г., Аскерко А.В., Милашевский А.В., Легкий А.С.* Методика оценки эффективности функционирования системы (сети) связи специального назначения по показателю устойчивости // Известия ТулГУ. Технические науки. 2021. №9. С. 221-228.

3. *Юрков Н.К.* Современное состояние исследований в области создания высоконадежной бортовой радиоэлектронной аппаратуры // НиКСС. 2021. №4 (36). С. 5-12.

4. *Будко П.А., Виноградено А.М., Меженов А.В., Заремба В.Е.* Метод адаптивного интеллектуального контроля технического состояния радиоэлектронных систем // Техника средств связи. 2019. №4 (148). С. 59-70.

5. *Рыжов Ю.В., Сакович Л.В., Небесная Ю.А*. Оценка надежности радиоэлектронных устройств с переменной структурой. Режим доступа: /https://www.semanticscholar.org/paper/EVALUATION-OF-RELIABILITY-OF-RADIO-ELECTRONIC-WITH-Ryzhov-Sakovich/9b36a6f4662ead84390adb0f571fb4d5c0ae02c2 (дата обращения: 10. 11.2022).

6. *Максаков С.А., Симаков А.Н.* Методика оценки воздействия факторов внешней среды на показатели надёжности радиоэлектронных устройств на этапе проектирования // Известия ТулГУ. Технические науки. 2021. №2. С. 83-91.

7. *Урюпин И.С., Шалумов А.С., Тихомиров М.В., Першин Е.О.* Разработка алгоритма расчета надежности несущих конструкций изделий радиоэлектронной аппаратуры при механических воздействиях. Режим доступа: https://publications.hse.ru/pubs/share/folder/4ordtou7fm/67285287.pdf (дата обращения: 10. 11.2022).

8. *Куатов Б.Ж., Рыбаков И.М., Юрков Н.К.* К проблеме создания цифровых моделей теплонагруженных элементов радиоэлектронной системы // НиКСС. 2022. №1 (37). С. 9-20.

9. *Соколов С.С., Иванов Д.А., Федулов Ю.В., Зобнин А.К.* Функциональная модель устойчивости радиоэлектронных средств в условиях электромагнитных излучений // Известия ТулГУ. Технические науки. 2022. №9. С. 253-261.

10. *Быков А. П., Пиганов М.Н.* Прогнозирование показателей качества бортовых радиоэлектронных устройств // Труды МАИ. 2021. №116. С. 78-97.

11. *Волочьий Б., Мандзий Б., Озирковский Л.* Новые возможности технологии обеспечения надежности радиоэлектронных систем. Режим доступа: https://www.researchgate.net/publication/ 263172302 New_Features_of_Reliability_Engineering_Technology_of_Radioelectronic_Systems (дата обращения: 10. 11.2022).

12. *Сильва И., Гедес Л.А., Васкес Ф.* Оценка надежности и доступности беспроводных сенсорных сетей для промышленных приложений. Режим доступа: https://www.mdpi.com/1424-8220/12/1/806/htm(дата обращения: 10. 11.2022).

13. *Ли К., Ли Х.* Совместное использование радиоресурсов для обеспечения надежности беспроводной сети в Интернет. Режим доступа: https://www.hindawi.com/journals/misy/2015/473763/(дата обращения: 10. 11.2022).

14. *Алёшкин Н.А., Зидерер Ю.Д.* Анализ рисков и угроз в процессе испытаний на электромагнитную совместимость // Новые импульсы развития: вопросы научных исследований. 2021. №2. С. 46-52.

15. *Юнкер Д.* Обеспечение надежности бескабельного управления. Режим доступа: https://www.controleng.com/articles/ensure-cableless-control-reliability/(дата обращения: 10. 11.2022).

METHODS FOR ENSURING THE RELIABILITY OF RADIO ELECTRONIC DEVICES

DENIS V. STOLBINSKY
Samara, Russia

PAVEL P. BEM
Samara, Russia

VADIM A. ANDREEV
Samara, Russia

KEYWORDS: *radio electronic devices, equipment reliability, control methods.*

ABSTRACT

Introduction. Modern society is highly dependent on electronic devices. They cover both household and industrial spheres of society, both in Russia and in foreign countries. Therefore, both domestic and foreign researchers are studying methods for ensuring the safety and reliability of the operation of radio-electronic devices, which determines the relevance of the topic under consideration. The purpose of the work is to consider the ideas of domestic and foreign researchers about the methods and approaches to ensuring the reliability of radio electronic devices. **Methods:** the method of dialectical materialism, the method of comparison and analogy, as well as the analysis and synthesis of the collected information. These methods will allow to reveal the issues of methodology from the position of domestic and foreign researchers, as well as to determine the best approaches for modern conditions for the distribution of radio electronics. The novelty of the work lies in the systematization of the views of domestic and foreign researchers on the problem of monitoring the activities of the PRUE. **Results:** the article will draw conclusions about the prospects of existing methods and the need for further study of this issue. Practical significance: the presented analysis can be used as a basis for applied research, as well as a guide for enterprises installing radio electronic devices.

REFERENCES

1. V.I. Mishchenko, A.P. Demin, V.A. Korbut (2021). Research and classification of operational factors affecting the reliability of radio-electronic weapons and military equipment. No. 3 (35), pp. 32-41.

2. S.G. Golubtsov, A.V. Askerko, A.V. Milashevsky, A.S. Legkiy (2021). Methods for evaluating the effectiveness of the functioning of a special-purpose communication system (network) in terms of stability. Izvestiya TulGU. *Technical science*. No. 9, pp. 221-228.

3. N.K. Yurkov (2021). Current state of research in the field of highly reliable on-board radio electronic equipment. No. 4 (36), pp. 5-12.

4. P.A. Budko, A.M.Vinogradenko, A.V. Mezhenov, V.E. Zaremba (2019). Method of adaptive intelligent control of the technical state of radio electronic systems. No. 4 (148), pp. 59-70.

5. Yu.V. Ryzhov, L.V. Sakovich, Yu.A. Nebesnaya (2022). Reliability assessment of radio electronic devices with variable structure. https://www.semanticscholar.org/paper/evaluation-of-reliability-of-radio-electronic-with-Ryzhov-Sakovich/9b36a6f4662ead84390adb0f571fb4d5c0ae02c2 (accessed 10.11.2022).

6. S.A. Maksakov, A.N. Simakov (2021). Methods for assessing the impact of environmental factors on the reliability indicators of radio electronic devices at the design stage. I*zvestiya TulGU. Technical science.* No.2, pp. 83-91.

7. I.S. Uryupin, A.S. Shalumov, M.V. Tikhomirov, E.O. Pershin (2022). Development of an algorithm for calculating the reliability of load-bearing structures for products of radio-electronic equipment under mechanical influences. https://publications.hse.ru/pubs/share/folder/4ordtou7fm/67285287.pdf (date of access: 10.11.2022).

8. B.Zh. Kuatov, I.M. Rybakov, N.K. (2022). Yurkov On the problem of creating digital models of heat-loaded elements of a radio-electronic system. No. 1 (37), pp. 9-20.

9. S.S. Sokolov, D.A. Ivanov, Yu.V. Fedulov, A.K. Zobnin (2022). Functional model of stability of radio-electronic means under conditions of electromagnetic radiation. *Izvestiya TulGU*. *Technical science*. No. 9, pp. 253-261.

10. A.P. Bykov, M.N. Piganov (2021). Forecasting quality indicators of on-board radio electronic devices. *Proceedings of MAI*. No. 116, pp. 78-97.

11. B. Volochy, B. Mandziy, L. Ozirkovsky (2022). New possibilities of technology for ensuring the reliability of radio electronic systems. https://www.researchgate.net/publication/263172302_New_Features_of_Reliability_Engineering_Technology_of_Radioelectronic_Systems (Accessed 10/11/2022).

12. I. Silva, L.A. Gedes, F. (2022). Vasquez Assessment of the reliability and availability of wireless sensor networks for industrial applications. https://www.mdpi.com/1424-8220/12/1/806/htm (date of access: 10.11.2022).

13. K. Lee, H. Lee (2022). Sharing radio resources to ensure the reliability of a wireless network in the Internet. https://www.hindawi.com/journals/misy/2015/473763/ (date of access: 10/11/2022).

14. N.A. Aleshkin, Yu.D. Ziderer (2021). Analysis of risks and threats in the process of testing for electromagnetic compatibility. *New impulses of development: issues of scientific research*. No.2, pp.46-52.

15. D. Juncker (2022). Ensuring the reliability of cableless control. https://www.controleng.com/articles/ensure-cableless-control-reliability/ (accessed 10/11/2022).

INFORMATION ABOUT AUTHORS:

Denis V. Stolbinsky, Pavel P. Bem, Vadim A. Andreev, PhD students, Samara National Research University named after Academician S.P. Koroleva, Samara, Russia

For citation: Stolbinsky D.V., Bem P.P., Andreev V.A. Methods for ensuring the reliability of radio electronic devices. H&ES Reserch. 2022. Vol. 14. No 6. P. 35-39. doi: 10.36724/2409-5419-2022-14-6-35-39 (In Rus)

doi: 10.36724/2409-5419-2022-14-6-40-52

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СЕТИ БЕСПРОВОДНОГО ШИРОКОПОЛОСНОГО ДОСТУПА СТАНДАРТА 802.16 С ИСПОЛЬЗОВАНИЕМ NETWORK SIMULATION 2 (NS-2)

ЛЕГКОВ
Константин Евгеньевич[1]

АННОТАЦИЯ

Введение. в работе рассмотрен процесс разработки имитационной модели беспроводного широкополосного доступа стандарта 802.16 с использованием Network Simulation 2. Такой подход позволяет быстро построить требуемую модель сети с помощью скриптового языка OTcl без необходимости вникать в структуру компилируемой части ns-2. В случае если необходима модификация или дополнение компилируемой части, это может быть сделано путем добавления (или изменения) C++ кода и перекомпиляции системы. Единственный недостаток такого подхода это трудности при изучении системы и отладке программ (моделей), возникающие вследствие использования двух языков. **Цель исследования:** В работе с использованием симулятора NS-2 необходимо было выявить возможности различных стандартов беспроводного широкополосного доступа, провести и анализ и сравнение. **Результаты:** Для реализации цели исследования был проведен процесс имитационного моделирования. На основании эксперимента было выявлено снижение потери пакетов и времени задержки при применении стандарта 802.16. по сравнению с другими стандартами беспроводного широкополосного доступа. **Практическая значимость:** применение данной модели при проектировании беспроводных сетей позволяет повысить эффективность передачи данных. **Обсуждение:** в качестве дальнейшего исследования требуется детальное рассмотрение влияние современных протоколов передачи данных с использованием имитационной модели.граммного управления, в том числе – реакции разложения или синтез наночастиц из меди и других металлов.

Сведения об авторе:

[1] к.т.н., главный редактор журнала “Наукоемкие технологии в космических исследованиях Земли”, Москва, Россия, ht-esresearch@yandex.ru

КЛЮЧЕВЫЕ СЛОВА: *компьютерное моделирование, инофкоммуникационные сети, беспроводный широкополосный доступ, симулятор, имитационное моделирование.*

Для цитирования: Легков К.Е. Разработка имитационной модели сети беспроводного широкополосного доступа стандарта 802.16 с использованием network simulation 2 (NS-2) // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 40-52. doi: 10.36724/2409-5419-2022-14-5-40-52

Введение

В настоящее время наблюдается активное развитие как инофкоммуникационных сетей, так и услуг, предоставляемых этими сетями [1-5]. Этот процесс требует не только разработки нового технологического оборудования, программных продуктов и стандартов, но и подготовки квалифицированных специалистов. Компьютерное моделирование, как показала практика, играет существенную роль при решении как тех, так и других задач [6-10]. В процессе разработки модель, аппроксимирующая свойства и поведение исследуемой сети, позволяет решать задачи по оптимизации и управлению [11-14]. Апробация тех или иных решений на модели несравнимо дешевле, чем на реальной системе, и позволяет исключить возможные ошибки [15-19].

В процессе разработки имитационной модели сети беспроводного широкополосного доступа стандартов 802.11 и 802.16 был использован программный продукт Network Simulation 2 (ns-2).

Симулятор ns-2 осуществляет имитационное моделирование сети на уровне пакетов, то есть, моделирует генерацию пакетов и прохождение их по сети. На прикладном уровне моделируется характер трафика, порождаемого различными приложениями: Web, FTP, Telnet, RealAudio. Кроме того, имеются абстрактные модели трафика, например Constant Bitrate. Возможно моделирование работы протоколов транспортного уровня UDP и различных реализаций TCP, multicast-протоколов, различных протоколов маршрутизации впроводных и беспроводных сетях, очередей с дисциплинами обслуживания DropTail и RED. Также моделируются некоторые факторы, относящиеся к физическому уровню, такие как задержка пакетов в каналах, возникновение ошибок, видимость/невидимость узлов в беспроводных сетях (как наземных, так и спутниковых), расход энергии батарей в устройствах с автономным питанием.

Результатом работы симулятора ns-2 являются выходные текстовые файлы, в которых регистрируется ход моделирования (моменты генерации/получения пакетов, состояние очередей, отброс пакетов в очередях и т. д.). Кроме того, в модель могут быть включены инструкции, вычисляющие любые величины, измерение которых требуется в конкретной задаче (задержка пакетов, пропускная способность и т. п.). Значения этих величин в ходе моделирования также могут регистрироваться в выходных файлах.

Для визуализации результатов служат аниматор NAM (Network Animator) и построитель графиков Xgraph. Кроме того, система содержит генератор топологий, упрощающий описание топологии больших сетей.

Симулятор ns-2 состоит из двух частей. Одна из них написана на языке C++ и должна быть перекомпилирована в случае внесения изменений и дополнений; другая написана на интерпретируемом языке OTcl (объектно-ориентированное расширение языка сценариев Tcl) и, соответственно, не требует компиляции. При этом иерархии классов в обеих частях имеют совпадающие части и в терминологии ns-2 называются компилируемой и интерпретируемой иерархиями, соответственно. Взаимодействие между частями, написанными на таких принципиально разных языках программирования, осуществляется согласно спецификации, определяющей способ обращения из tcl-сценария (скрипта) к любому методу классов компилируемой иерархии и возвращение назад результатов, а также способ обращения из программы на C++ к любому методу, описанному в Tcl-сценарии. Во втором случае, фактически, интерпретатор языка Tcl вызывается из C++ как функция. По замыслу создателей ns-2, все методы, имеющие дело с отдельными пакетами и потому требующие высокого быстродействия, относятся к компилируемой части. Интерпретируемая часть отвечает за менее частые события, чем передача пакетов, обеспечивающие управление ходом моделирования, и манипуляцию объектами, описанными в компилируемой части. Также, Tcl-скриптом является собственно описание модели сети, подлежащей исследованию.

Такой подход позволяет быстро построить требуемую модель сети с помощью скриптового языка OTcl без необходимости вникать в структуру компилируемой части ns-2. В случае если необходима модификация или дополнение компилируемой части, это может быть сделано путем добавления (или изменения) C++ кода и перекомпиляции системы. Единственный недостаток такого подхода – это трудности при изучении системы и отладке программ (моделей), возникающие вследствие использования двух языков.

Network Simulation 2 разработан для операционных систем Linux, поэтому программный продукт для работы в операционных системах семейства Windows запускается с помощью эмулятора Ubuntu, и эмулятора терминала Xming (рис. 1).

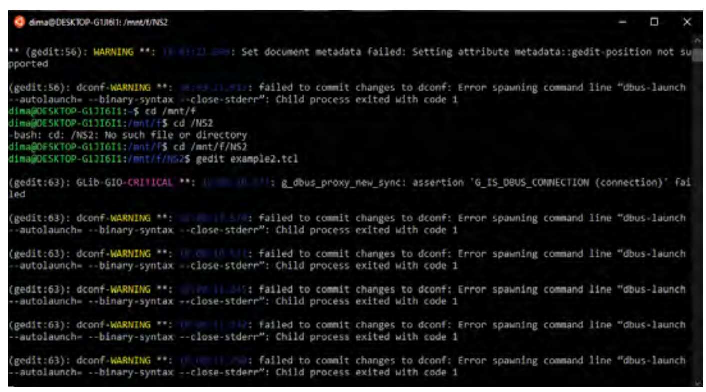

Рис. 1. Окно Ubuntu в ОС Windows 10

Ubuntu имеет вид командной строки, при этом работа в эмуляторе после установки и настройки среды ограничивается двумя командами:

– gedit example.tcl где команда gedit запускает файл example.tcl для редактирования через оболочку Xming (рис. 2);

– s example.tcl запускает файл example.tcl для исполнения.

Xming – это эмулятор терминала X-Windows с открытым исходным кодом (X-сервер), который работает на компьютерах с операционной системой (ОС) Microsoft Windows. Контент Xming позволяет машинам с ОС Windows отображать графические программы для ОС Linux, выполняемые на удаленных серверах с ОС Linux. В дополнение к базовой процедуре установки покажем, как использовать клиентскую программу PuTTY SSH для защиты рабочей фазы терминала X-Window под оболочку Xming (рис. 3).

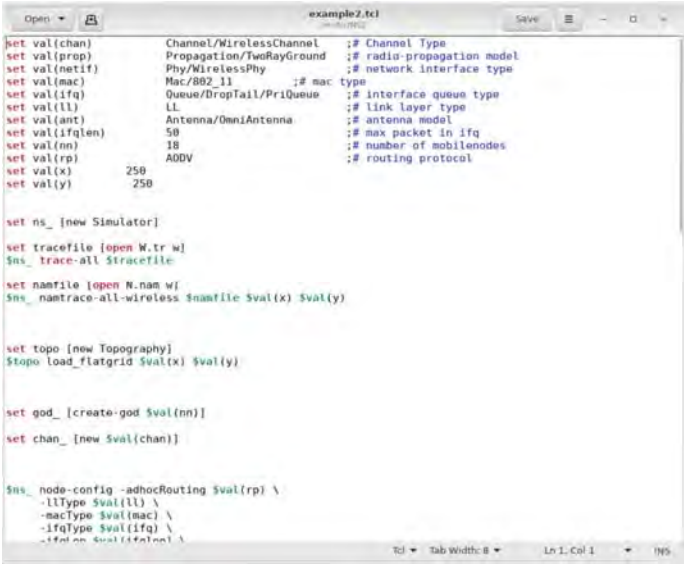

Рис. 2. Xming – эмулятор терминала X-Windows

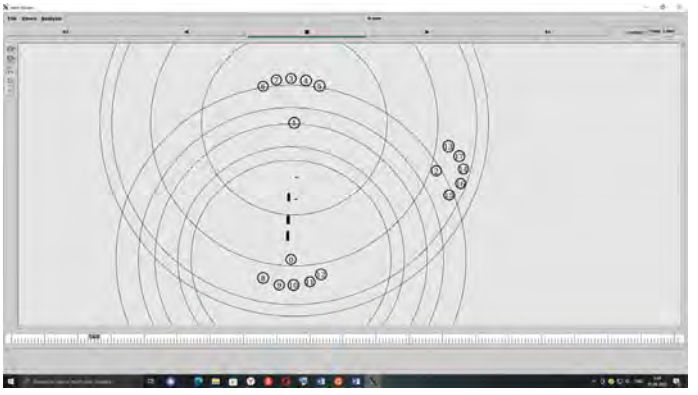

Рис. 3. Внешний вид разработанной модели

После проведения моделирования проводится анализ результатов эксперимента:

1. Визуальный – при помощи файла <mov_wireless.nam>.
2. Аналитический – при помощи файла <graph.tr> и программы Trace Graph, в результате должна быть получена таблица, описывающая общую информацию о сети.
3. Графический – при помощи файла <graph.tr> и программы Trace Graph.

Описание процесса моделирования

Функционирование сети моделируется в виде прохождения по ней потоков требований в виде пакетов, причем эти пакеты в модели представляются транзактами (динамическими модельными объектами, перемещающимися по модели сети). Транзакты генерируются пунктами отправления (отправителями, или источниками) и через сеть доходят до пункта назначения (приемника, или получателя), подвергаясь по пути задержкам в элементах сети. Множества источников и получателей будут задаваться пользователем в составе исходных данных модели как подмножества общего множества узлов сети.

Пример установки потоков трафика между узлами:

```
# TCP connections between node_(0) and node_(1)

set tcp [new Agent/TCP]
$tcp set class_ 2
set sink [new Agent/TCPSink]
$ns_ attach-agent $node_(0) $tcp
$ns_ attach-agent $node_(1) $sink
$ns_ connect $tcp $sink
set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ns_ at 10.0 "$ftp start"
```

Кроме источников и получателей транзактов, стационарными элементами уровневой сети являются также коммутаторы или маршрутизаторы (со своими портами) и каналы (тракты). Они размещаются в узлах (так же как источники и получатели), а каналы (тракты) их соединяют. Пропускные способности каналов и коммутационных портов могут задаваться в составе исходных данных модели.

В момент генерации очередного транзакта (в конкретном узле) определяется его пункт назначения. Прохождение транзакта по сети производится с использованием упрощенной версии известных протоколов RIP, OSPF, а также разработанных на основе методов, обеспечивающих прохождение пакетов требований по кратчайшим маршрутам. Выбирается метрика определения длин маршрутов (количество узлов на маршруте, текущая совокупная длина очередей на маршруте или др.). В процессе модельного прогона производится регулярное измерение длин очередей, и в случае превышения ими заданного (достаточно высокого) уровня, будет индицироваться перегрузка сети, информация об этом доводится до сведения должностного лица (ДЛ, оператора) и прогон модели прекращаться.

Пакетная CS

Уровень CS находится поверх уровня MAC и выполняет следующие функции:

– получает PDU более высокого уровня;
– выполняет классификацию;
– доставляет PDU CS в MAC SAP;
– получает PDU CS от равноправного объекта.

В текущей реализации Packet CS выполняет только классификацию. Метод, используемый для классификации пакетов, зависит от реализации. Также может быть полезно реализовать несколько решений, чтобы найти подходящее соединение. Модель поддерживает определяемые пользователем классификаторы.

Структура класса классификатора

Чтобы реализовать новый классификатор, необходимо создать подкласс класса SDUClassifier и реализовать метод classify (Packet *). SDUClassifier поддерживает приоритет, который можно использовать для указания порядка вызова классификаторов. Чем меньше значение приоритета, тем раньше он будет вызван (значение по умолчанию = 0).

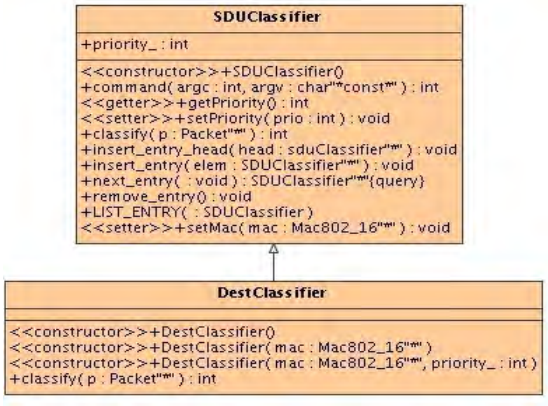

Рис. 4. Диаграмма классов классификатора пакетов

Приоритет должен быть установлен до добавления классификатора в MAC, так как он используется для упорядочения списка классификаторов.

$classifier set-priority $prio

Изменяется приоритет классификатора. Значение по умолчанию – 0.

$mac reset-classifiers

Очищается список классификатора в MAC. Это должно быть вызвано перед добавлением пользовательского классификатора пакетов.

$mac add-classifier $classifier

Добавляется классификатор в список используемых классификаторов пакетов.

Подуровень MAC

В этом разделе представлен подуровень MAC, который в настоящее время поддерживает PMP.

Структура модуля MAC

Mac802.16 является подклассом класса MAC. Это абстрактный класс, который содержит общие элементы BS и MS. Например, он хранит MAC MIB и PHY MIB. Это интерфейс с другими уровнями для отправки и получения пакетов (рис. 5).

MAC имеет список классификаторов пакетов (SDUClassifier), который сопоставляет каждый исходящий пакет с надлежащим идентификатором соединения (CID). Используя TCL, пользователь настраивает список используемых классификаторов. Текущая реализация использует IP-адрес назначения в качестве классифицирующего элемента.

ServiceFlowHandler отвечает за обработку запросов/ответов потока. Он также хранит список потоков для узла.

SS регистрируется в BS, и BS может быть подключен к нескольким SS. Класс PeerNode содержит информацию об одноранговом узле, такую как его соединения и статус. Соединения также доступны через ConnectionManager, который содержит список входящих и исходящих соединений.

Абстрактный класс WimaxScheduler используется для создания интерфейса с MAC. В основном существует два типа планировщиков: один для BS, а другой для SS. Поскольку планировщик указан в TCL, легко реализовать абстрактный класс и изменить его.

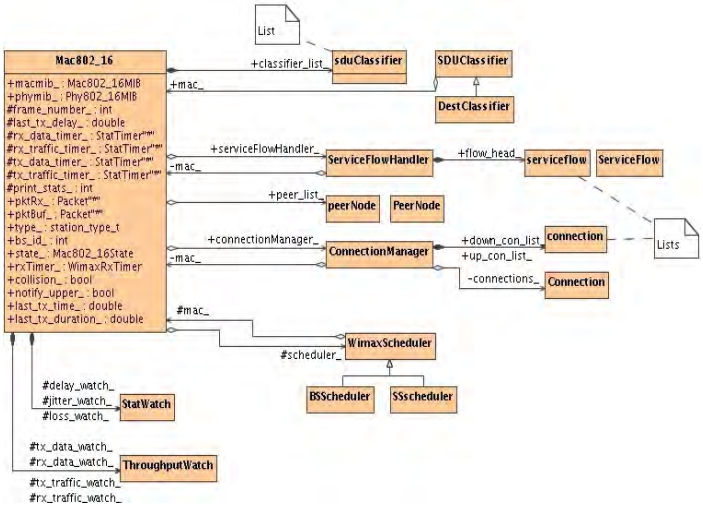

Рис. 5. Диаграмма классов MAC 802.16

Наконец, MAC вычисляет статистику с помощью объектов StatWatch и ThroughputWatch для информации о пакетах и трафике. Значения используются для запуска событий, но их также можно распечатать во время моделирования для последующей обработки.

Поскольку BS и SS имеют разные конечные автоматы, мы определили 2 подкласса, а именно

*Mac802_16BS*и Mac802_16SS, как показано на рисунке 6.

Рис. 6. Классы Mac802_16, Mac802_16BS и Mac802_16SS

Адресация и подключение

Каждый MAC имеет уникальный адрес, закодированный как int, который определен в классе MAC NS-2.

Модель также определяет идентификаторы соединения как int, но в сообщениях они передаются как 16-битные. CID назначаются во время инициализации и динамической настройки соединений.

При инициализации на БС создаются следующие соединения:

– начальный диапазон (входящий и исходящий);

– за олнение (входящее и исходящее);

– трансляция (исходящая);

– адаптивная антенная система (AAS) (исходящая, не используется).

При инициализации на SS создаются следующие соединения:

– начальный диапазон (входящий и исходящий);

– за олнение (входящее и исходящее);

– рансляция (входящая).

Дополнительно при входе в сеть настраиваются следующие соединения и назначаются CID:

– базовый CID (входящий и исходящий);

– первичный CID (входящий и исходящий);

– вторичный CID (входящий и исходящий);

– CID данных.

В настоящее время модель поддерживает только одно подключение для передачи данных.

Формат MAC PDU

Модель определяет новый заголовок для переноса пакетов IEEE 802.16.

Структура заголовка пакета

Диаграмма классов класса hdr_mac802_16 показана на рисунке 7.

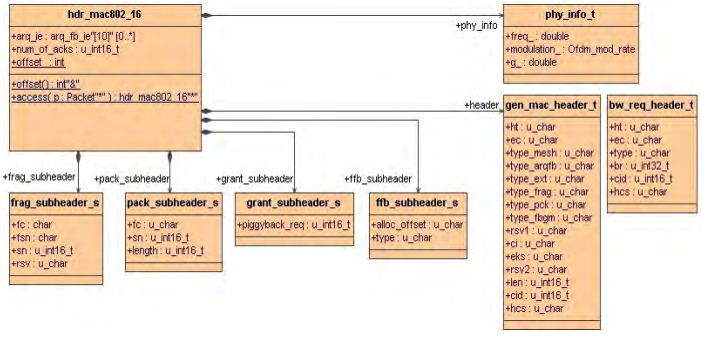

Рис. 7. Диаграмма классов заголовка MAC

Заголовок содержит три основных элемента:

– Виртуальный физический заголовок типа phy_info_t. Эта структура используется для переноса физической информации, такой как частота, модуляция и циклический префикс.

– Общий заголовок MAC типа gen_mac_header_t, содержащий общую информацию MAC. Структура может быть преобразована в bw_req_header_t, когда пакет представляет собой запрос пропускной способности.

– Структуры для хранения различных подзаголовков. Структуры присутствуют во всех пакетах, но атрибут типа общего заголовка указывает, является ли запись допустимой или нет.

Когда ARQ включен, заголовок также содержит информацию обратной связи.

Для сообщений управления MAC полезная нагрузка содержит информацию о переменном размере.

Поскольку не рекомендуется использовать указатели в пакетах, мы реализуем список в виде массивов и включаем количество элементов в списке. При необходимости можно обновить максимальное количество элементов.

В таблице 1 указаны пакеты, определенные в настоящее время в модели. Все определения пакетов находятся в файле mac802_16pkt.h. Для вычисления размера пакета в файле mac802_16pkt.cc реализованы служебные функции.

Таблица 1

Категория	Сообщения определены
Синхронизация	DL-MAP/DCD UL-MAP/UCD RNG-REQ/RSP REG-REQ/RSP
Сервисные потоки	DSA-REQ/RSP/ACK
Мобильность	MOB_NBR_ADV MOB_SCN-REQ/RSP MOB_BSHO-REQ/RSP MON_SSHO-REQ MOB_HO-IND MOB_SCN-REP MOB_ASC-REP

Построение и передача блоков PDU MAC

Построение и передачу пакетов можно разделить на три этапа:

1. Прием исходящего пакета с верхнего уровня: MAC просматривает классификаторы, чтобы найти правильный CID. Если найден допустимый CID, он добавляет заголовок MAC по умолчанию и помещает пакет в очередь соединений.

2. Планирование: каждый кадр планировщики просматривают список соединений, чтобы найти пакеты для передачи. В BS планировщик выполняет распределение пакетов, а затем передает пакеты из очереди соединений в пакеты. В MS он использует полученную карту UL для определения распределения и передачи пакетов в пакеты.

3. Передача: два таймера проходят через DL и UL MAP для передачи пакетов, хранящихся в пакетных очередях.

Фрагментация

Фрагментация может быть включена/отключена в зависимости от соединения. В настоящее время значением по умолчанию является включение фрагментации.

При планировании пакетов для передачи планировщик проверяет, включена ли фрагментация для соединения, и разбивает пакет, чтобы он соответствовал пакету. Контекст фрагментации хранится в файле Connection.

Метод transfert_packets в файле scheduling/wimaxscheduler.cc обеспечивает передачу пакета из очереди соединения в пакеты.

Услуги планирования

Структура класса позволяет указывать различные службы данных, а именно UGS, rtPS, nrTPS и Best Effort. Службы указаны в классе ServiceFlow. Подробную информацию о QoS.

Планирование пакетов осуществляется планировщиком. Этот планировщик взаимодействует с MAC через четко определенный API, позволяющий выполнять индивидуальные реализации.

Планировщики

Для разных типов узлов требуются разные планировщики пакетов. В IEEE 802.16 BS управляет распределением пропускной способности, и существует бесконечное количество реализаций. Модель включает абстрактный класс WimaxScheduler, созданный для простого использования различных планировщиков пакетов. Этот класс уже содержит две реализации: SSscheduler для SS и BSscheduler для BS (рис. 8). Эти планировщики можно заменить с помощью TCL.

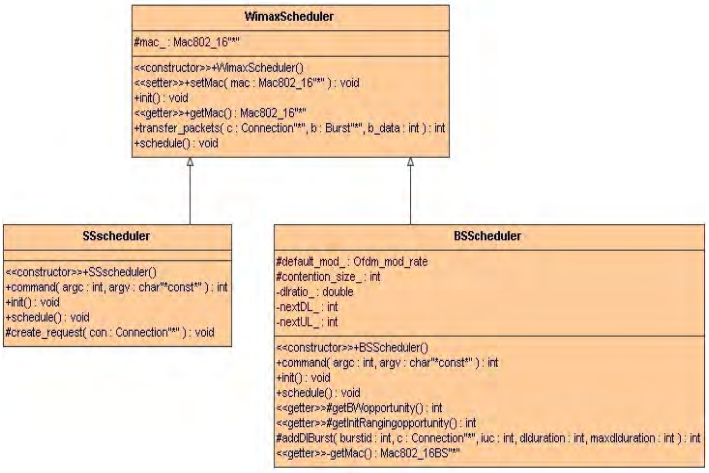

Рис. 8. Диаграмма классов планировщика пакетов

При реализации нового планировщика должны быть реализованы следующие методы:

– *init ()*:: инициализировать планировщик;

– *process (Packet *)*: этот метод используется для обработки пакетов, полученных планировщиком (например, сообщений синхронизации);

– *start_ulsubframe ():* код, который должен выполняться в начале нового подкадра восходящей линии связи;

– *start_dlsubframe ():* код, который должен выполняться в начале нового подкадра нисходящей линии связи.

Подробное описание планировщиков по умолчанию доступно в разделах PHY.

TCL-команды

$mac set-scheduler $scheduler

Установите планировщик MAC. Он удаляет ранее назначенный планировщик, если он присутствует.

Распределение пропускной способности и механизмы запроса

В этом разделе описывается реализация различных механизмов, с помощью которых SS может запрашивать пропускную способность.

Разрешение конфликтов

BS выделяет слоты, подверженные коллизиям, в направлении восходящей линии связи. Эти слоты используются в двух случаях:

– ервоначальный запрос ранжирования;

– запрос пропускной способности.

Модель поддерживает усеченную двоичную экспоненциальную отсрочку для разрешения конфликтов. Сообщения UCD, передаваемые BS, содержат размеры окна (в виде степени двойки). БС также принимает решение о количестве слотов, выделенных в каждом кадре.

На рисунке 9 показана структура класса, используемая для разрешения конфликтов. Подкадр восходящей линии связи содержит BwContentionslot и RngContentionSlot. Оба являются подклассами ContentionSlot, которые предоставляют основные механизмы, связанные с конкуренцией.

Во время входа в сеть SS выполняет определение дальности, чтобы отрегулировать мощность своей передачи. На этом этапе SS генерирует RangingRequest. SS выбирает случайную отсрочку в пределах окон, предоставленных BS, и сохраняет ее. Затем SS уменьшает значение счетчика каждый раз, когда в кадре обнаруживается новый конкурирующий слот. Когда счетчик достигает 0, пакет передается.

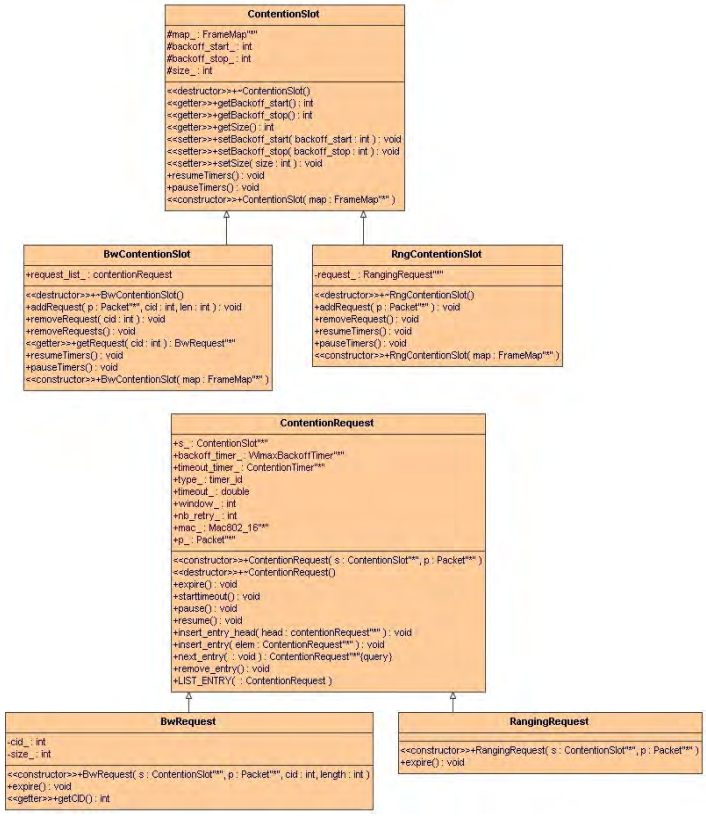

Рис. 9. Конкурентные слоты и конкурирующие запросы

TCL-команды
Mac/802_16rng_backoff_start_2
Mac/802_16rng_backoff_stop_6

Необходимо установить размер окна отсрочки для начальных запросов ранжирования

Mac/802_16bw_backoff_start_2
Mac/802_16bw_backoff_stop_6

Необходимо установить окна отсрочки для запросов пропускной способности

Mac/802_16 set contention_rng_retry_16

Количество повторных передач для отправки запросов на определение дальности.

Mac/802_16 set request_retry_2

Количество повторных передач для запросов пропускной способности.

Окна отсрочки – это параметры MAC, а количество конкурирующих слотов для ранжирования и полосы пропускания – это параметр планировщика BS.

MAC-поддержка PHY

В настоящее время модель поддерживает TDD. В этом режиме передача по восходящей линии связи происходит после нисходящей линии в каждом кадре.

Сообщения DL_MAP и UL_MAP, отправляемые в каждом кадре, определяют распределение пакетов и возможности передачи для каждой станции.

Информация, содержащаяся в UL_MAP, относится к тому же кадру (рис. 10).

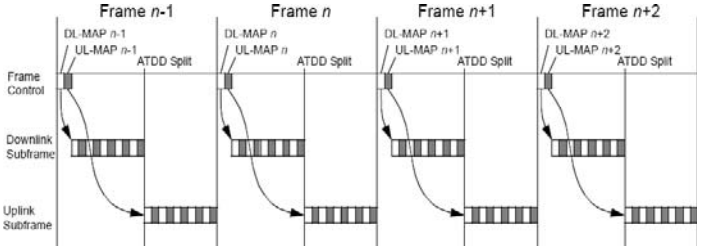

Рис. 10. Релевантность по времени DL_MAP и UL_MAP

Вход в сеть и инициализация

Когда SS хочет присоединиться к сети, ему необходимо выполнить вход в сеть. Модель реализует следующие компоненты входа в сеть:

– сканирование нисходящего канала;
– получение параметров передачи;
– начальное ранжирование;
– регистрация.

Можно настроить следующие параметры:

– та меры для сканирования каналов;
– частота сообщений DCD/UCD;
– параметры для начального ранжирования (размер окна отсрочки и количество слотов на кадр);
– распределение каналов.

Некоторые аспекты реализуются в соответствии с IEEE 802.16e, поэтому вход в сеть может быть уменьшен, если SS получила параметры передачи от обслуживающей BS или во время сканирования.

Ранжирование

Ранжирование – это механизм, позволяющий SS поддерживать хорошее качество связи, регулируя мощность передачи и модуляцию.

Во время начального ранжирования SS включает профиль DIUC по умолчанию для использования при передаче. Это позволяет моделировать узлы, передающие данные с разной скоростью.

В настоящее время не реализован алгоритм, позволяющий использовать возможности измерения дальности. Он используется для добавления дополнительной задержки к сетевой записи. Периодическое ранжирование и запрос CDMA также не реализованы.

TCL-команда:
$mac set-diuc ProfileID ;# 1<= ProfileID <= 11

Необходимо установить профиль для использования MAC. Команда действительна только в MS.

Качество обслуживания

Платформа определяет структуры для поддержки реализации планировщиков, которые используют различные классы обслуживания.

Каждое соединение может быть связано с ServiceFlow и соответствующими параметрами QoS.

Потоки QoS в настоящее время не реализованы в модели NIST. По умолчанию при входе в сеть устанавливается одно соединение для передачи данных в каждом направлении, и для распределения используется BE.

TCL-команды
$mac set-servicehandlerFlowHandler
Замените обработчик потока службы по умолчанию.

Процедуры передачи обслуживания на уровне MAC

Модель поддерживает мобильность уровня 2. В зависимости от конфигурации MS может выполнять сканирование и передачу обслуживания между BS. В этом разделе представлены параметры конфигурации, влияющие на возможность передачи обслуживания.

Сканирование

Когда качество связи ухудшается, MS может послать MOB-SCN_REQ обслуживающей BS, чтобы запросить интервал сканирования с целью обнаружения окружающих BS. На рисунке 11 показана последовательность сообщений во время сканирования, реализованная в модели.

Чтобы инициировать отправку MOB-SCN_REQ, MS отслеживает уровень сигнала входящих пакетов. Когда уровень пересекает порог, отправляется сообщение.

По умолчанию для порога установлено значение RXThreshold, поэтому сканирование не используется. Чтобы включить сканирование, измените атрибут lgd_factor_ MIB на значение больше 1,0. Чем выше значение, тем раньше начнется сканирование.

Рис. 11. Поток обслуживания

Во время сканирования MS собирает значения RSSI входящих пакетов. Эти значения сообщаются обслуживающей БС, которая использует эту информацию для выбора наилучшей целевой БС. После того, как MS получает указание на выбранную BS, она ожидает несколько кадров, прежде чем сообщить о своем намерении выполнить передачу обслуживания. Задержка введена для того, чтобы обеспечить обмен трафиком, буферизованным во время сканирования, перед переключением БС.

Реализованы различные режимы сканирования:

– При сканировании без ассоциации MS пытается идентифицировать и синхронизироваться с одной или несколькими BS. Он также оценивает качество сигнала.

– На уровне ассоциации 0 целевая BS не имеет информации о сканирующей MS и предоставляет только распределения ранжирования на основе конкуренции. После отправки запроса на ранжирование MS ожидает ответа от BS со значением тайм-аута по умолчанию, равным 50 мс.

– На уровне ассоциации 1 обслуживающая БС согласовывает с целевыми БС время, в которое MC найдет выделенную область ранжирования. После отправки запроса на ранжирование MS ожидает ответа от BS со значением тайм-аута по умолчанию, равным 50 мс.

Уровень ассоциации 2 в настоящее время не реализован.

Чтобы разрешить эти различные режимы сканирования и выполнять быструю передачу обслуживания, требуется WiMAXCtrlAgent. WiMAXCtrlAgent — это агент, выполняющий 3 функции. Первый заключается в обмене информацией DCD/UCD между соседними BS. Во-вторых, инициировать отправку сообщений NBR-ADV на MS. Третий — синхронизировать обслуживающую БС и целевую БС при выполнении сканирования уровня 1 или 2. Обмен сообщениями осуществляется по проводным каналам с использованием стандартных IP-пакетов.

TCL-команды

Mac/802_16 set lgd_factor_factor ;# factor >= 1.0

Необходимо установить коэффициент, используемый для генерации ссылки, которая не работает. Когда полученная мощность меньше фактора *RXThresh_, генерируется триггер для запуска сканирования. Чем выше коэффициент, тем быстрее сгенерируется триггер.

Mac/802_16 set scan_duration_50

Необходимо установить количество кадров для сканирования.

Mac/802_16 set interleaving_interval_50

Количество кадров, чередующихся между двумя итерациями сканирования.

Mac/802_16 set scan_iteration_2

Необходимо установить количество итераций для выполнения сканирования.

Mac/802_16 set nbr_adv_interval_0.5 ;#in seconds

Интервал времени между двумя сообщениями MOB_NBR-ADV

Mac/802_16 set scan_req_retry_3

Необходимо установить количество повторных передач для MOB_SCAN-REQ

Agent/WimaxCtrl set debug_0 ;#set to 1 to print debug

Указывает, следует ли печатать отладочную информацию о контроллере сканирования.

Agent/WimaxCtrl set adv_interval_1.0 ;# in seconds

Необходимо установить временной интервал между обменами информацией DCD/UCD между соседними BS.

Этот обмен осуществляется с использованием магистральной сети.

Agent/WimaxCtrl set default_association_level_0

Установите используемый уровень сканирования. Информация включена в сообщение MOB_SCAN-RSP, отправляемое BS на MS.

Agent/WimaxCtrl set synch_frame_delay_ 50;#

Задержка обработки между приемом MOB_SCAN-REQ и отправкой MOB_SCAN-RSP, когда требуется синхронизация с целевыми BS.

Каркасная структура

Схема, используемая для представления кадра, очень похожа на структуру, определенную в IEEE 802.16 для TDD. Кадр (класс FrameMap) содержит подкадр нисходящей линии связи и восходящей линии связи (абстрактный класс SubFrame, классы DlSubFrame и UlSubFrame). Сами подкадры разделены на интервалы PHY PDU.

В каждом из этих интервалов полоса пропускания выделяется пакетами (абстрактный класс Burst, класс UlBurst и класс DlBurst) для разных станций. Каждый из этих пакетов может иметь различную модуляцию и частоту, называемую профилем (класс Profile).

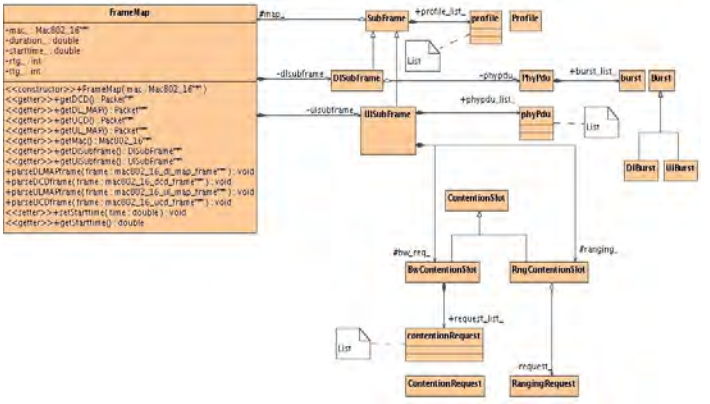

Рис. 12. Диаграмма классов кадров

Обычно БС выделяет пропускную способность станции для передачи своих данных. В некоторых случаях, как правило, при начальных запросах диапазона и полосы пропускания, SS должны конкурировать друг с другом за доступ к среде. Эти интервалы (класс ContentionSlot) присутствуют только в восходящей линии связи, поскольку BS имеет полный контроль над трафиком нисходящей линии связи.

Класс FrameMap также содержит методы для извлечения и анализа управляющих сообщений. В BS планировщик создает структуру карты в соответствии с алгоритмом распределения, а затем вызывает функции getDL_MAP, getUL_MAP, getDCD и getUCD для извлечения пакетов, содержащих необходимую информацию для отправки на SS.

На SS планировщик вызывает обратные функции parseDL_MAP, parseUL_MAP, parseDCD и parseUCD для воссоздания структуры данных, необходимой для правильного приема и передачи пакетов.

Пакетная обработка

На рисунке 13 показаны потоки пакетов для входящих и исходящих пакетов.

Пакет, полученный от верхнего уровня, классифицируется с использованием зарегистрированных классификаторов. Поскольку классификаторов может быть несколько, MAC обращается к ним один за другим, пока не будет найден действительный CID. или все классификаторы были протестированы. Если CID действителен, пакет добавляется в соответствующую очередь, в противном случае он отбрасывается.

При получении нового пакета, т. е. его первого бита, выполняются шаги, показанные на рисунке 13. По окончании приема пакет обрабатывается PHY.

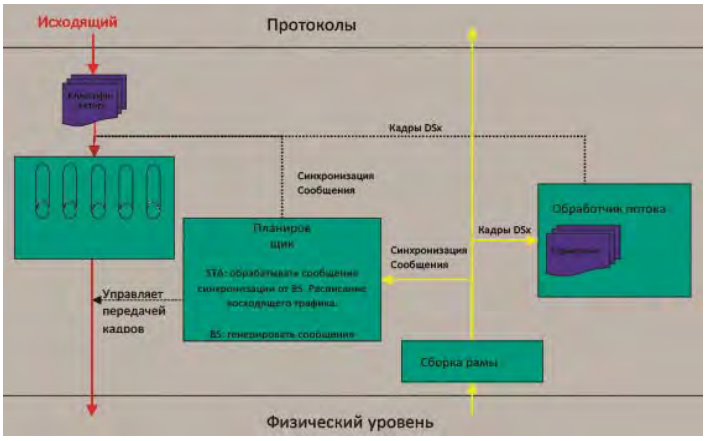

Рис. 13. Обзор обработки пакетов

BS-планировщик

Планировщика пакетов для БС можно настроить с помощью следующих команд:

set scheduler [new WimaxScheduler/BS]

Создает планировщик пакетов для BS.

$scheduler set-contention-size $size

Необходимо установить количество конкурирующих слотов, которые будут выделены для начальных запросов диапазона и пропускной способности в каждый кадр.

Планировщик реализует планировщик Best-Effort в сочетании с алгоритмом циклического перебора для распределения пропускной способности между пользователями.

Для поддержки BE на SS генерируются запросы пропускной способности, указывающие объем данных для передачи.

Соотношение между подкадрами нисходящего и восходящего каналов фиксировано и настраивается через TCL.

WimaxScheduler/BS set dlratio_0.3

Указывает, что 30% кадра предназначено для нисходящей линии связи, а 70% – для восходящей.

Планировщик также позволяет пользователям иметь различные модуляции.

$scheduler set-default-modulation $modulation

Он устанавливает модуляцию, используемую для начальных интервалов запросов диапазона и пропускной способности. Пакеты профилей создаются по умолчанию следующим образом:

Имя профиля	Модуляция
DIUC_PROFILE_1, UIUC_PROFILE_1	OFDM_BPSK_1_2
DIUC_PROFILE_2, UIUC_PROFILE_2	OFDM_QPSK_1_2
DIUC_PROFILE_3, UIUC_PROFILE_3	OFDM_QPSK_3_4
DIUC_PROFILE_4, UIUC_PROFILE_4	OFDM_16QAM_1_2
DIUC_PROFILE_5, UIUC_PROFILE_5	OFDM_16QAM_3_4
DIUC_PROFILE_6, UIUC_PROFILE_6	OFDM_64QAM_2_3
DIUC_PROFILE_7, UIUC_PROFILE_7	OFDM_64QAM_3_4

Пользователь может выбрать пакетный профиль для использования с помощью TCL, используя следующее:

[$SSWithWiMax set mac_(0)] set-diuc 7

По умолчанию профиль (модуляция) одинаков для ОБА нисходящей линии связи и восходящей линии связи.

SS планировщик

set scheduler [new WimaxScheduler/SS]

Создает планировщик пакетов для SS.

Конфигурация TCL

Phy/WirelessPhy/OFDM set g_0 ;# cyclic prefix

Установлен циклический префикс для использования. Допустимые значения: 0,25 (1/4), 0,125 (1/8), 0,0625 (1/16), 0,03125 (1/32). При увеличении циклического префикса накладные расходы увеличиваются, что снижает максимальную пропускную способность.

Mac/802_16 set fbandwidth_5e+6 ;# frequency bandwidth (MHz)

Настроена полоса пропускания частот. Установка более высокой пропускной способности увеличивает пропускную способность.

Mac/802_16 set rtg_state 10 ;# number of PS to switch from receiving to transmitting

Время, необходимое для переключения с приема на передачу. Увеличение значения уменьшает максимально достижимая пропускная способность.

Mac/802_16 set ttg_state 10 ;# number of PS to switch from transmitting to receiving

Время, необходимое для переключения с передачи на прием. Увеличение значения уменьшает максимально достижимое значение пропускной способности.

Mac/802_16 set channel_0 ;# channel number

Выбран канал для использования. Это настраивается на MAC и передается на физический уровень. Необходимо установить его на БС. MS будет сканировать каналы для обнаружения окружающих BS.

Конфигурация

Чтобы начать использовать модель IEEE 802.16 в симуляциях, необходимо выполнить несколько шагов.

Настройка узла

Уровни MAC и физический уровеньзадаются с помощью метода node-config в TCL:

$BSWithWiMax node-config
-macType Mac/802_16/BS
-phyType Phy/WirelessPhy/OFDM

$SSWithWiMax node-config
-macType Mac/802_16/SS
-phyType Phy/WirelessPhy/OFDM

Настройка классификатора пакетов

В IEEE 802.16 пакеты, полученные уровнем MAC от верхних уровней, классифицируются, чтобы направить их на соответствующее соединение. Модель предлагает классификатор на основе MAC-адреса назначения и типа пакета.

 # Create classifier
set classifier [new SDUClassifier/Dest]# Set the classifier priority
$classifer set-priority 1
 # Retrieve the MAC layer and delete all registered classifiers [$nodeWithWiMax set mac_(0)] reset-classifiers
 # Retrieve the MAC layer and set classifier [$node-WithWiMax set mac_(0)] add-classifier $classifier

К MAC добавляется классификатор по умолчанию (DestClassifier). Чтобы добавить изменение классификатора, необходимо сбросить список и добавить новый классификатор.

Настройка планировщика

Для обеспечения гибкости уровень MAC может использовать различные типы планировщиков. В основном есть один для базовых станций (BS) и один для абонентских станций (SS).

Для BS следующий код TCL устанавливает планировщик

 # Create scheduler
set scheduler [new WimaxScheduler/BS] # Add scheduler
[$nodeWithWiMax set mac_(0)] set-scheduler $scheduler

Этот планировщик создается автоматически при создании базовой станции MAC 802.16. Для SS необходимо использовать следующее

 # Create scheduler
set scheduler [new WimaxScheduler/SS] # Add scheduler
[$nodeWithWiMax set mac_(0)] set-scheduler $scheduler

Этот планировщик теперь создается автоматически при создании MAC 802.16 SS.

Настройка канала

Чтобы обеспечить многосотовую топологию, уровни MAC могут работать на разных частотах. Чтобы установить частоты, пользователь может установить номер канала для MAC.

 # Retrieve the MAC layer and set classifier
[$nodeWithWiMax set mac_(0)] set-channel 1 #valid 0-4

Статистика

Некоторые статистические данные собираются на уровне MAC. Следующая команда используется для отображения их значений во время моделирования.

Mac/802_16 set print_stats_true

Отслеживание

Модель IEEE 802.16 вводит новые значения в файл трассировки. Появляются две новые причины отбрасывания пакета:

– CID: этот код причины используется, когда пакет, полученный на уровне MAC, не может быть сопоставлен ни с одним соединением.

– QWI: у каждого соединения есть очередь для хранения ожидающих кадров. Когда очередь заполнена, пакет отбрасывается с использованием этого кода причины.

– F G: указывает на ошибку при передаче фрагмента.

Введен новый тип пакета. Иногда БС необходимо обмениваться данными для целей синхронизации. Новый агент под названием Agent/WimaxCtrl обрабатывает эту связь и отправляет пакеты, помеченные как WimaxCtrl.

Примечание о трассировках при использовании фрагментации:

Если трассировка MAC включена и используется фрагментация, фрагменты будут отображаться как отправленные, но не полученные. В последнем фрагменте весь пакет может быть декодирован и передан на верхний уровень, который затем создаст запись трассировки на стороне получателя. Например, рассмотрим пакет размером 1520 байт, который будет фрагментирован на четыре фрагмента по 396, 396, 396 и 364 байта. Файл трассировки будет содержать четыре записи «отправить» для каждого из фрагментов, но только одну запись «получено» размером 1520 байт для всего пакета.

Таблица 2

Результаты моделирования

Параметры качества функционирования	**УСЛУГИ в сетях WiMAX**			
	VoIP	**Видеосвязь**	**ПД**	**Видео**
Скорость передачи	128 Кбит/с	300 Кбит/с	256 кБит/с	3 Мбит/с
Поток трафика	В реальном масштабе времени	Изменяемый, пакетами	Non-real time, bursty	Изменяемый
Общее число сгенерированных пакетов	2433337	2434585	254323	234344
Число ретранслированных пакетов	2433337	2434585	254323	234344
Число недоставленных пакетов	178	435	112	341
Средняя задержка	0,1276279901	0,1749320837	0,1122044363	0,1744543423
Максимальная задержка	0,17423	0,23435	0,17491	0,29045
Вероятность своевременной передачи сообщения	0,99	0,99	0.99	0,99
Потери пакетов	< 1%	<1% для аудио; <2% для видео	Нет	< 10-8
Изменение времени задержки	< 20 мсек	< 2 сек	Не приемлемо	< 2 сек
Время задержки	< 100 мсек	< 250 мсек	Гибкое	< 100 мсек

Заключение

В работе рассмотрен процесс разработки имитационной модели беспроводного широкополосного доступа стандарта 802.16 с использованием Network Simulation 2. С использованием симулятора NS-2 необходимо было выявить возможности различных стандартов беспроводного широкополосного доступа, провести анализ и сравнение. Для реализации цели исследования был проведен процесс имитационного моделирования. На основании эксперимента было выявлено снижение потери пакетов и времени задержки при применении стандарта 802.16.

По сравнению с другими стандартами беспроводного широкополосного доступа. Применение данной модели при проектировании беспроводных сетей позволяет повысить эффективность передачи данных. В качестве дальнейшего исследования требуется детальное рассмотрение влияние современных протоколов передачи данных с использованием имитационной модели.

Литература

1. *Буренин А.Н., Легков К.Е.* Обеспечение эффективного функционирования информационных подсистем автоматизированных систем управления сложными организационно-техническими объектами на основе процедур оперативного управления ресурсами информационных служб // Информация и космос. 2017. №3. С. 64-72.

2. *Гмурман В.Е.* Теория вероятностей. Математическая статистика. М.: Высшая школа, 2004. 480 с.

3. *Барабаш П.А., Воробьев С.П., Курносов В.И., Советов Б.Я.* Информационные технологии в глобальной информационной инфраструктуре. СПБ.: ООО «Наука», 2008. 552 с.

4. *Буренин А.Н., Легков К.Е., Боговик А.В.* Модели систем телекоммуникаций современной системы связи специального назначения // Технологии информационного общества. X Международная отраслевая научно-техническая конференция: сборник трудов. 2016ю. С. 209-210.

5. *Буренин А.Н., Легков К.Е.* К вопросу мониторинга параметров, характеризующих состояние инфокоммуникационной системы специального назначения // Технологии информационного общества. X Международная отраслевая научно-техническая конференция: сборник трудов. 2016. С. 211-212.

6. *Буренин А.Н., Легков К.Е., Боговик А.В.* Моделирование процедур поддержки процессов организационного управления системами специального назначения // Технологии информационного общества. X Международная отраслевая научно-техническая конференция: сборник трудов. 2016. С. 215-216.

7. *Легков К.Е., Буренин А.Н.* Модели и методы оперативного мониторинга информационных подсистем перспективных автоматизированных систем управления // Информация и космос. 2016. № 4. С. 46-60.

8. *Буренин А.Н., Нестеренко О.Е., Ледянкин И.А., Легков К.Е.* Алгоритм оценивания целесообразности распараллеливания вычислительной задачи // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2016. № 1. С. 68-71.

9. *Буренин А.Н., Легков К.Е., Емельянов А.В.* Основные положения системного анализа и подход к построению модели информационной подсистемы инфокоммуникационной системы специального назначения // Системы синхронизации, формирования и обработки сигналов. 2016. Т. 7. № 3. С. 17-23.

10. *Буренин А.Н., Нестеренко О.Е., Легков К.Е.* К вопросу моделирования процесса мониторинга параметров управления инфокоммуникационных сетей специального назначения // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2015. № 1. С. 60-63.

11. *Буренин А.Н., Легков К.Е.* К вопросу моделирования процессов управления качеством функционирования инфокоммуникационных сетей специального назначения // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2015. № 1. С. 63-67.

12. *Васильев В.А., Буренин А.Н., Легков К.Е.* Модели управления качеством функционирования инфокоммуникационных сетей специального назначения // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2015. № 1. С. 84-88.

13. *Буренин А.Н., Легков К.Е., Емельянов А.В.* Модели организации управления процессами файлового обмена в инфокоммуникационных сетях специального назначения // Труды Ростовского государственного университета путей сообщения. 2015. № 3. С. 5-11.

14. *Легков К.Е.* Основные подходы к управлению процессами функционирования сложных инфокоммуникационных систем // Вестник воздушно-космической обороны. 2015. № 4. С. 69-75.

15. *Буренин А.Н., Легков К.Е., Нестеренко О.Е.* Основные положения управления контентом специального назначения // Системы синхронизации, формирования и обработки сигналов. 2015. Т. 6. № 4. С. 210-212.

16. *Старцев Д.В., Легков К.Е.* Анализ современных компьютерных сетей и среды передачи данных // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 111-114.

17. *Кудрявцев Д.Ю., Легков К.Е.* Состав и способы защиты сетей на основе технологии long term evolution // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 261-264.

18. *Федоров А.Е., Легков К.Е.* Моделирование упреждающего и реагирующего протоколов маршрутизации в беспроводной мобильной адаптивной сети // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 362-365.

19. *Легков К.Е.* К вопросу о самоорганизации, самовосстановлении и самодиагностики распределенных сетей специального назначения // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 62-65.

DEVELOPMENT OF A SIMULATION MODEL OF AN 802.16 WIRELESS BROADBAND ACCESS NETWORK USING NETWORK SIMULATION 2 (NS-2)

KONSTANTIN E. LEGKOV
Moscow, Russia

KEYWORDS: *computer modeling, foreign communication networks, wireless broadband access; simulator; simulation modeling.*

ABSTRACT

Introduction: the paper considers the process of developing a simulation model of wireless broadband access of the 802.16 standard using Network Simulation 2. This approach allows you to quickly build the required network model using the OTcl scripting language without having to delve into the structure of the compiled part of ns-2. If modification or addition of the compiled part is necessary, this can be done by adding (or changing) the C++ code and recompiling the system. The only drawback of this approach is the difficulties in studying the system and debugging programs (models) arising from the use of two languages. **The purpose of the study:** In the work using the NS-2 simulator, it was necessary to identify the capabilities of various wireless broadband access standards, to conduct both analysis and comparison. **Results:** In order to realize the purpose of the study, a simulation modeling process was carried out. Based on the experiment, a decrease in packet loss and delay time was revealed when using the 802.16 standard. compared to other wireless broadband access standards. **Practical significance:** the use of this model in the design of wireless networks makes it possible to increase the efficiency of data transmission. **Discussion:** As a further study, a detailed consideration of the impact of modern data transmission protocols using a simulation model is required.

REFERENCES

1. A.N. Burenin, K.E. Legkov (2017). Ensuring the effective functioning of information subsystems of automated control systems for complex organizational and technical objects based on procedures for operational management of resources of information services. *Information and space*. No. 3, pp. 64-72.

2. V.E. Gmurman (2004). Probability theory. Mathematical statistics. Moscow: Higher School. 480 p.

3. P.A. Barabash, S.P. Vorobyov, V.I. Kurnosov, B.Ya. Sovetov (2008). Information technologies in global information infrastructure. St. Petersburg: Nauka LLC. 552 p.

4. A.N. Burenin, K.E. Legkov, A.V. Bogovik (2016). Models of telecommunication systems of the modern special-purpose communication system. *Technologies of the information society. X International Industry Scientific and Technical Conference: a collection of works*, pp. 209-210.

5. A.N. Burenin, K.E. Legkov (2016). On the issue of monitoring parameters characterizing the state of a special purpose

infocommunication system. *Information society technologies. X International Industry Scientific and Technical Conference: proceedings*, pp. 211-212.

6. A.N. Burenin, K.E. Legkov, A.V. Bogovik (2016). Modeling of procedures for supporting organizational management processes of special purpose systems. *Information society technologies. X International Branch Scientific and Technical Conference: proceedings*, pp. 215-216.

7. A.N. Burenin, K.E. Legkov (2016). Models and methods of operational monitoring of information subsystems of advanced automated control systems. *Information and Cosmos.* No. 4, pp. 46-60.

8. A.N. Burenin, O.E. Nesterenko, I.A. Ledyankin, K.E. Legkov (2016). Algorithm for evaluating the feasibility of parallelization of computing tasks. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 68-71.

9. A.N. Burenin, K.E. Legkov, A.V. Emelyanov (2016). The main provisions of system analysis and an approach to building a model of the information subsystem of a special purpose infocommunication system. *Synchronization systems, signal generation and processing*. Vol. 7. No. 3, pp. 17-23.

10. A.N. Burenin, O.E. Nesterenko, K.E. Legkov (2015). On the issue of modeling the process of monitoring control parameters of special purpose infocommunication networks. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 60-63.

11. A.N. Burenin, K.E. Legkov (2015). On the issue of modeling quality management processes of functioning of special purpose infocommunication networks. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 63-67.

12. V.A.Vasiliev, A.N. Burenin, K.E. Legkov (2015). Models of quality management of functioning of special purpose infocommunication networks. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 84-88.

13. A.N. Burenin, K.E. Legkov, A.V. Emelyanov (2015). Models of organization of management of file exchange processes in special purpose infocommunication networks. *Proceedings of the Rostov State University of Railways*. No. 3, pp. 5-11.

14. K.E. Legkov (2015). Basic approaches to managing the processes of functioning of complex information and communication systems. *Bulletin of Aerospace Defense*. No. 4, pp. 69-75.

15. A.N. Burenin, K.E. Legkov, O.E. Nesterenko (2015). Basic provisions of special purpose content management. *Synchronization systems, signal generation and processing*. Vol. 6. No. 4, pp. 210-212.

16. D.V. Startsev, K.E. Legkov (2014). Analysis of modern computer networks and data transmission media. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 111-114.

17. D.Yu. Kudryavtsev, K.E. Legkov (2014). Composition and methods of network protection based on long term evolution technology. *Proceedings of the North Caucasus branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 261-264.

18. A.E. Fedorov, K.E. Legkov (2014). Modeling of proactive and responsive routing protocols in wireless mobile adaptive network. *Proceedings of the North Caucasus branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 362-365.

19. K.E. Legkov (2014). On the issue of self-organization, self-healing and self-diagnosis of distributed special purpose networks. *Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics*. No. 1, pp. 62-65.

INFORMATION ABOUT AUTHOR:

Konstantin E. Legkov, Ph.D., editor-in-chief of H&ES Research, Moscow, Russia

For citation: Legkov K.E. Development of a simulation model of an 802.16 wireless broadband access network using network simulation 2 (NS-2). *H&ES Reserch*. 2022. Vol. 14. No 6. P. 40-52. doi: 10.36724/2409-5419-2021-14-6-40-52 (In Rus)

doi: 10.36724/2409-5419-2022-14-6-53-57

ИСПОЛЬЗОВАНИЕ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ СИСТЕМ РАДИОСВЯЗИ

НАЙДЕНОВА
Юлия Игоревна[1]

САФАРЬЯН
Ольга Александровна[2]

АЛФЕРОВА
Ирина Александровна[3]

РЕШЕТНИКОВА
Ирина Витальевна[4]

Сведения об авторах:

[1] студент группы МБИС11, Донской Государственный Технический университет, Ростов-на-Дону, Россия, alicefoxmur@mail.ru

[2] к.т.н, доцент, доцент кафедры "Кибербезопасность информационных систем", Донской Государственный Технический университет, Рос-тов-на-Дону, Россия, safari_2006@mail.ru

[3] старший преподава-тель кафедры "Кибербезопасность информационных сис-тем", Донской Государственный Технический университет, Ростов-на-Дону, Россия, a.alferova.donstu@yandex.ru

[4] к.т.н, доцент кафедры "Инфокоммуникационных технологий и систем связи", Северо-Кавказский филиал ордена Трудового Красного Знаме-ни ФГБОУ ВО "Московский технический университет связи и информатики", г. Ростов-на-Дону, Россия irina_reshetnikova@mail.ru

АННОТАЦИЯ

Введение. Функционирование телекоммуникационных систем и сетей определяет практически все стороны развития науки и техники, процессы и явления, протекающие в обществе. В свою очередь, качество функционирования телекоммуникационных систем и сетей обеспечивается развитием технологий передачи и обработки информации. **Целью работы** является разработка экспертной системы на основе модели системы контроля технического состояния генераторов сигналов в инфотелекоммуникационных системах. **Методы и результаты исследования:** В статье разработана динамическая экспертная система (ЭС) на основе модели системы контроля технического состояния генераторов сигналов в телекоммуникационных системах. В предлагаемой системе принятие решений основывается на постоянном анализе параметров частотно-временных параметров сигналов, формируемых генераторами в инфотелекоммуникационных системах. В ходе работы было проведён анализ экспертных систем, была выбрана динамическая экспертная система из класификации по связям с реальным временем, предложена структура экспертной системы, рассмотрен каждый из её элементов, разработана экспертная система, которая позволяет прогнозировать изменение параметров генераторов передающих каналов в телекоммуникационных системах, а также проведено тестирование полученной экспертной системы на основе двух предположений, которое позволяет сделать выводы о корректности разработки. Для этого приводится результат обработки входных данных на основе двух предположений - закона нормального распределения и равномерного закона распределения. На основании этого можно сделать вывод о работоспособности предложенного разработанного варианта построения ЭС и реализующего ее программного продукта. Экспертная система даёт возможность анализа поступающих данных в текущем времени, а также формирования вывода.

КЛЮЧЕВЫЕ СЛОВА: *телекоммуникационная сеть, экспертная система, система искусственного интеллекта, классификация экспертных систем, генераторы, сигналы.*

Для цитирования: Найденова Ю.И., Сафарьян О.А., Алферова И.А., Решетникова И.В. Использование экспертных систем для повышения надежности систем радиосвязи // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 6. С. 53-57. doi: 10.36724/2409-5419-2022-14-6-53-57

Введение

Функционирование телекоммуникационных систем и сетей определяет практически все стороны развития науки и техники, процессы и явления, протекающие в обществе. В свою очередь, качество функционирования телекоммуникационных систем и сетей обеспечивается развитием технологий передачи и обработки информации.

Высокая эффективность функционирования современных телекоммуникационных сетей, характеризуемая значительным объёмом обрабатываемого трафика и высокой скоростью передачи данных, достигается путем соответствия всех параметров системы требуемым значениям и, прежде всего, соответствия частотно-временных параметров сигналов номинальным значениям, определяемыми протоколами обмена. Условием обеспечения указанного требования является наличие системы, которая позволила бы гибко реагировать на изменения параметров систем связи и восстанавливать ее характеристики.

Непрерывный мониторинг, диагностирование, а также прогнозирование изменения параметров позволяют не только определить текущее техническое состояние телекоммуникационной сети, но и сформировать прогноз её изменения [1]. При неточном определении значений одного из параметров возможны результаты, при которых происходит смещение оценок всех частотно-временных параметров сигнала.

С учетом сложности решаемых в указанной постановке задач одним из возможных подходов для проведения мониторинга, диагностирования и прогнозирования технического состояния телекоммуникационных систем может являться использование методов искусственного интеллекта (ИИ), в частности экспертных систем (ЭС) [2].

Целью статьи является разработка экспертной системы на основе модели системы контроля технического состояния генераторов передающих каналов в телекоммуникационных системах.

Методы и результаты исследования

Экспертные системы возникли как результат [3]:

– с одной стороны, большого объема практического использования методов искусственного интеллекта при решении задач определения состояния сложных систем в условиях априорной неопределенности части данных о состоянии системы и ее параметрах;

– с другой стороны, большого числа теоретических результатов, полученных в рамках множества научных дисциплин, которые изучают методы решения задач интеллектуального характера с использованием электронной вычислительной машины.

Первый вопрос, решаемый при представлении знаний – это вопрос о том, что будет в себе хранить база знаний. Второй вопрос касается вида хранения фактов в базе знаний, так как существуют различные виды хранения фактов в базе знаний, это либо суждения, либо формулы, которые при обработке, будут выдавать параметры и рассматриваться вхождение параметра в некоторый диапазон.

Экспертная система представляет собой набор программ, выполняющий функции эксперта при решении задач из некоторой предметной области [4]. Существуют различные классификации экспертных систем, одной из которых является классификация по связи с реальным временем.

Принято считать три её разновидности:

– статичес ая;

– квазидинамическая;

– динамичес ая.

Так как динамическая экспертная система работает в сопряжении с датчиками в режиме реального времени с непрерывной интерпретацией получаемых данных, именно она и была выбрана для построения экспертной системы мониторинга, диагностики и прогнозирования.

Структура динамической экспертной системы состоит из:

– пользовательской подсистемы, которая формирует данные для определения текущих значений;

– рабочей памяти, которая хранит исходные и промежуточные данные в текущий момент задачи;

– базы знаний, содержащей хранение фактов, которые были описаны экспертом, описывающих рассматриваемую предметную область.

Помимо фактов, база знаний может в себя включать:

– процедурную часть, позволяющую реализовывать множество функций и процедур, реализующие расчетные алгоритмы;

– подсистемы принятия решений, анализирующей полученные значения в соответствии с фактами, расположенными в базе знаний.

Для формирования текущего состояния и прогноза изменения характеристик необходимо определить закон изменения их значений, который из-за большого числа воздействующих факторов следует рассматривать как реализацию случайного процесса во времени.

Принятие решений системой искусственного интеллекта (СИИ) основывается на постоянном анализе оценок параметров сигналов генераторов, получаемых с использованием многомерной функции правдоподобия, связывающей между собой значения измеряемых фаз сигналов и текущие характеристики частоты генераторов, такие как средняя частота и относительная нестабильность формируемых сигналов, а также их изменение с течением времени [5].

Для формирования функции правдоподобия используется ЭС, в которой реализованы следующие операции:

– измерение текущих значений фаз сигналов генераторов;

– моделирование на основе предполагаемых законов распределения значений фаз сигналов генераторов;

– вычисление функционалов в виде суммы по числу измерений квадратов разностей между измеренными значениями фаз сигнала и смоделированными на основе соответствующего закона распределения;

– выбор в качестве действительного закона распределения текущих значений частоты генераторов закона, которому соответствует наименьшее значение минимума функционала;

– выбор в качестве оценки отклонения длительности временного интервала измерений значения, соответствующего аргументу минимума выбранного функционала.

Алгоритм, реализующий предлагаемую последовательность операций, приведен на рисунке 1.

Рис. 1. Алгоритм обработки результатов мониторинга параметров телекоммуникационной системы

После составления архитектуры проекта и рассмотрения всех возможных блоков экспертной системы проводится разработка ее структурной схемы. Результат разработки показан на рисунке 2.

Рис. 2. Структурная схема экспертной системы

Для реализации данной системы, необходимо более точно проработать алгоритм работы каждого блока экспертной системы [6].

При оценке частотно-временных параметров сигналов входными значениями для работы ЭС являются следующие величины [7]:

– число генераторов, формирующих сигналы для передачи информации в телекоммуникационной системе;

– номинальные значения частоты каждого генераторов;

– номинальная относительная нестабильность частоты генераторов;

– оличество измерительных интервалов;

– номинальная длительность интервала.

После ввода входных значений производится обработка параметров в решателе, где для каждого из предполагаемых законов распределения, нормального или равномерного, производится моделирование текущего значения частоты сигнала генератора, моделирование длительности текущего интервала измерений, моделирование измеряемой фазы сигнала генератора, необходимых для дальнейшей работы ЭС [8].

На основе полученных результатов для различных законов распределения вычисляются значения функционалов. Каждый функционал определяется как сумма по числу измерений квадратов разностей между измеренными значениями фаз сигнала и смоделированными на основе соответствующего закона распределения. В качестве оценки длительности временного интервала измерений, текущего значения частоты генераторов выбираются соответствующие параметры того закона распределения, для которого минимум функционала будет меньше. Математическое представление функционала имеет вид

$$L(\delta t) = \frac{\sum_{n=0}^{N} \frac{\left(\Phi_n - \Phi_n^{(0)} - \omega_n^{(0)} \cdot \delta t\right)^2}{2\sigma_0^2 \cdot t_0^2}}{\sum_{n=0}^{N} \frac{\left(\omega_n^{(0)}\right)^2}{2\sigma_0^2 \cdot t_0^2}}, \quad (1)$$

где Φ_n и $\Phi_n^{(0)}$ – измеренное и номинальное значение фазы n -го сигнала соответственно; $\omega_n^{(0)}$ – номинальная частота n-го сигнала; δt – предполагаемое отклонение длительности временного интервала измерений от номинального значения t_0.

На основе данных, которые поступают из подсистемы приобретения знаний, в подсистеме принятия решений организуется:

− мониторинг технического состояния каждого генератора в телекоммуникационных системах,

− диагностика, в результате которой определяются значения параметров в телекоммуникационных системах

− прогнозирование по результатам последовательных измерений на каждом интервале, позволяет дать вероятностное изменение параметров генераторов.

В статье проведен анализ функционирования ЭС при оценивании текущего значения частоты генераторов, отклонения которой, после оценки, подчинены нормальному закону.

Исследования проводились при следующих исходных данных:

– ч сло генераторов – 1000;

– номинальные значения частоты генераторов $2 \cdot \pi \cdot 10^9$ рад/с;

– номинальная относительная нестабильность частоты генераторов 10^{-7};

– оличество измерительных интервалов 100;

– номинальная длительность интервала 10^{-3}.

На основании выбранных для оценки законов распределения – нормального и равномерного, параметры которых (математическое ожидание и дисперсия), которые определялись по результатам измеренных значений частоты генераторов,

получили результат обработки, представленный на рис. 3. Сплошной линией показано значение функционала для нормального закона распределения отклонений текущих значений частоты генераторов от средних значений, штриховой линией – для равномерного закона распределения.

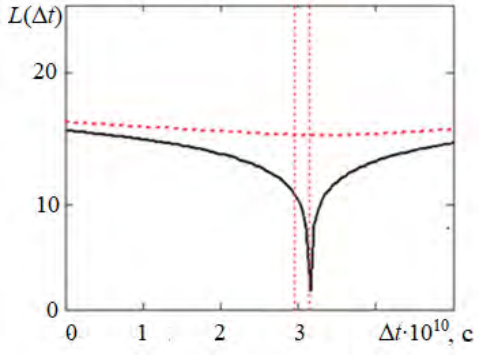

Рис. 3. Результат обработки на основе двух предположений

Выполненный анализ показал, что при выборе в качестве предполагаемого закона распределения, совпадающего с исследуемым законом распределения, минимум получаемого функционала будет меньше, и получаемое при этом значение отклонения оценки длительности временного интервала измерений от действительного значения также будет меньше, чем для любого другого закона распределения [9].

В частности, при моделировании было получено, что минимальное значение функционала, соответствующего нормальному закону распределения, составляет $-1.3 \cdot 10^{-10}$, при равномерном законе распределения $-1.4 \cdot 10^{-10}$. При этом отклонение оценки длительности временного интервала измерений в точке минимума функционала, соответствующего нормальному закону распределения, равно $-5 \cdot 10^{-10}$отклонение оценки длительности временного интервала измерений в точке минимума функционала, соответствующего равномерному закону распределения, равно $-4{,}9 \cdot 10^{-10}$.

Заключение

По результатам моделирования можно сделать вывод, что при исследовании текущих значений частоты генераторов и длительности временного интервала измерений может использоваться ЭС, в которой реализованы следующие операции:

– измерение текущих значений фаз сигналов, формируемых в телекоммуникационной системе;

– моделирование на основе предполагаемых законов распределения значений частот тестовых сигналов генераторов;

– вычисление функционалов в виде суммы по числу измерений квадратов разностей между измеренными значениями фаз сигнала и смоделированными на основе соответствующего закона распределения частот тестовых сигналов;

– выбор в качестве действительного закона распределения текущих значений частоты генераторов закона, которому соответствует наименьшее значение минимума формируемого функционала;

– выбор в качестве оценки отклонения длительности временного интервала измерений значения, соответствующего аргументу минимума выбранного функционала.

На основании этого можно сделать вывод о работоспособности предложенного разработанного варианта построения ЭС и реализующего ее программного продукта. Экспертная система даёт возможность анализа поступающих данных в текущем времени, а также формирования вывода.

Литература

1. *Сафарян О.А., Найденова Ю.И.* Практическое применение динамической экспертной системы (ЭС) на основе модели системы контроля технического состояния генераторов передающих каналов в источниках телекоммуникаций // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики. Сборник научных трудов II международной научно-практической конференции. Екатеринбург, 2022. С. 69-71.

2. *Габриелян Д.Д., Кульбикаян Б.Х., Костенко П.И., Сафарян О.А.* Искусственный интеллект в системе мониторинга, диагностики и прогнозирования технического состояния радиотехнических систем // Вестник Ростовского государственного университета путей сообщения. 2021. № 4. С. 91-99.

3. *Козлов А.Н.* Интеллектуальные информационные системы: учеб. Издательство ФГБОУ ВПО Пермская государственная сельскохозяйственная академия, 2013. 278 с.

4. *Боровская Е.В., Давыдов Н.А.* Основы искусственного интеллекта: учеб. М.: Лаборатория знаний, 2020. 130 с.

5. Экспертные системы. Принципы работы и примеры / под ред. Р. Форсайт. М.: Радио и связь, 2009. 224 с.

6. *Веденов А.А.* Моделирование элементов мышления. М.: Наука, 2009. 160 с.

7. *Любарский Ю.Я.* Интеллектуальные информационные системы. М.: Наука, 2015. 228 с.

8. *Сафарян О.А., Костенко П.И., Пилипенко И.А.* Использование нечеткой логики в системе управления радиомаяками навигационно-посадочного комплекса // Радиолокация, навигация, связь. Материалы XXVII Международной научно-технической конференции, посвященной 60-летию со дня рождения Ю.А. Гагарин и Г.С. Титова. В 4-х томах. Воронеж, 2021. С. 46-52.

9. *Балдин К.В., Башлыков В.Н., Рукосуев А.В.* Теория вероятностей и математическая статистика: Учебник. М.: Дашков и К, 2016. 472 с.

10. *Лорье Ж.-Л.* Системы искусственного интеллекта. М.: Мир, 2009. 568 с.

USING EXPERT SYSTEMS TO IMPROVE THE RELIABILITY OF RADIO COMMUNICATION SYSTEMS

JULIA I. NAYDENOVA
Rostov-on-Don, Russia

OLGA A. SAFARYAN
Rostov-on-Don, Russia

IRINA A. ALFEROVA
Rostov-on-Don, Russia

IRINA V. RESHETNIKOVA
Rostov-on-Don, Russia

KEYWORDS: *telecommunication network, expert system, artificial intelligence system, classification of expert systems, generators, signals.*

ABSTRACT

Introduction. The article develops a dynamic expert system (ES) based on a model of a system for monitoring the technical condition of signal generators in telecommunication systems. In the proposed system, decision-making is based on a constant analysis of the parameters of the time-frequency parameters of signals generated by generators in infotelecommunication systems. **The purpose of the work** is to develop an expert system based on a model of a system for monitoring the technical condition of signal generators in infotelecommunication systems. **Research results:** In the course of the work, an analysis of expert systems was carried out, a dynamic expert system was selected from the real-time communication classification, the structure of the expert system was proposed, each of its elements was considered, an expert system was developed that allows predicting changes in the parameters of transmission channel generators in telecommunication systems, and the resulting expert system was tested based on two assumptions, which allows us to draw conclusions about the correctness of the development. For this purpose, the result of processing the input data is given based on two assumptions – the law of normal distribution and the uniform distribution law. On the basis of this, it can be concluded that the proposed developed version of the ES construction and the software product implementing it is working. The expert system makes it possible to analyze incoming data in the current time, as well as generate an output.

REFERENCES

1. O.A. Safaryan, Yu.I. Naydenova (2022). Practical application of a dynamic expert system (ES) based on a model of a system for monitoring the technical condition of transmitting channel generators in telecommunication sources. Infocommunication technologies: topical issues of the digital economy. *Collection of scientific papers of the II international scientific-practical conference*. Edited by V.P. Shuvalov. Comp. M.P. Karacharova. Yekaterinburg, pp. 69-71.

2. D.D. Gabrielyan, B.Kh. Kulbikayan, P.I. Kostenko, O.A. Safaryan (2021), Artificial intelligence in the system of monitoring, diagnostics and forecasting of the technical condition of radio engineering systems. *Bulletin of the Rostov State University ways of communication*. No. 4, pp. 91-99.

3. A.N. Kozlov (2013). Intelligent information systems. Perm: Publishing House of FGBOU VPO Perm State Agricultural Academy. 278 p.

4. E.V. Borovskaya, N.A. Davydov (2020). Fundamentals of Artificial Intelligence. Moscow: Knowledge Laboratory. 130 p.

5. Expert systems. Principles of operation and examples / ed. R. Forsyth. Moscow: Radio and communication, 2009. 224 p.

6. A.A. Vedenov (2009). Modeling of the elements of thinking. Moscow: Nauka. 160 p.

7. Yu.Ya. Lyubarsky (2015). Intelligent information systems. Moscow: Nauka. 228 p.

8. O.A. Safaryan, P.I. Kostenko, I.A. Pilipenko (2021). The use of fuzzy logic in the control system of radio beacons of the navigation and landing complex, in the collection: Radio location, navigation, communication. *Proceedings of the XXVII International Scientific and Technical Conference dedicated to the 60th anniversary of Yu.A. Gagarin and G.S. Titova*. In 4 volumes. Voronezh, pp. 46-52.

9. K.V. Baldin, V.N. Bashlykov, A.V. Rukosuev (2016). Theory and Mathematical Statistics: Textbook. Moscow: Dashkov i K. 472 p.

10. J.-L. Laurier (2009). Artificial intelligence systems. Moscow: Mir. 568 p.

INFORMATION ABOUT AUTHORS:
Julia I. Naydenova, Don State Technical University, Rostov-on-Don, Russia
Olga A. Safaryan, Don State Technical University, Rostov-on-Don, Russia
Irina A. Alferova, Don State Technical University, Rostov-on-Don, Russia
Irina V. Reshetnikova, North Caucasus branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia

For citation: Naydenova Ju.I., Safaryan O.A., Alferova I.A., Reshetnikova I.V. Using expert systems to improve the reliability of radio communication systems. H&ES Reserch. 2022. Vol. 14. No 6. P. 53-57. doi: 10.36724/2409-5419-2022-14-6-53-57 (In Rus)

CONTECH 2022: ПЛАНОМЕРНОЕ ДВИЖЕНИЕ К ИМПОРТОЗАМЕЩЕНИЮ КОНТЕНТА И ТЕХНОЛОГИЙ

АЛЕКСЕЙ ЖДАНОВ

В Москве 9 ноября 2022 года состоялась VII ежегодная конференция "ConTech 2022. Контент и технологии для цифрового ТВ в России". Эксперты, собранные организаторами форума – TMT Conference, "Телеспутником" и TelecomDaily – поделились опытом успешного импортозамещения иностранного контента, профессиональных и потребительских технологий в сфере медиателекома, обозначив при этом проблемные области, требующие дальнейшей консолидации усилий рыночных игроков и государства.

В этом году конференция ConTech 2022 была организована в коллаборации с World Content Market 2022 – международным рынком телевизионного и цифрового контента. Этим был обусловлен повышенный интерес слушателей к потоку, посвященному анализу ситуации с контентом в платном ТВ и на OTT-платформам.

Технологическая сессия также собрала заинтересованную аудиторию, активно включившуюся в диалог о перспективах импортозамещения программных и аппаратных продуктов, используемых для производства и распространения цифрового контента.

Генеральный партнер конференции – мультиплатформенный оператор Триколор; партнер сессии, посвященной семейному контенту – телекомпания "Первый ТВЧ". Также партнерами конференции выступили: "Медиалогистика" (проект компании MSK-IX), "НТВ-Плюс", GS Labs, EPG Service и NLE. Конференция прошла при поддержке Ассоциации Анимационного Кино и Международной Академии Связи. На площадке мероприятия собралось более 200 делегатов, онлайн-трансляция собрала более 100 зрителей.

Дефицита контента нет

Центральной темой пленарной дискуссии "Индустрия цифрового ТВ в России: регулирование, тренды, ресурсы, прогнозы, инсайты" стали предварительные итоги года. Эксперты подтвердили, что уход из России крупнейших американских правообладателей не привел к серьезному дефициту контента. Телеканалы и онлайн-платформы увеличивают объем предложения прежде всего российского контента, дополняя его южнокорейской и турецкой продукцией. Большинство экспертов согласились, что именно турецкие сериалы сейчас занимают топовые позиции по смотрению как в платном ТВ, так и в OTT. Комментируя этот тезис, заместитель генерального директора ВГТРК Александр Нечаев высказал мнение, что популярность турецких и корейских сериалов связана с временным отказом каналов ВГТРК от показа сериальных мелодрам. "Мы видим невероятный рост популярности турецких мелодрам и корейских дорам. Мы это связываем не с тем, что они внезапно стали популярны, а с тем, что ВГТРК как главный производитель мелодрам в стране временно ушла с этого поля, потому что переключилась на информационные и квазиинформационные жанры. Дефицит этого продукта для подсевшего на него как на приятный расслабляющий релаксант народонаселения, особенно женского, стал очень высок. Как только мы выйдем обратно на этот рынок с over-предложением мелодрам, уровень суперпотребления турецких и корейских мелодрам и дорам снизится до привычного, потому что российские мелодрамы нашему зрителю привычнее и понятнее", – отметил замглавы ВГТРК.

Из слов директора по развитию видеосервиса Wink Антона Володькина следует, что вымывание голливудского контента привело к оттоку его приверженцев с легальных платформ на пиратские, но сейчас эта аудитория возвращается. "Мы интуитивно [до ухода голливудских мейджоров] купили очень много контента, понимая, что зрителей надо чем-то развлекать. Смотрят Турцию, Азию и независимых иностранных мейджоров. Это дало приток новой аудитории – потребителей российских сериалов, которые не нашли их на каналах ВГТРК. Но нельзя сказать, что те, кто был лоялен западному контенту, переключились на турецкие сериалы. Эти люди в моменте ушли в "серую" зону. Но поскольку пользоваться пиратскими ресурсами неудобно, а мы много всего скупили, статистика стала выглядеть как пациент, который смиряется с неизлечимой болезнью. Сначала он не признает российский контент, потом думает о нем, а в итоге смотрит сериалы Бондарчука и других прекрасных режиссеров на платформах. Качество российского контента улучшилось", – рассказал директор по развитию Wink.

Директор департамента цифровых продуктов "НТВ-Плюс" Константин Смирнов выделил категорию зрителей, которых российские легальные платформы все-таки потеряли. Это спортивные болельщики, лишившиеся трансля-

ций ведущих зарубежных чемпионатов. "Фанаты "Манчестер Юнайтед" не переключатся на "Ярославский шинник", – подчеркнул Константин Смирнов.

Комментируя меры господдержки, в которых нуждается медиаотрасль, директор по маркетингу Триколора Алексей Липилин высказался за распространение льгот, которыми пользуются ИТ-компании, на компании сферы медиа. "Мы чувствуем поддержку государства, но у нас основную помощь получает ИТ-отрасль. При этом компании, работающие в медиаотрасли, хотят, чтобы меры поддержки всё же были сходными. Прежде всего, речь идет о льготах по страховым взносам, НДС. Возможно, государство обратит внимание на то, что медиаотрасль нуждается в подобной поддержке. Нам бы это очень помогло", – отметил Алексей Липилин.

В ходе Public Talk "Линейное ТВ в онлайн-кинотеатрах: эксперименты с контентом или "новая нормальность"? Антон Володькин и заместитель генерального директора по контенту онлайн-кинотеатра "Иви.ру" Иван Гринин обменялись мнениями о том, как за счет линейных телеканалов удержать и расширить аудиторию онлайн-сервисов. Эксперты сошлись во мнении, что линейные телеканалы, прежде всего тематические, которые видеосервисы включают в свою контентную матрицу, позволяют расширять аудиторию, которая дополняет потребление VoD линейным телесмотрением. Поскольку ТВ-канал вещает безостановочно, пользователю не нужно тратить время на поиск нужного контента. Кроме того, удобству зрителей отвечает возможность конверсивности VoD и линейного просмотра.

Еще одним важным выводом Public Talk стала констатация необходимости серьезных вложений сервиса в развитие линейного вещания на его платформе. По словам Ивана Гринина схема "20 каналов мультиплекса плюс один канал" на практике не работает. Представители "Иви.ру" и Wink согласились, что необходимо стремиться к наполнению пакетов линейных каналов, так, чтобы их число приближалось к пакетам крупных кабельных или спутниковых операторов – более 150. Wink реализует именно такой подход – в его пакетах более 300 каналов. В то же время Иван Гринин посетовал, что требование закона получать сигнал 20 общедоступных каналов на платформе "Витрина ТВ" резко сужает возможность монетизировать линейное телесмотрение. В этой связи Иван Гринин предложил отрасли продолжать доводить до регулятора позицию о негативном эффекте по сути монопольного вещания каналов мультиплексов в онлайне через единую платформу, добиваясь пересмотра этого требования.

К технологической независимости в медиателекоме

Эксперты сессии технологического потока "Назад в будущее: станет ли импортонезависимость драйвером развития рынка цифрового ТВ?" рассматривали последствия санкций и ухода из России зарубежных вендоров, технологические возможности операторов и импортозамещение ПО для медиаизмерений.

"С отечественным софтом все хорошо, с оборудованием – все плохо. Мы используем как зарубежное ПО, так и отечественное. Это не связано с событиями этого года, так исторически сложилось. Но любое ПО должно работать на сервере. С серверами есть определенные проблемы", – поделился директор проекта "Медиалогистика" (MSK-IX) Григорий Кузин. Он также высказал мнение, что в текущем году самым безопасным каналом доставки медиаконтента становятся выделенные оптико-волоконные линии, тогда как риски спутниковой доставки и каналов общедоступного интернета существенно выросли.

Руководитель службы новых продуктов Триколора Валерий Петров представил новый продукт под брендом "Триколор" – линейку телевизоров Смарт ТВ, состоящую из четырех моделей с диагоналями 32, 43, 50 и 55 дюймов. Все модели, за исключением 32-дюймовой, поддерживают разрешение Ultra HD, "младшая" модель в линейке имеет разрешение HD. Телевизоры от Триколора работают на базе операционной системы Android 11, имеют оперативную память 1,5 Гб и 8 Гб, что позволяет просматривать потоковое видео и устанавливать приложения. Все телевизоры адаптированы для работы в сетях спутникового, кабельного и эфирного телевидения, оснащены двухдиапазонным Wi-Fi, разъемами HDMI и USB, слотами CI для CAM-модуля. На телевизоры предустановлено фирменное приложение "Триколор Кино и ТВ", а все покупатели телевизора в фирменном интернет-магазине получают годовую подписку на сервисы Триколора.

О полной готовности дистрибуторской сети NLE к выводу на рынок телевизоров с брендом "Триколор" заявила ведущий специалист по развитию и продвижению NLE Светлана Сафиулина. По ее словам, каналы поставок NLE в новых условиях работают надежно и стабильно, и дистрибутор продолжает расширять ассортимент товаров, ориентированных на монтажные организации на рынке платного ТВ и салоны соответствующего оборудования. Благодаря сотрудничеству с российскими и китайскими производителями складские запасы NLE постоянно пополняются, при этом дистрибутор успешно адаптировался к изменению логистических маршрутов.

Председатель комитета по стратегическому развитию медиапроектов при совете директоров Триколора Николай Орлов рассказал о новых приложениях, разработанных независимыми специалистами. Оценить работу приложений смогут пользователи гибридных приёмников. Оператор приглашает к сотрудничеству софтверные компании. Поскольку речь идет о полноценном стартапе, в Триколоре готовы обсуждать с разработчиками условия монетизации приложений.

Отвечая на вопрос о рисках несанкционированных подключений и взломов вещания телеканалов и OTT-платформ, начальник отдела продаж GS Labs Роман Хлопов высказался за отказ от небезопасных вещательных технологий зарубежных вендоров и переход на российское ПО и оборудование, внесенное в соответствующие реестры Минцифры и Минпромторга.

Опытом перехода на российское ПО для гибридных медиаизмерений поделился директор департамента специальных проектов "Агентства 2" Денис Белослюдов. По его словам, перспективы гибридных измерений связаны с необходимостью нивелировать ограничения, присущие панельным и онлайн-измерениям, сохраняя сильные стороны того и другого метода и добиваясь их синергии. Поскольку в России не было ПО для задач анализа телесмотрения - как для панельных исследований, так и гибридных, в "Агентстве 2" приняли решение заказать разработку по собственному техническому заданию у российской софтверной компании. К настоящему моменту медиаизмеритель уже начал использовать новое российское ПО в своей работе и готов получать гибридные данные в интересах телеканалов, дистрибуторских компаний и игроков рекламного рынка.

Больше семейного контента

Сессия "Семейный просмотр: каким должен быть телеконтент, который объединяет и старших, и младших?" собрала наибольшую аудиторию в ходе конференции, поскольку ее участники сконцентрировались на актуальной теме создания телепроектов для разных поколений телезрителей.

Директор по производству контента Триколора Марина Гаспарян привлекла внимание участников сессии к новому каналу в линейке фильмовых телеканалов собственного производства оператора – Scream.

Сетка нового канала, который начал свое вещание в конце октября, включает в себя фильмы американского, европейского и азиатского производства в жанре "Ужасы" и "Мистика". При этом контент Scream в полной мере является актуальным и современным: 70% фильмов, демонстрируемых в эфире телеканала, выпущены в 2018-2022 годах. По мнению Марины Гаспарян, Scream хорошо подходит и для семейного показа, учитывая, что совместные просмотры хорроров очень популярны у молодых пар.

Директор по маркетингу EPG Service Александра Скрипочка поделилась данными исследований, проведенных в ее компании. Зритель в среднем готов тратить на выбор контента для ежедневного просмотра до 20 минут, при этом решающими факторами для него становятся рейтинги IMDB и "Кинопоиска", информация о режиссерах, актерах с их фотографиями. Эти элементы должны присутствовать как в экранных телегидах, так и в карточках тайтлов на платформах.

Комментируя рост популярности трансляций киберспорта, директор спортивных проектов Триколора Мария Гришко отметила, что аудитории таких трансляций и платного ТВ практически не пересекаются. В то же время в Триколоре видят перспективы такого вещания в онлайн-кинотеатре. Также Мария Гришко рассказала, что заменить показ зарубежных турниров трансляциями отечественных соревнований практически невозможно. Тем не менее, в Триколоре, где сделана ставка именно на российский спорт, не видят серьезного негативного эффекта для своей аудитории из-за отсутствия в эфире трансляций популярных зарубежных состязаний.

Участники сессии о детской анимации "Где водятся волшебники и другие несказочные проблемы детского анимационного контента в России" подчеркнули важность разработки отечественных программных продуктов для создания мультипликации. Зарубежное ПО для 3D-анимации больше не лицензируется и не поддерживается в России, при этом отдельно взятая студия не может выделить достаточные средства для разработки значительной части требуемого ПО. Поэтому необходимо выделение государственных средств на такую разработку, причем речь должна идти о совместных проектах: в одиночку создавать современное ПО для анимации нереально.

Завершила деловую программу конференции питч-сессия телевизионных новинок сезона, включая тематические каналы, анимационные и кинопроекты. Одним из запоминающихся моментов питч-сессии стал рассказ о новых проектах директора службы рекламы и продвижения телекомпании "Первый ТВЧ" Марии Черкасской. За последние годы телекомпания увеличила пакет производимых и дистрибутируемых каналов в два раза – до 35 единиц, сейчас он включает тематические, киносериальные, детские и спортивные каналы.

В начале ноября телекомпания обновила телеканал "Еда премиум". Теперь он называется Food time, изменен визуальный концепт и оформление студии и самих программ. Сетка канала расширена за счет новых кулинарных шоу, в том числе в формате баттлов и гастрономических путешествий. Кроме того, осенью этого года "Первый ТВЧ" начал дистрибутировать и новый телеканал Триколора – Scream.

Завершила контентный поток и конференцию в целом демонстрация ролика телеканала "Наша Сибирь 4K". Как рассказал генеральный директор "Нашей Сибири" Денис Инякин, телеканал фокусируется на контенте о природе, показывая ее 24 часа "такой, какая она есть, без рекламы и новостей". Создатели телеканала из Кемерово не боятся говорить о своей любви к природе в программах собственного производства, и надеются, что их чувства разделят и зрители партнерских платформ по всей стране, в сотрудничестве с которыми заинтересована "Наша Сибирь".