НАУЧНЫЙ ЖУРНАЛ

ТЕЛЕКОММУНИКАЦИИ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

№2-2021

(*Дата издания: ноябрь 2021 г.*)

УЧРЕДИТЕЛЬ:

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ» (МТУСИ)

РЕДАКЦИОННАЯ ПОДГОТОВКА:

Отдел организации научно-исследовательской работы студентов (ОНИРС МТУСИ)

СОДЕРЖАНИЕ №2-2021

«Цифровые технологии радиосвязи и телерадиовещания»

«Сетевые технологии и системы телекоммуникаций»

«Информационные технологии и автоматизация процессов в системах связи»

НЕЙРОННАЯ СЕТЬ ДЛЯ ВОСЬМИЭЛЕМЕНТНОЙ ФАЗИРОВАННОЙ АНТЕННОЙ РЕШЕТКИ

Ахмад Али,
магистрант МТУСИ, Москва, Россия,
aliahmad2423aall@gmail.com

Николаев Алексей Владимирович,
доцент, заведующий кафедрой ТЭДиА, д.т.н., МТУСИ, Москва, Россия,
mosipg@yandex.ru

Титовец Павел Александрович,
старший преподаватель кафедры ТЭДиА, к.т.н., МТУСИ, Москва, Россия,
paveltitovec@yandex.ru

Аннотация

Приводится описание сформированной обучающей выборки (базы данных), которая представляет собой массив информации по сдвигам фаз в произвольных направлениях и является основой для интеллектуального управления во времени и в пространстве формой диаграммы направленности антенны. Представлены результаты тестирования такой антенной системы с использованием рекуррентной нейронной сети и показана перспективность метода машинного обучения (Deep learning) для решения сложных динамических задач в области технической электродинамики и антенн.

Ключевые слова: *фазированная антенная решётка, интеллектуальная антенна, нейронная сеть, искусственный интеллект, глубокое обучение, машинное обучение.*

Введение

В области антенной техники наблюдается тенденция перехода от традиционных антенных систем с фиксированной формой диаграммы направленности к интеллектуальным антенным системам, способным динамически изменять свою диаграмму с целью уменьшения уровня шума и помех, устранения эффекта замирания радиосигнала и др. Широкое развитие фазированных антенных систем для мобильной сотовой связи требует постоянной динамической их подстройки в зависимости от количества абонентов и их потребностей. Для решения данных задач могут быть применены алгоритмы искусственного интеллекта (ИИ). Основная цель представляемого в статье исследования заключалась в определении амплитуд и фаз для восьмиэлементного лабораторного макета фазированной антенной решетки, при которых можно задать требуемую диаграмму направленности с помощью ИИ.

Фазированная антенная решетка

Антенны с фазированной решеткой состоят из множества стационарных антенных элементов, которые питаются когерентно и используют управление переменной фазой или временной задержкой на каждом элементе для сканирования луча под заданными углами в пространстве. Основная причина использования массивов элементов - это создание направленного луча, который можно изменять (сканировать) электронным способом [1, 7-8].

Принципиальная схема луча линейной фазированной антенной решетки представлена на рисунке 1.

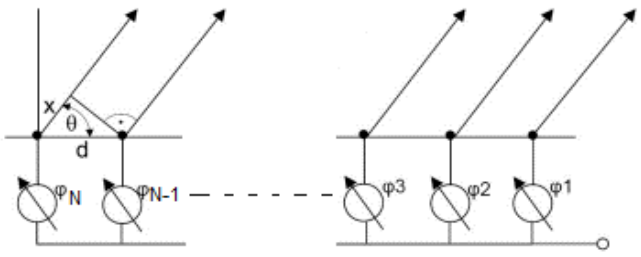


Рис. 1. Принципиальная схема фазированного луча линейной антенной решетки

Сдвиг фазы ϕ между двумя последовательными элементами постоянен и называется приращением фазы. Эти формулы можно вывести из рисунка 1:

$$\mathbf{x = d{\cdot}cos\theta \rightarrow \frac{2\pi}{\phi} = \frac{\lambda}{x} \rightarrow \phi = \frac{2\pi}{\lambda} d{\cdot}cos\theta,} \quad (1)$$

где d – расстояние между элементами, θ – угол между плоскостью антенны и направлением излучения.

Диаграмма направленности фазированной антенной решетки

Как показано на рисунке 2, множитель решетки задаётся следующим соотношением:

$$\mathbf{S(\theta, \varphi, A, \delta)= \sum_{n=1}^{M} A_n . exp[jnkd(cos\theta cos\theta_a + sin\theta sin\theta_a cos(\varphi - \varphi_a)) + j\delta n]}\,, \quad (2)$$

где A=[A_1,A_2,……..A_N] , δ=[δ_1, δ_2, …… δ_N] , An и δn представляют собой амплитуду и фазу текущего возбуждения n-го элемента решётки; $k = 2\pi / \lambda$ – волновое число; λ – длина волны, d – равномерное расстояние между элементами, (θ, φ) – интересующее направление и (θa, φa) – направление оси решётки [2].

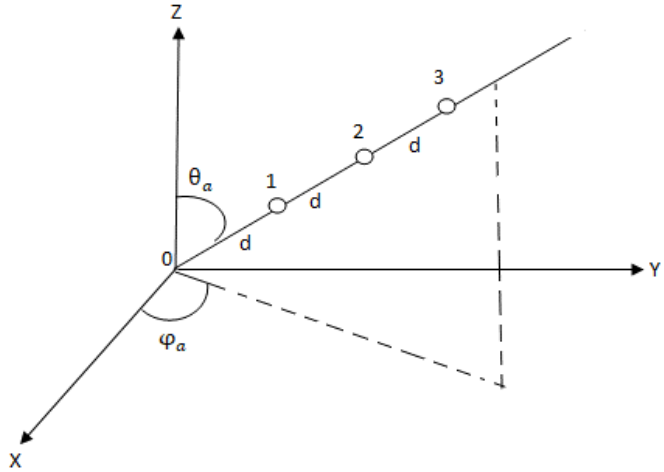


Рис.2. Геометрическая интерпретация линейной антенной решетки

Диаграмма направленности антенной решетки получается путём умножения множителя решетки на диаграмму направленности (ДН) элемента решетки.

Искусственные нейронные сети

Нейронная сеть представляет собой совокупность нейронов, соединенных друг с другом определенным образом. Рассмотрим один нейрон (рис. 3):

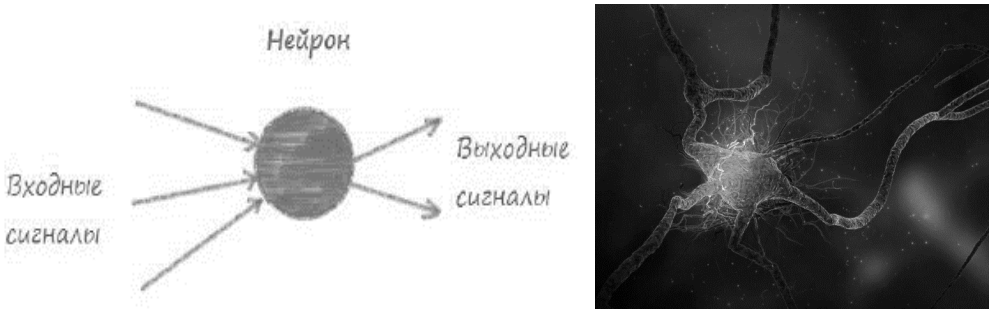


Рис. 3. Модель нейрона и его биологическая схема

Нейрон представляет собой элемент, который вычисляет выходной сигнал (по определенному принципу) из совокупности входных сигналов, то есть основная последовательность действий одного нейрона такова:

- прием сигналов от предыдущих элементов сети;
- комбинирование входных сигналов;
- вычисление выходного сигнала;
- передача выходного сигнала следующим элементам нейронной сети.

Алгоритм наименьшего среднего квадрата (*LMS - Least Mean Square*)

LMS – это итеративный алгоритм формирования диаграммы направленности, который использует оценку вектора градиента из доступных данных. Этот алгоритм выполняет последовательные корректировки вектора весов в направлении отрицательного значения вектора градиента, что в конечном итоге приводит к минимальной *MSE (Mean Square Error* – среднеквадратическая ошибка) между выходом формирователя луча и ожидаемой формой сигнала.

Как показано на рисунке 4, выходом решётки (t) является взвешенная сумма принятых сигналов n(t) на элементах решётки и весов решётки n (t), где k = 1,2, …… , N , N – количество антенных элементов.

Веса решётки (1, 2, ..., N) итеративно вычисляются на основании выходного сигнала решётки (t); (t) опорный сигнал, аппроксимирующий требуемый сигнал и предыдущие весовые коэффициенты [3].

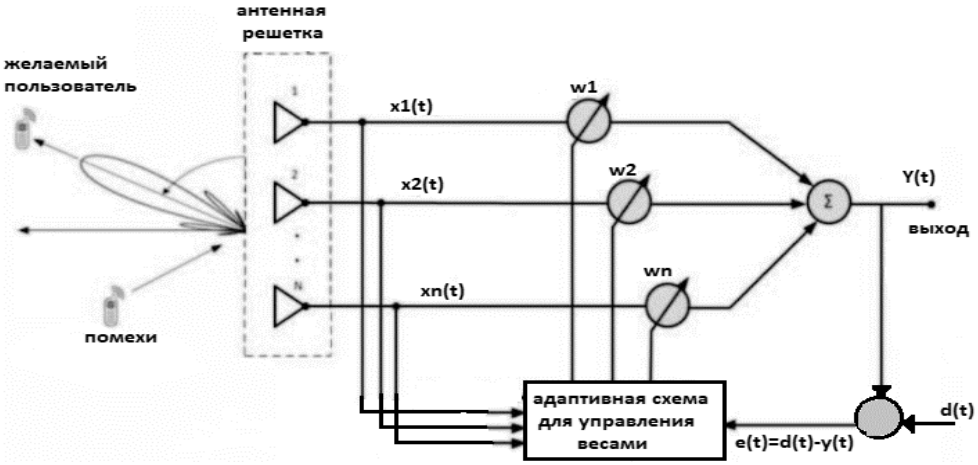


Рис. 4. Принцип наименьшего среднего квадрата в антенной решетке

Выход антенной решётки (t):

$$(t) = \quad (t) \quad (t), \tag{3}$$

где означает транспонирование весового вектора .

Принятый сигнал (t) определяется выражением:

$$(t) = \quad (t) + \sum_{K=1}^{M} a(\theta i)\, i(t) \; + \; , \tag{4}$$

где – желаемый вектор управления, (t) - опорный сигнал, ( ) - вектор управления помехами, (t) – сигнал помехи и (t) – шумовой сигнал. Ошибка (t) используется для вычисления новых весов (обновления весов) и определяется выражением:

$$(t) = (t) - (t), \tag{5}$$

$$e(t)=d(t) - \quad (t)\cdot x(t). \tag{6}$$

Результаты тестирования макета антенной решетки

На рисунке 5а приведена антенная решетка, собранная в лаборатории, статические элементы которой неизменны. Количество элементов $N = 8$. Расстояние между элементами $d = 19$ cm, амплитуда сигнала 1В.

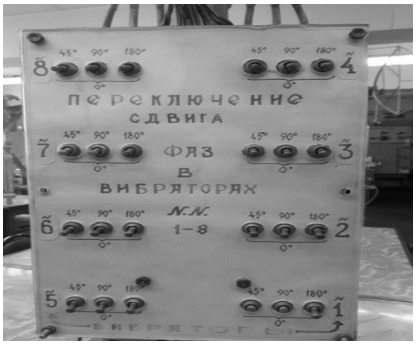


Рис. 5a. Макет антенной решётки

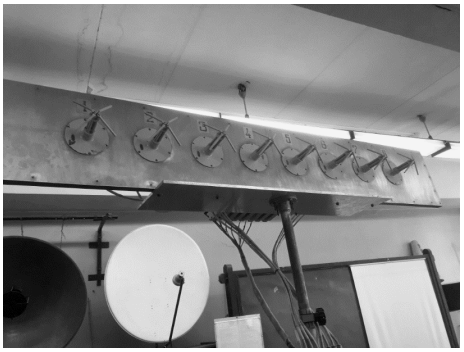


Рис. 5b. Возможные фазовые углы

На рисунке 5b видно, что для каждого элемента есть 3 ключа для значений фазовых углов 45°, 90°, 180°. Значения возможных фазовых углов для каждого элемента в лаборатории были выбраны: 0°, 45°, 90 °, 135°, 180°, 225°, 270°, 315°, 360° = 0°.

Сравнивая основную и приблизительную теоретическую ДН под углом 45° (рис. 6a), отметим, что оба они имеют главный лепесток под углом 45°, но боковые лепестки имеют большую амплитуду. На рисунке 6b показана ДН при -40°, 30° , Отметим , что оба имеют главный лепесток при -40°и 30°, но с небольшим отклонением. Кроме того видно, что распределение боковых лепестков другое. Это связано с ограничением установки фаз в отдельных элементах лабораторной антенной решётки.

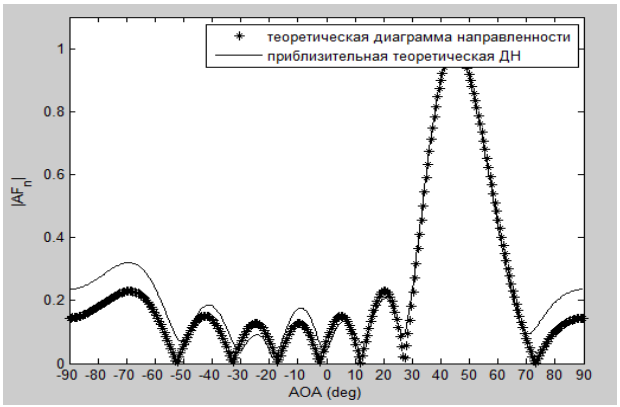


Рис. 6a. Теоретическая ДН при 45°

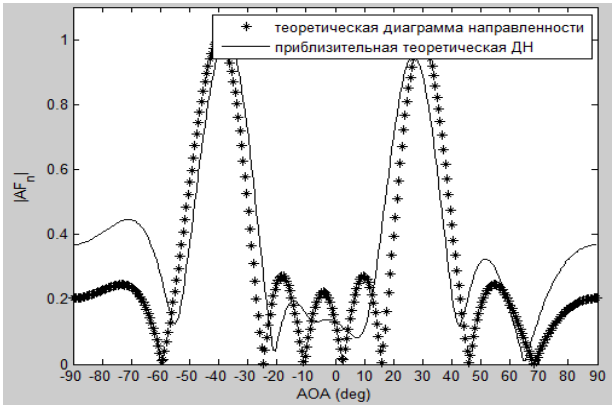


Рис. 6b. Теоретическая ДН при - 40°, 30 °

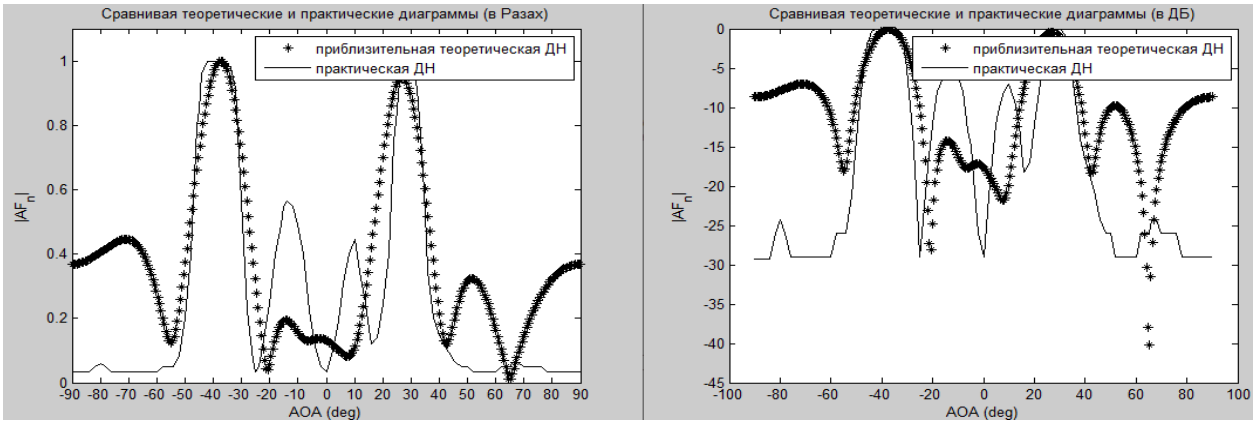


Рис. 7. Теоретическая и практическая диаграмма при -40 °, 30 ° (в разах и дБ)

На рисунке 7 представлена теоретическая и практическая диаграммы при -40°, 30° (в разах и дБ). Оба графика имеют главный лепесток при -40° и 30°, но амплитуда и распределение боковых лепестков различны, что связано также с ограничением установки фаз в отдельных элементах лабораторной решётки.

Сравнивая основную и приблизительную теоретическую ДН (рис. 8), отметим, что у обоих из них есть основные лепестки на -60, -30, 0, 30 и 60, и нет боковых лепестков. На приблизительной диаграмме мы замечаем, что антенна не фиксирует сигналы помех в нулевые точки как на основной диаграмме, что также связано с ограничениями установки фаз в отдельных элементах лабораторной решётки.

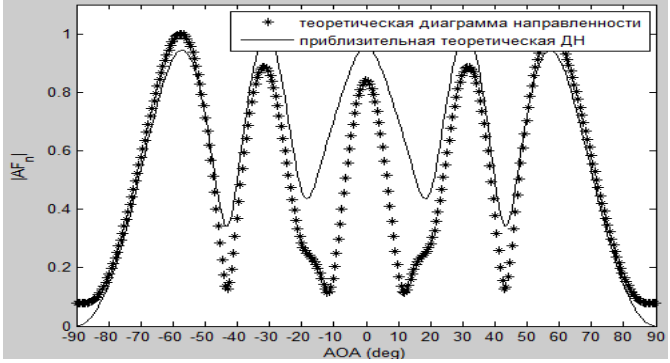


Рис. 8. Основная и приблизительная теоретическая ДН при -60, -30, 0, 30, 60

Сравнивая теоретические и практические диаграммы при -60, -30, 0, 30, 60 (в разах и в дБ), мы отмечаем, что оба имеют главный лепесток на -30, 0 и 30, но при -60 и 60 главный лепесток теоретически становится боковым лепестком практически, это связано с ограничением установки фазы в отдельных элементах лабораторной решётки.

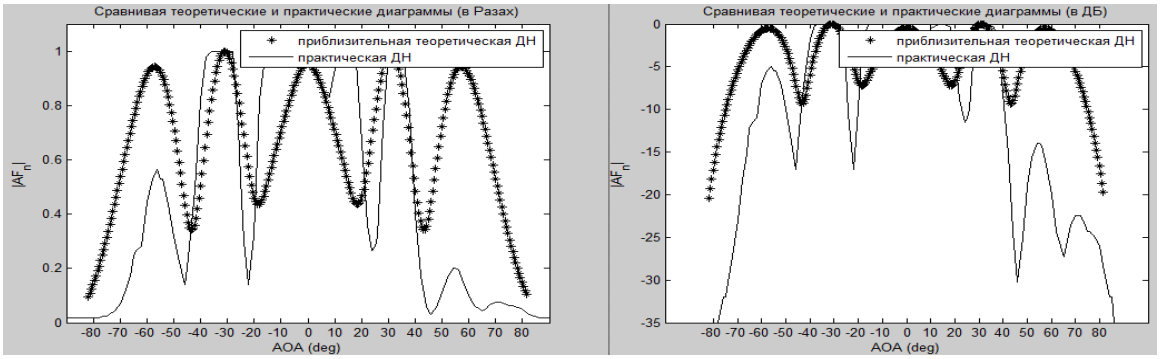


Рис. 9. Теоретическая и практическая диаграммы при -60,-30,0,30,60 (в разах и в дБ)

Рекуррентная нейронная сеть

Это особый вид искусственной нейронной сети. Эта сеть состоит из одного или нескольких скрытых слоёв и имеет один или несколько циклов обратной связи.

Обычно она содержит элемент задержки единицы z^{-1} (рис. 10), который даёт этим сетям свойства локальной памяти, позволяя хранить шаблоны активности и определять их в нейронной сети более одного раза [4].

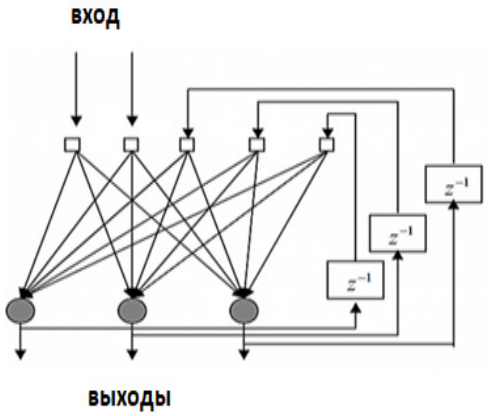


Рис. 10. Схема рекуррентной нейронной сети

Этап обучения (*training phase*)

На этом этапе генерируются входная и выходная пары искусственной нейронной сети (предварительная обработка) для обучения сети на них и сохранения параметров веса после достижения наилучших результатов обучения.

Сначала формируется корреляционная матрица (correlation matrix) входящих сигналов, принимаемых M элементами системы антенных решеток:

$$R_{xx}=E\{X(K)X(K)^{H}\}=\begin{bmatrix} R11 & R12\cdots & R1M \\ \vdots & \ddots & \vdots \\ RM1 & RM2\cdots & RMM \end{bmatrix}, \quad (7)$$

где H относится к сопряженному транспонированию (conjugate transpose).

Первая строка корреляционной матрицы Rxx принимается за вход нейронной сети, поскольку она содержит достаточную информацию о принятом сигнале как:

$$Z=[R_{11}\ R_{12}\ldots\ldots\ldots\ldots\ldots\ R_{1M}] \quad (8)$$

Тогда входной вектор нормируется к единице, чтобы быть более подходящим в качестве входа нейронной сети:

$$B=\frac{}{} \quad (9)$$

Поскольку нейронная сеть не работает с комплексным числом, берутся действительная и мнимая части (квадратурные составляющие сигнала) каждого элемента в векторе (B), в связи, с чем размерность вектора (B) будет вдвое больше (1x2M).

Желаемый выходной сигнал нейронной сети генерируется из весового уравнения формирователя диаграммы направленности без искажений с минимальной дисперсией (*MVDL Minimum Variance Distortionless*). Веса, которые генерируются из формирователя луча MVDL, могут обеспечить оптимальное формирование луча и направить основной луч диаграммы направленности к нужным пользователям и обнулить нежелательных пользователей в оптимальной форме.

Вес антенной решетки на основе формирователя луча *MVDL*:

$$W_{op}= (A_d \cdot R_{xx}^{-1})/(A_d^{H} \cdot R_{xx}^{-1} \cdot A_d), \quad (10)$$

где A_d относится к вектору рулевого управления (steering vector) для K желаемых сигналов, принимаемых антенной решеткой с M элементами.

Процесс обучения нейронной сети показан на рисунке 11.

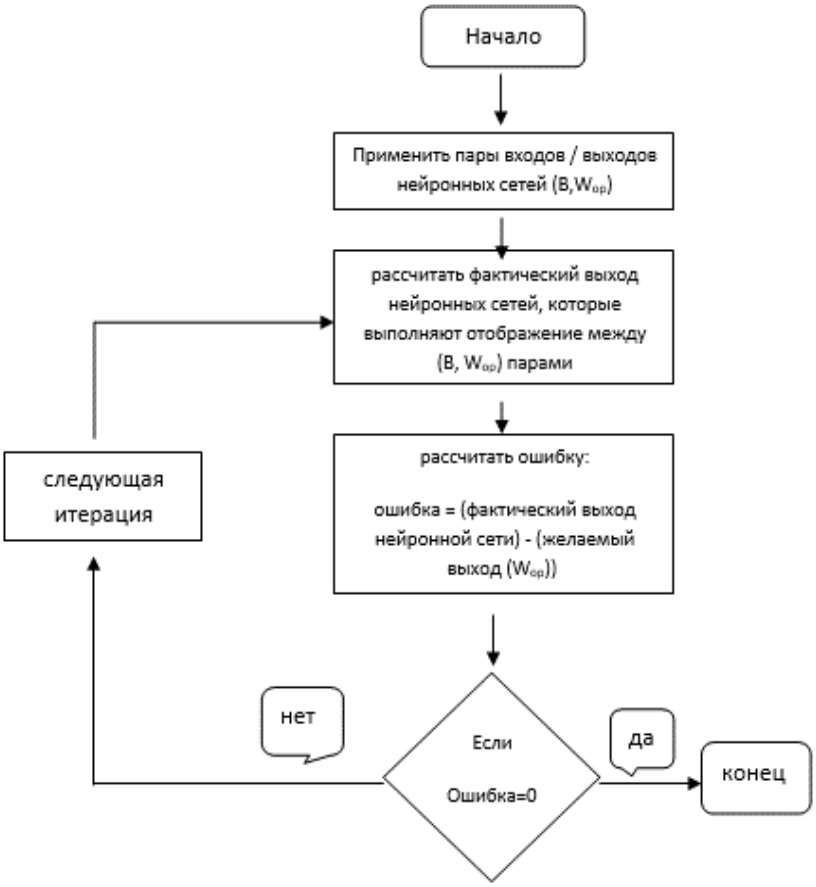


Рис. 11. Порядок обучения нейронной сети

Как показано на рисунке 11, обучение завершается после достижения сетью наилучшей производительности обучения (ошибка между фактическим и целевым выходным приближением W_{op}, приближающимся к нулю). Затем веса запоминаются нейронной сетью. При этом сеть будет использовать эти весовые коэффициенты для оценки выходных данных выборки, на которых она ранее не обучалась («невидимая» выборка данных»).

Стоит отметить, что для достижения наилучшей эффективности обучения сети требуется более одного пробного обучения, а сохраненные веса сети относятся к эмпирическим знаниям, полученным сетью в процессе обучения.

Этап производительности (*Performance Phase*) и результат тестирования ИИ

На этом этапе нейронная сеть оценит веса новых входящих сигналов, которые она ранее никогда не видела во время этапа обучения (сеть не обучалась на них).

Далее вычисляется матрица корреляции R_{xx} принятого сигнала, а затем – единственный вход для нейронной сети – это вектор B. При этом сеть будет оценивать (или прогнозировать) на основе эмпирических знаний, полученных в процессе обучения результат – оптимальный вес $W_{op.}$ Полученные веса используются системой антенных решеток для формирования множества узких диаграмм направленности в желаемых направлениях (в сторону абонента) и обнуления в направлении реальных помех [5,6].

ERNN обучается с использованием контролируемых алгоритмов обучения, таких как алгоритм Левенберга Марквардта *(LM)(Levenberg Marquardt)*, алгоритм эластичного обратного распространения *(Rprop)(Resilient backpropagation)* и алгоритм *GDX (gradient descent algorithm with variable learning and momentum factor)* (градиентный спуск с переменным обучением и фактором импульса). Единственным входом в сеть является вектор B, а выходом будет оптимальный вес W_{op}.

После достижения результата обучения искусственной нейронной сети, диаграмма направленности системы антенных решеток получается из уравнения коэффициента решетки, которое задаётся следующим образом:

$$AF=|W_{op}(k).e^{-j(i-1)\alpha(k)}| \text{ , } i=1,2,\ldots\ldots\ldots M \qquad (11)$$

где α(k) – угол поиска (searching angle) [-90°,90°] с шагом 1˚(step size) от -90° до 90°.

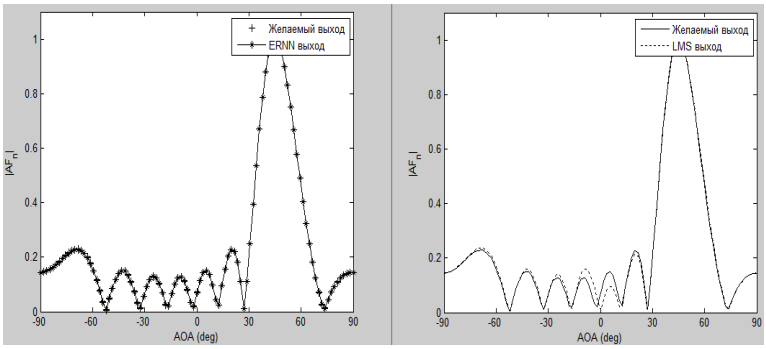
На рисунке 12 показано сравнение между выходом LMS, выходом ERNN и желаемым выходом под углом 45°.

Сравнение желаемого выхода с выходом алгоритма LMS (рис. 12b) показывает небольшое отличие между двумя диограммами.

Сравнение желаемого выхода с выходом сети ERNN (рис. 12a) показывает полное соответствие между двумя диаграммами.

Таким образом, ERNN даёт лучшие результаты, чем алгоритм LMS.

Важное примечание: разница между двумя рисунками очень мала, и причина этого в том, что база данных, которая у нас использовалась, невелика, а при использовании глубокого обучения база данных должна быть очень большой.



a b

Рис. 12. Сравнение между выходом LMS, выходом ERNN и желаемым выходом под углом 45°

Машинное обучение (Деревья решений (*Decision trees*))

Деревья решений – это способ представления правил в иерархической, последовательной структуре, где каждому объекту соответствует единственный узел, дающий решение.

Деревья решений – это логический алгоритм классификации, основанный на поиске конъюнктивных закономерностей.

Применение деревьев решений: описание данных, классификация, регрессия.

Практическая реализация лабораторных данных на Python

В ходе исследований была создана база данных, в которой входными данными являются номер антенного элемента и желаемый угол, обеспечивающий максимальную диаграмму направленности, а выход - соответствующий фазовый угол, который должен быть установлен в лабораторном макете.

Мы обучили эту базу данных дереву решений на Python (рис. 13) и смогли нарисовать дерево решений и предсказать значения, которых нет в базе данных.

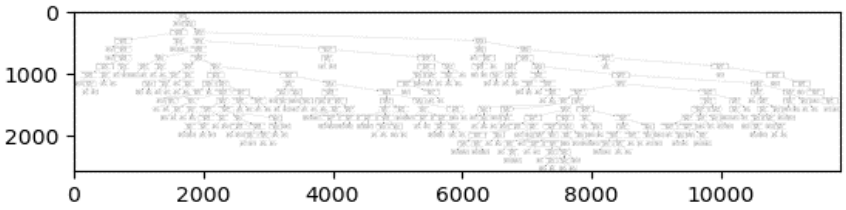


Рис. 13. Деревья решений на Python

Примеры предсказаний с использованием дерева решений:

1. Предсказать конкретное значение фазового угла **второго** антенного элемента, если бы желаемый угол был **14 °**?

predict([[2,14]]) = : **[45°.]**

2. Какими были бы значения фазовых углов **всех элементов** антенной решетки, если бы желаемый угол был **35 °**?

predict([[1,35]]) = **: [0 °.]** predict([[2,35]]) = : **[90 °.]** predict([[3,35]]) = : **[225 °.]**
predict([[4,35]]) = : **[315 °.]** predict([[5,35]]) = : **[45 °.]** predict([[6,35]]) = : **[135 °.]**
predict([[7,35]]) = : **[270 °.]** predict([[8,35]]) = : **[0 °.]**

Выводы

В результате проведённого в настоящей работе теоретического исследования определены фазы восьми элементов лабораторного макета фазированной антенной решетки, формирующие различные ДН *СМАРТ* антенн, которые позволяют одновременно обслуживать главными лепестками несколько абонентов в зоне обслуживания. Полученные экспериментальные данные показали возможность формирования до пяти главных лепестков в ДН *СМАРТ* антенны. Нейронные сети и машинное обучение могут быть использованы для повышения эффективности функционирования фазированной антенной решетки. Результаты настоящего исследования предполагается использовать при постановке лабораторного курса работ по методам формирования ДН *СМАРТ* антенн а кафедре ТЭиА в МТУСИ.

Литература

1. *Haring J., Majer N., Hronec R.* Directional pattern analysis of a linear phased antenna arrays Dept. of Telecommunications and Multimedia, Faculty of Electrical Engineering.
2. *Theodoros N. Kapetanakis , Ioannis Vardiambasis, George Liodakis, Melina Ioannidou.* Smart Antenna Design Using Neural Networks, Conference Paper. August 2013.
3. *D. M. Motiur Rahaman , Md. Moswer Hossain, Md. Masud Rana.* Least Mean Square (LMS) For Smart Antenna // Universal Journal of Communications and Network, 2013, pp-16-21.
4. *Lubna Badri.* Development of Neural Networks for Noise Reduction », researchgate.net/publication/233893443. December 2012.
5. *Adheed H. Sallomi, Sulaiman Ahmed.* Elman Recurrent Neural Network Application in Adaptive Beamforming of Smart Antenna System // International Journal of Computer Applications. November 2015. researchgate.net/publication/284223881.
6. *Воронцова К.В., Дьяконова А.Г., Золотых Н.Ю., Николенко С.И., Moore Andrew др.* Машинное обучение (Machine Learning), Деревья решений (Decision trees). Презентация по машинному обучению. *Уткин Л.В*.
7. *Titovets P.A.* Technique for increasing the antenna gain-to-noise-temperature of satellite communications earth stations with axisymmetric reflectors // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 45-51.
8. *Shherbakov A.V., Petruhin G.D., Miroshnikova N.E., Titovets P.A.* Estimation of underwater optical communication link operating distance // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 3. С. 54-60.

NEURAL NETWORK FOR EIGHT-ELEMENT PHASED ANTENNA ARRAY

Ahmad Ali,
Graduate MTUCI, Moscow, Russia,
aliahmad2423aall@gmail.com

Alexey V. Nikolaev,
Associate Professor, Head of the Department of TEDiA, Doctor of Technical Sciences, MTUCI, Moscow, Russia,
mosipg@yandex.ru

Pavel A. Titovets,
Senior Lecturer of the Department of TEDiA, Ph.D., MTUCI, Moscow, Russia,
paveltitovec@yandex.ru

Abstract

A description of the formed training sample (database) is given, which is an array of information on phase shifts in arbitrary directions and is the basis for intelligent control in time and space of the shape of the antenna directional pattern. The results of testing such an antenna system using a recurrent neural network are presented and the prospects of the machine learning method (Deep learning) for solving complex dynamic problems in the field of technical electrodynamics and antennas are shown.

Keywords: *phased array antenna, smart antenna, neural network, artificial intelligence, deep learning, machine learning.*

АНАЛИЗ МЕТОДИК ИЗМЕРЕНИЯ ОТНОСИТЕЛЬНОЙ ИНТЕНСИВНОСТИ ШУМА (RIN) ЛАЗЕРНОГО ИЗЛУЧЕНИЯ

Кашевский Игорь Станиславович,
магистрант МТУСИ, Москва, Россия,
Deminell@yandex.ru

Сперанский Валентин Сергеевич,
доцент кафедры РТС, к.т.н., МТУСИ, Москва, Россия,
speransky.v@yandex.ru

Аннотация
Приведены результаты исследования относительной интенсивности шума лазерного излучения для оптической системы передачи сигналов. Проведён анализ типовых методик измерения RIN путём проведения серии измерений параметров приёмо-передающей оптической системы radio over fiber (ROF). На основе сравнения результатов различных методов измерения RIN показано, что наиболее эффективным методом измерения в лабораторных условиях является метод, основанный на вычитании шумов разного происхождения из суммарного значения.

Ключевые слова: *метод вычитаний, калибровка по дробовому шуму, ROF, шум относительной интенсивности, RIN, источник лазерного излучения.*

За последние десятилетия в сфере сверхширокополосных приёмо-передающих систем наблюдается процесс замещения «электронных» систем на «фотонные». Такой переход связан в первую очередь с тем, что фотон, по своей природе, не имеет заряда и массы, в отличие от электронов. Вследствие этого фотонные системы не подвержены влиянию электромагнитных полей, а так же имеют более широкую полосу пропускания сигнала.

В современных оптоволоконных технологиях требования к оптическим передатчикам и лазерам постоянно растут, поскольку они являются одной из главных составных частей волоконно-оптической системы связи. Отношение сигнал/шум в линиях оптической связи существенно зависит от нестабильности мощности лазерного излучения. В связи с этим необходимо знать особенности и характеристики этой нестабильности.

Определение шума относительной интенсивности (RIN)

Измерение RIN служит индикатором качества лазерных приборов. Его можно рассматривать как тип обратного измерения отношения несущей к шуму [1,5, 6-13]. Поэтому, чем выше значение RIN, тем больше шумы лазера, что влечёт за собой введение более высокого штрафа по мощности от RIN.

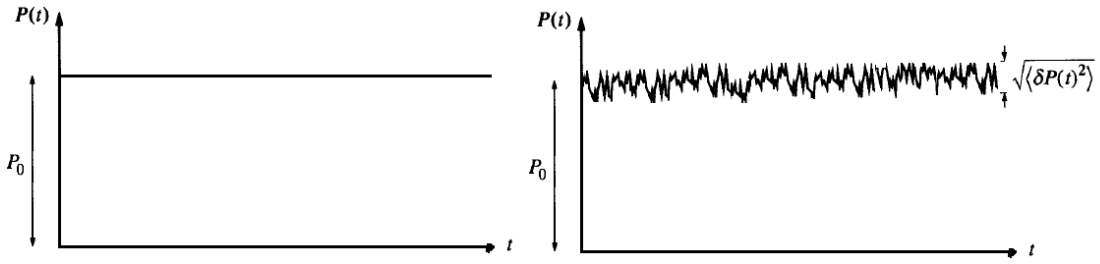


Рис.1. а) идеальная выходная мощность для лазера с постоянным смещением;
б) реальная выходная мощность лазера с интенсивным шумом

Рисунок 1а иллюстрирует идеальную выходную интенсивность лазера, смещенную на уровне постоянного тока, в то время как все параметры, влияющие на лазер (температура и др.), считаются постоянными. На рисунке 1б изображён реальный случай, когда выходная интенсивность лазера вызывает колебания мощности из-за шума интенсивности. При определении RIN учитывается вклад вариаций интенсивности лазера в общий электрический шум на входе приемника. Данная часть электрического шума в соотношении с мощностью электрического сигнала определяет RIN.

Определение RIN в аналитической связано со следующими условиями: предполагается, что RIN – это белый шум (постоянный для всех частот); RIN нормируется на полосу пропускания 1 Гц для обеспечения сравнения флуктуации интенсивности лазера при использовании приемников с различной полосой пропускания [1]:

$$RIN = \frac{<\delta P(t)^2>}{P_0^2 * \Delta f}\ [1/\text{Hz}]; \quad (1)$$

где $\delta P(t)$ – флуктуации оптической интенсивности, t – среднее время, P_0 – оптическая мощность постоянного тока, а Δf – полоса пропускания шума (полоса пропускания системы обнаружения).

Следовательно, RIN является отношением мощности лазерного шума, нормированной на полосу пропускания 1 Гц, к средней (или постоянной) мощности фототока, рассматриваемой в электрической области [1].

$$RIN\ \left[\frac{dB}{Hz}\right] = 10log\ \left(\frac{<\delta P(t)^2>}{P_0^2 * \Delta f}\right)[dB] - 10\log\left(\Delta f\right)[Hz]; \quad (2)$$

Измерение RIN

RIN часто измеряется в электрической области путем прямого обнаружения. Фотоприемник используется для преобразования мощности оптического шума в электрический сигнал. Спектр этого электрического шумового сигнала является целью измерения. В этом случае электрический анализатор спектра (ESA) является критически важным инструментом. Так как выходной фототок от детектора обычно является слабым, зачастую после детектора необходимо разместить электрические микроволновые усилители. Это усиление должно быть достаточно высоким, чтобы соответствовать чувствительности анализатора спектра (AC) [2]. В действительности измерение RIN имеет некоторые ограничения, для преодоления которых существует несколько методов вычисления RIN.

Экспериментальная установка

На рисунке 2 приведена схема типичной установки для измерения RIN. Назначение установки заключается в том, чтобы зарегистрировать излучение с помощью фотоприемника, а затем разделить переменную (шум) и постоянную составляющую фототока.

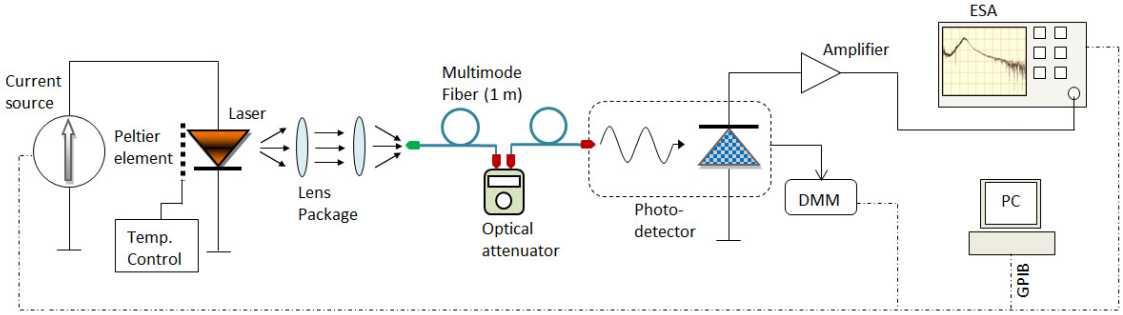


Рис. 2. Схема измерения RIN

Ограничения измерения RIN

На практике к чистому лазерному шуму интенсивности добавляются дополнительные источники шума от других используемых электрических компонентов: темновой ток от фотоприемника и тепловой шум от электрических элементов, таких как усилители и АС. Являясь дополнительными источниками, они генерируют шумы, смешивающиеся с шумом интенсивности лазера. Помимо этого, следует учитывать наличие ещё одного источника шума, связанного с квантовой природой света - дробовой шум.

Общий обнаруженный шум

Измеряемая с использованием анализатора спектра (АС) общая мощность шума является суммарной величиной шумов от всех источников шума, нормированный в полосе 1 Гц) [3,4].

$$N_{TOTAL}\ (f) = N_{Laser}(f) + N_{Shot} + N_{Thermal}(f)\ [\text{W/Hz}] \quad (3)$$

RIN в единицах дБ/Гц, измеренный с учётом теплового шума, дробового шума в фотоприемнике и теплового шума в электрическом предусилителе может быть представлен в виде следующего выражения [4].

$$RIN = \frac{S_p + \sigma_{shot}^2 + \sigma_{th}^2 + \sigma_{amp}^2}{\Re^2 P_{opt}^2} = RIN_{laser} + RIN_{error} \quad (4)$$

где S_p – спектральная плотность мощности шума интенсивности лазера, которая вносит свой вклад в значение RIN. остальные члены выражения рассматриваются как ошибки – RIN_{error}.

Методы измерения RIN

Различные методы вычисления RIN связанны с проблемой наличия шумов, созданных дополнительными источниками. При использовании метода вычитания различные источники шума обрабатываются отдельно и вычитаются из общего члена шума. В этом случае вводится специальный способ калибровки измерительной системы, предполагающий, что тепловой шум может быть легко вычтен. Данный метод широко используется в оптоволоконной связи, где измерение RIN производится для модулированных оптических систем и требуется измерение значение RIN на определенной частоте.

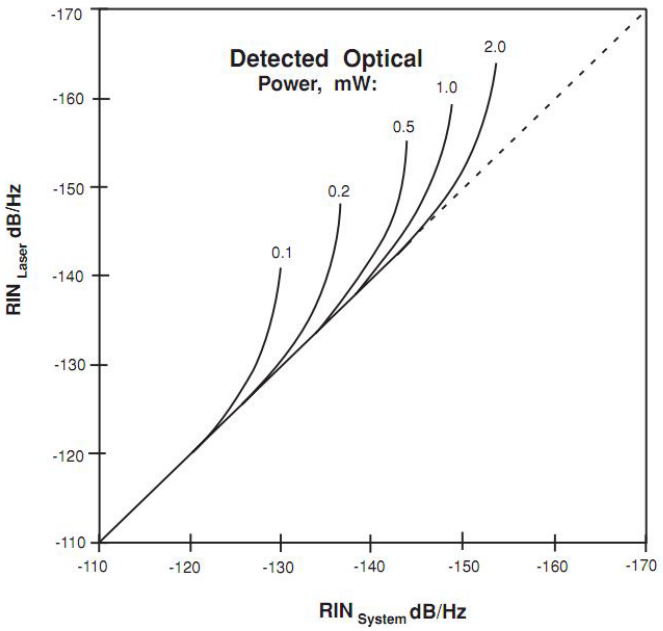


Рис. 3. RIN_{Laser}, рассчитанный по измеренной RIN_{system} (RIN_{TOT}), в зависимости от средней мощности [3]

Поскольку значение RIN представляет интерес только на определенной частоте, система калибруется для дробового шума гораздо более точно.

Метод вычитания

При использовании данного метода дополнительные шумы вычисляются отдельно и вычитаются из итогового значения RIN. Тепловой шум измеряется на измерительном стенде при выключенном лазере, т.е. на ФД не приходит лазерное излучение. При этом имеет место темновой фототок ФД и тепловой шум электроники (полный фоновый шум). Дробовой шум, тем не менее, вычисляется из измеренного DC фототока, когда лазер включен. ФД показывает среднее значение DC фототока при помощи миллиамперметра. Данный прибор регистрирует вольтаж электрического сигнала. Фототок может быть вычислен путем деления этого значения на постоянный фактор 1 мВ/мА. Следовательно, спектральная плотность мощности дробового шума может быть вычислена как:

$$P_{n,shot} = (i_n)^2 * 50\Omega = 2q * I_{DC} * 50\Omega, \quad (5)$$

где I_{DC} – это среднее значение фототока, 50Ω – сопротивления нагрузки.

Вычисленный шум вычитается из измеренного общего значения RIN для определения RIN в дБ.

Данный метод нужно использовать с большой осторожностью при определении RIN_{Laser}. При вычислении маленьких значений из исходных маленьких значений параметров, ошибки в полученных значениях, близкие к избыточному шуму лазера, могут сильно повлиять на результат. Так же ошибки в точности амплитудно-частотной характеристики фотодиода могут сильно влиять на результат измерений увеличения эффектов. Помимо этого, важно знать полную частотную характеристику всей системы, прежде чем реализовывать метод вычитания шумов.

Метод калибровки по дробовому шуму

Основная проблема метода вычитания шумов состоит в том, что он требует определения различные параметры системы передачи, в частности частотных характеристики различных компонентов. Точность этого метода ограничена вследствие необходимости вычислять и измерять множества этих параметры. В тоже время, в

методе калибровки по дробовому шуму используется самокалибровочный механизм, который устанавливает и поддерживает все параметры измерительной системы и обеспечивает более точный результат измерений.

Данный метод основан на том факте, что при фиксированном токе смещения лазера шум от различных источников возрастает с уменьшением мощности ЛИ при использовании динамического оптического аттенюатора. Как показано на рисунке 4, тепловой шум не зависит от оптической мощности, следовательно, при изменении мощности ЛИ тепловой шум будет постоянным. С другой стороны, дробовой шум в данном случае возрастает линейно (10дБ/декада), а интенсивность шума лазера возрастает квадратично (20дБ/декада).

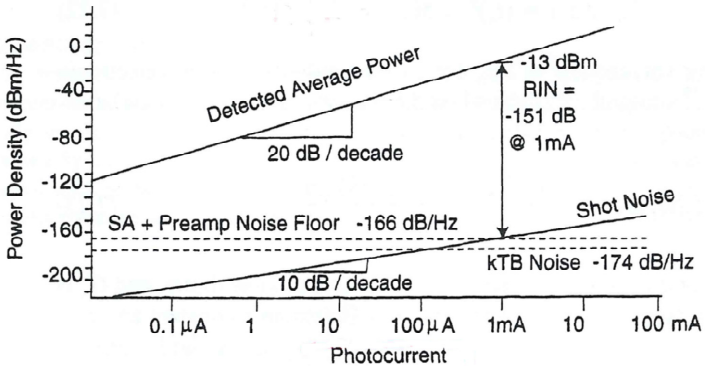


Рис. 4. Вариации различных шумов при изменении фототока на фиксированном токе смещения

Полный электрический шум как функция зарегистрированного фототока равен:

$$P_N = H(f) * 10^{\frac{RIN}{10}} * I_{DC} + 2q * H(f) * I_{DC} + P_{th}, \qquad (6)$$

где P_N – это полный шум спектральной плотности мощности (PSD) на анализаторе спектра, I_{DC} – это среднее значение DC фототока, P_{th} – тепловой шум, *H(f)* – транс-импеданс системы фотодетектор-АС.

Первый квадратичный член в уравнении 6 соответствует квадратичной связи между шумом интенсивности и полным шумом PSD. Второй член получается из дробового шума, который имеет линейную зависимость. В данном случае значения P_N и I_{DC} измеряются при различных настройках оптического аттенюатора (~10 шагов или более). Вследствие этих измерений может быть получена кривая второго порядка, как показано на рисунке 5, где пунктирная линия соответствует линейной зависимости только дробового шума, шум интенсивности в данном случае ничтожно мал. При очень низких значениях фототоков кривая близка по значениям к пунктирной кривой, поскольку шум интенсивности очень мал.

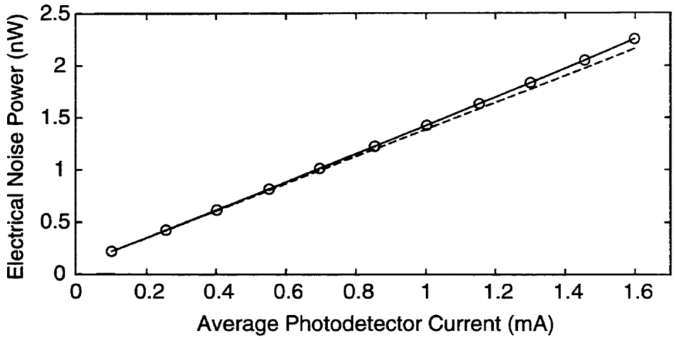


Рис. 5. Серия измерений параметров P_N и I_{DC} при различных настройках оптического аттенюатора

Используя метод наименьших квадратов квадратичной функции ($Y = a_1X^2 + a_2X + a_3$) для измеренных значений можно вычислить коэффициенты данного уравнения. Используя данное выражение для соответствующего уравнения 6, калибровочный член *H(f)* и, следовательно, значения RIN могут быть вычислены из соотношений:

$$H(f) = \frac{a_2}{2q}, \qquad (7)$$

$$RIN = 10\log\left(\frac{a_1}{H(f)}\right). \qquad (8)$$

Данные соотношения должны быть рабочими для каждой интересующей частоты.

Преимущества данного метода заключаются в том, что он имеет меньшую погрешность (большую точность) за счёт самокалибровки. С другой стороны, этому методу свойственны ряд ограничений: очевидно, что процедура измерений достаточно длительная, но самое главное, метод может быть использован только для сис-

тем с ограниченным дробовым шумом. Данный метод не подходит для систем, ограниченных тепловым шумом, имеющих малую оптическую мощность лазера, а также содержащих электронику с недостаточно низким уровнем шума. Однако его использование целесообразно в случае выполнения стендовых лабораторных измерений, при которых важна точность измерений и оптическая система ограничена только дробовым шумом.

Измерение RIN системы связи

С использованием метода калибровки по дробовому шуму была проведена серия измерений системы передачи Emcore, представленная в таблице 1 и на рисунке 6. Результаты измерений получились близкими к типовым значениям.

Таблица 1

Результаты измерений

F, GHz	0.3	0.6	0.9	1.2	1.5	1.8	2.1	2.4	2.7
P_{th}, W*10^{-20}	4.01	4.67	5.97	5.58	7.21	11.8	11	17	20.4
P_N, W*10^{-20}	5.73	6.3	7.41	7.67	9.73	14.5	15.8	20.9	25.7
RIN, dB/Hz	-146.54	-146.78	-147.3	-145.66	-144.83	-144.5	-141.98	-142.9	-141.5

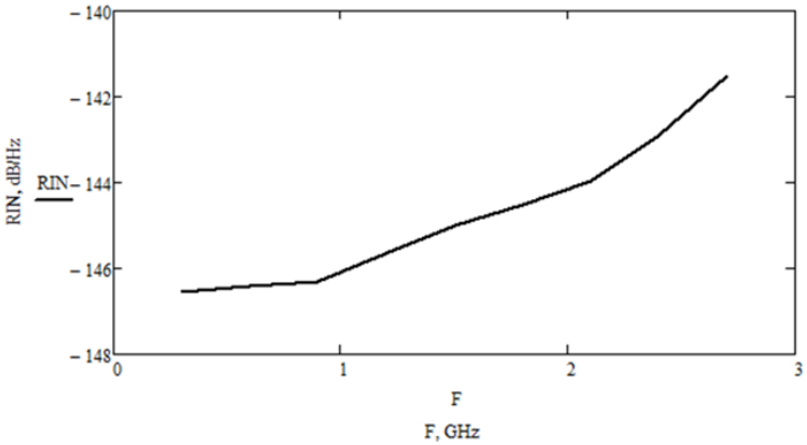


Рис. 6. Измерение RIN системы связи при постоянном I_{DC}

Литература

1. Основы микроволновой фотоники, *Урик Винсент Дж.-мл., МакКинни Джейсон Д., Вилльямс Кейт Дж.,* 2016.
2. Lightwave signal analyzers measure relative intensity noise. Product Note 71400-1, Agilent Technologies, 2000.
3. *R. Hui and M. O'Sullivan,* Fiber Optic Measurement Techniques, Academic Press, Boston, USA, 2009, pp. 259-363.
4. *Westbergh P., et al.* Speed enhancement of VCSELs by photon lifetime reduction // Electronics Letters. Vol. 46. No. 13, June 2010.
5. *Marpaung D.* High dynamic range analog photonic links: design and implementation, January 2009.
6. *Сперанский В.С., Абрамов С.В., Клинцов О.И.* Сочетание кодового разделения абонентов и OFDM при передаче данных по волокну // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 3. С. 32-35.
7. *Грибанов П.В., Сперанский В.С.* Современные тенденции развития систем наблюдения за воздушной обстановкой // Телекоммуникации и информационные технологии. 2018. Т. 5. № 1. С. 16-20.
8. *Сперанский В.С., Абрамов С.В., Клинцов О.И.* Передача сверхширокополосных сигналов по волокну // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 12. С. 18-20.
9. *Сперанский В.С., Мирошникова Н.Е., Рындин С.С.* О новом лабораторном практикуме по дисциплине "цифровые сигнальные процессоры" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 2. С. 29-32.
10. *Сперанский В.С., Абрамов С.В., Клинцов О.И., Шувалов В.М.* Особенности аналоговой и цифровой передачи радиосигналов по волокну // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 9. С. 38-42.
11. *Сперанский В.С., Косичкина Т.П.* Проект нового учебного пособия по дисциплинам, связанным с изучением цифровых сигнальных процессоров // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2016. Т. 5. № 3. С. 37-38.
12. *Сперанский В.С.* Методы повышения разрешения РЛС // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 1. С. 133-136.
13. *Славянский А.С., Сперанский В.С.* Беспроводные сенсорные устройства на основе эффекта переизлучения // Телекоммуникации и информационные технологии. 2016. Т. 3. № 1. С. 21-26.

ANALYSIS OF METHODS FOR MEASURING RELATIVE INTENSITY LASER RADIATION NOISE (RIN)

Igor S. Kashevsky,
Graduate MTUCI, Moscow, Russia,
Deminell@yandex.ru

Valentin S. Speransky,
Associate Professor of the Department of RTS, Ph.D., MTUCI, Moscow, Russia,
speransky.v@yandex.ru

Abstract

The results of a study of the relative intensity of laser radiation noise for an optical signal transmission system are presented. The performed analysis of typical RIN measurement methods makes it possible to measure the parameters of the transmit-receive optical radio communication system over optical fiber (ROF). Based on the results of measurements of RIN measurement methods, an effective measurement method in laboratory conditions is shown; it is a method based on subtracting noise of different origins from the total value.

Keywords: *subtraction method, shot noise calibration, ROF, relative intensity noise, RIN, laser source.*

АНАЛИЗ ВЛИЯНИЯ НА КАЧЕСТВО ИЗОБРАЖЕНИЙ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК СИГНАЛА В СИСТЕМАХ ЦИФРОГОВО ВЕЩАТЕЛЬНОГО ТЕЛЕВИДЕНИЯ

Долгов Станислав Геннадиевич,
начальник отдела наземной сети доставки программ ФГУП РТРС, г. Москва, Россия,
dolgov.stan@yandex.ru

Балобанов Андрей Владимирович,
доцент кафедры ТиЗВ, к.т.н., МТУСИ, г. Москва, Россия,
a.v.balobanov@mtuci.ru

Аннотация

Приведён анализ параметров и характеристик сигналов изображения в системах цифрового телевидения и их влияние на качество передаваемого сигнала с учётом специфика систем наземного телевизионного вещания стандарта DVB-T2. Рассмотрены основные подходы проведения мониторинга параметров транспортного потока и их влияние на качество передаваемого сигнала, а также наличия искажений и артифактов в изображении. Показано, что в качестве контрольных точек мониторинга целесообразно выбирать точки на стыках звеньев, где происходит преобразование цифрового сигнала

Ключевые слова: *система цифрового эфирного вещания DVB-T2, QoS, QoE, выход оборудования кодирования и мультиплексирования, вход возбудителя цифрового телевизионного передатчика, высокочастотный выход RF цифрового телевизионного передатчика, измерительный приемник-анализатор.*

Введение

Создание сети цифрового эфирного телевидения (далее – ЦЭТВ) в Российской Федерации – необходимый шаг в развитии единого информационного пространства страны и решения проблемы информационного неравенства между жителями крупных городов и малочисленных населенных пунктов. На начало 2009 года в России около трех миллионов россиян могли смотреть только один телеканал. Почти половина жителей страны (44%) могла принимать не более четырех телеканалов. При этом технические возможности аналогового вещания были исчерпаны.

Цифровое телерадиовещание предусматривает широкое внедрение трансляции в форматах высокой и сверхвысокой четкости. В перспективе, с учетом развития технологий сжатия изображения, в составе мультиплексированного потока DVB-T2 можно передавать до двух программ сверхвысокой четкости. Кроме того, трансляция в стандарте DVB-T2 обеспечивает расширение зоны покрытия и улучшает качество принимаемого сигнала.

Таким образом, эксплуатация сети ЦЭТВ на территории нашей страны ставит приоритетную задачу, а именно сохранение высокого качества телевизионных программ при доставке их конечному пользователю. Это означает, что у телезрителя 24 часа в сутки должна иметься возможность просмотра без искажений изображения и звука интересующей его ТВ-программы. С учётом этого актуальным является вопрос эффективности методов оценки качества цифрового ТВ-изображения.

Оценка качества ТВ-программ

Сеть цифрового телевизионного вещания в Российской Федерации – это сложный технологический комплекс, состоящий из федерального центра формирования мультиплексов, центров космической связи, спутниковой группировки, региональных центров формирования мультиплексов, радиотелевизионных станций.

На рисунке 1 представлена структурная схема фрагмента сети ЦЭТВ, иллюстрирующая процесс преобразования и передачи цифровых телевизионных сигналов от источников телепрограмм к телезрителю.

Система цифрового эфирного телевизионного вещания включает три этапа доставки телевизионного сигнала от аппаратной формирования программ до телезрителя:

1) Формирование в федеральном центре мультиплексов сигнала пакета программ из сигналов от нескольких вещателей;
2) Доставку сигнала пакета программ мультиплекса до объектов с использованием спутниковой и наземной инфраструктура сети ЦЭТВ.
3) Трансляцию сигнала пакета программ мультиплекса с объекта связи сети ЦЭТВ для непосредственного приема телезрителями.

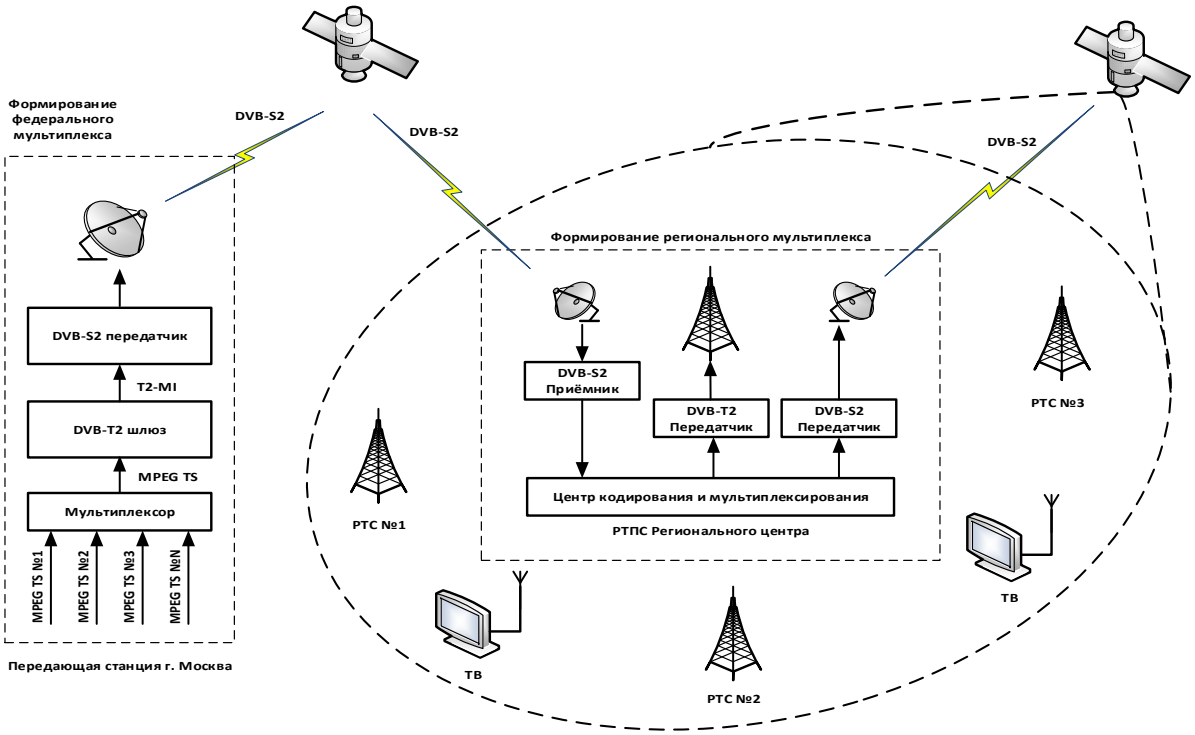


Рис. 1. Структурная схема цифрового телевизионного вещания в Российской Федерации

Для оценки качества ТВ-программ, доставляемых телезрителю, используются два основных подхода: мониторинг параметров транспортного потока и анализ качества изображения и звука, доставляемых телезрителю. В англоязычной литературе данные подходы, как правило, имеют названия «Качество сервиса» (Quality of Service, QoS) и «Качество зрительского восприятия» (Quality of Experience, QoE).

Рассмотрим подробнее применение метода QoS для контроля качества цифровых ТВ-программ в системе DVB-T2.

Термин «QoS» подразумевает оценку характеристик аппаратуры, используемой для построения сети цифрового ТВ-вещания, а также канала передачи. Метод предусматривает обеспечение основных узлов телевизионного тракта профессиональной измерительной аппаратурой, с помощью которой осуществляется круглосуточный мониторинг сети DVB-T2, выявляются проблемные зоны и фиксируются технические сбои в ее работе.

Критерием качества передаваемой ТВ-программы при использовании метода QoS является обеспечение заданного уровня технических характеристик сети DVB-T2. Данный уровень определяется при составлении договора между производителем ТВ-программ (заказчиком) и вещателем (исполнителем). Критериями качества телевизионного тракта в данном методе являются корректность структуры передаваемых цифровых потоков, соответствие радиочастотных параметров излучаемого в эфир сигнала установленным нормам и другие качественные показатели сети.

Очевидно, что для достижения высокого качества «картинки» и звукового сопровождения на экране телевизора необходимо обеспечить контроль соответствия параметров цифрового сигнала согласно ГОСТ Р 55696 и ГОСТ Р 58912-2020 на всех стадиях передачи сигнала [1-3].

При этом не достаточно вести только визуальный контроль с помощью дежурных операторов, как это было принято в аналоговом телевещании, т

Так как постепенное ухудшение параметров цифрового сигнала до определенных значений никак не проявляется на приемном устройстве. Однако при достижении критических значений параметров качество резко снижается до неприемлемого уровня, вплоть до полного прекращения приема сигнала. В связи с этим нужен непрерывный автоматизированный мониторинг параметров цифровых сигналов на всех этапах передачи сигнала с целью своевременного выявления ухудшения параметров и приближения их к критическим значениям.

Для контрольных точек мониторинга целесообразно выбирать точки на стыках звеньев где происходит преобразование сигнала. На рисунке 2 показаны контрольные точки между звеньями, подлежащих контролю.

Рассмотрим подробнее каждую контрольную точку.

Контрольная точка 1 – выход оборудования кодирования и мультиплексирования (выход шлюза T2-MI). В этой точке контролю подлежат параметры 1-, 2- и 3-го приоритетов последовательного асинхронного транспортного потока ASI в соответствии со стандартом ГОСТ Р 55696-2013 [1].

Контрольная точка 2 – вход возбудителя цифрового телевизионного передатчика.

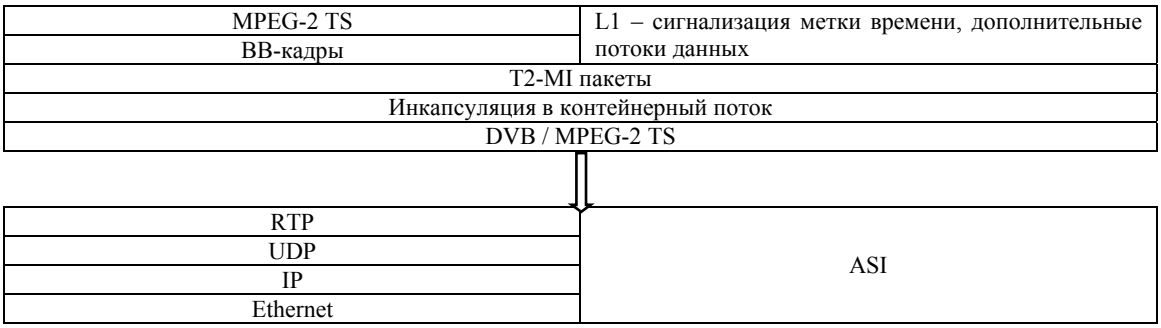
Цифровой поток, доставляемый до входа передатчика, переносит изображение и звук, подвергнутые компрессии (на территории РФ сжатие ТВ-изображения для передачи в системе цифрового эфирного вещания DVB-T2 осуществляется кодером стандарта H.264). При доставке цифрового потока до телевизионного пере-

датчика по каналу связи на него могут воздействовать различные дестабилизирующие факторы, приводящие к искажению передаваемой информации. Если в цифровом потоке без сжатия искажение одного бита в большинстве ситуаций приведет лишь к некорректному отображению одного пиксела в кадре, то в цифровом потоке с компрессией влияние искажений каждого бита чрезвычайно высока. Так, при искажении всего нескольких бит из миллиона в потоке со сжатием изображение на экране может ухудшиться до неузнаваемости. Поэтому на входе передатчика стандарта DVB-T2 в процессе вещания необходимо осуществлять постоянный мониторинг цифрового потока, переносящего ТВ-программы, в частности при работе ТВ-передатчика в режиме подачи на его вход потока T2-MI (T2 Modulator Interface, или интерфейс модулятора T2). Данный вид потока объединяет несколько транспортных потоков MPEG-2 TS, предназначенных для передачи в различных PLP, а также служебную информацию, необходимую для настройки ТВ-передатчика [4-6].

Для контроля качества цифровых потоков на входе ТВ-передатчика подключается соответствующий анализатор, который осуществляет круглосуточный контроль транспортного потока на входе цифрового передатчика. Регламентирующим документом измерений в системах DVB является «Руководство по измерениям в системах DVB. Дополнение для T2-MI (интерфейс модулятора)» [4]. В нем указаны ошибки, наличие которых необходимо проверять в потоке T2-MI. Как показывает практика, контроль наличия ошибок в структуре потока T2-MI является чрезвычайно важным звеном для обеспечения высокого качества ТВ-программ, доставляемых пользователю. Для подтверждения справедливости данного утверждения, необходимо обратиться к технологии формирования потока T2-MI. Пакеты транспортного потока MPEG-2 TS, несущего ТВ-программы, один за другим помещаются в BB-кадры, имеющие собственный заголовок и возможность переноса дополнительной служебной информации. В BB-кадре, в зависимости от выбора режима помехозащитного кодирования, может содержаться до 35 транспортных пакетов MPEG (длиной 188 байт). Сформированные BB-кадры помещаются в T2-MI пакеты, являющиеся частью T2-MI-потока. В T2-MI пакетах также могут передаваться метки времени, обеспечивающие работу цифрового передатчика в режиме одночастотной сети, а также пакеты L1-сигнализации, переносящие набор значений, описывающих режим работы передатчика DVB-T2. Сформированные T2-MI пакеты помещаются в полезную нагрузку транспортных пакетов контейнерного потока MPEG-2 TS, (таблица 1). Данная операция осуществляется для передачи потока T2-MI по уже существующим интерфейсам, разработанным для потока MPEG-2 TS (интерфейсы ASI, SPI, TS over IP и др.). Далее контейнерный поток MPEG-2 TS, содержащий пакеты T2-MI, доставляется на вход передатчика. Передатчик, извлекая данные из пакетов с L1-сигнализацией, самостоятельно настраивается на режим работы и, при условии корректности потока T2-MI, начинает формирование радиосигнала, излучаемого в эфир.

Таблица 1

Стек протоколов для формирования и передачи T2-MI



Распространение потока T2-MI от федерального центра формирования мультиплексов до передатчиков DVB-T2 в регионах с учетом огромных расстояний в нашей стране осуществляется по спутниковым и (или) наземным каналам связи. При этом, как и в случае с любой системой передачи, на спутниковый и наземный канал воздействуют различные дестабилизирующие факторы. При повреждении структуры одного из транспортных пакетов MPEG-2 TS, переносящих T2-MI, велика вероятность того, что будет поврежден целый пакет T2-MI, в котором может переноситься до 35 транспортных пакетов, содержащих изображение и видео. Для цифровых потоков с компрессией повреждение такого количества информации непременно вызовет длительный срыв в отображении ТВ-программы на экране пользователя. В случае, если был поврежден T2-MI-пакет с меткой времени или L1-сигнализацией, также происходит срыв работы передатчика DVB-T2.

Авторами был проведен эксперимент, заключавшийся в подаче на входы ASI и TS over IP передатчика DVB-T2 преднамеренно искаженного потока T2-MI. Каждая из ошибок, приведенная в документе A14-1 [5], вызывает полный срыв в работе ТВ-передатчика и, как следствие, прекращение излучения радиосигнала в эфир. При этом процесс восстановления синхронизации передатчика с потоком T2-MI может занимать длительное время, в течение которого телезритель не будет иметь возможности просмотра телепередач.

Поэтому контроль целостности потока является необходимым условием для обеспечения высокого качества передаваемых программ. Операторам связи следует знать, что корректность структуры транспортного потока, а также нахождение радиочастотных параметров в пределах нормы не гарантируют удовлетворенность телезрителя телепередачей. Даже в случае отсутствия зафиксированных технических сбоев в системе DVB-T2, в изображении на экране телезрителя могут проявляться артефакты и искажения, влияющие на субъективное

качество восприятия ТВ-программ телезрителем. Возможные причины данного явления могут заключаться в том, что в транспортном потоке MPEG-2 TS при воздействии дестабилизирующих факторов могут искажаться биты, находящиеся в полезной нагрузке передаваемых пакетов, где переносятся кадры сжатого изображения и звука. Данная часть транспортных пакетов не контролируется анализаторами транспортных потоков, так как для анализатора она является де факто случайным набором битов. Искажение даже малого числа битов в сжатом кадре может привести к полному его разрушению. Но даже если передаваемые пакеты доходят до телевизионного приемника неискаженными, при декодировании изображения могут проявляться эффекты перекомпрессии, проявляющиеся в виде блочности изображения и других артефактов.

Контрольная точка 3 – высокочастотный выход RF цифрового телевизионного передатчика, точнее, выход направленного ответвителя измерительного отрезка антенно-фидерного тракта между выходом передатчика и фидером передающей антенны. Контролируемые параметры и методы их измерений регламентируются ГОСТ Р 58912-2020 [2].

Контрольная точка 4 – точка размещения измерительного приемника-анализатора с приемной антенной на местности в данной зоне обслуживания.

Методы измерения покрытия в зонах обслуживания и оценка результатов измерений подробно описаны в [1].

Измерение параметров телевизионного сигнала

В соответствии с [1] качество приема сигнала цифрового телевещания в зоне обслуживания при условии соответствия параметров установленным нормам в контрольных точках 1–3 будет зависеть от следующих факторов:

- напряженности электромагнитного поля телевизионного сигнала в точке приема;
- технических характеристик приемной антенны;
- высоты подвеса приемной антенны;
- затухания сигнала в антенном фидере приемной антенны;
- технических характеристик приемного устройства (цифрового телевизионного приемника или приставки);
- уровня мешающих сигналов (помех различного происхождения) в точке приема.

Контрольные точки между звеньями приведены на рисунке 2.

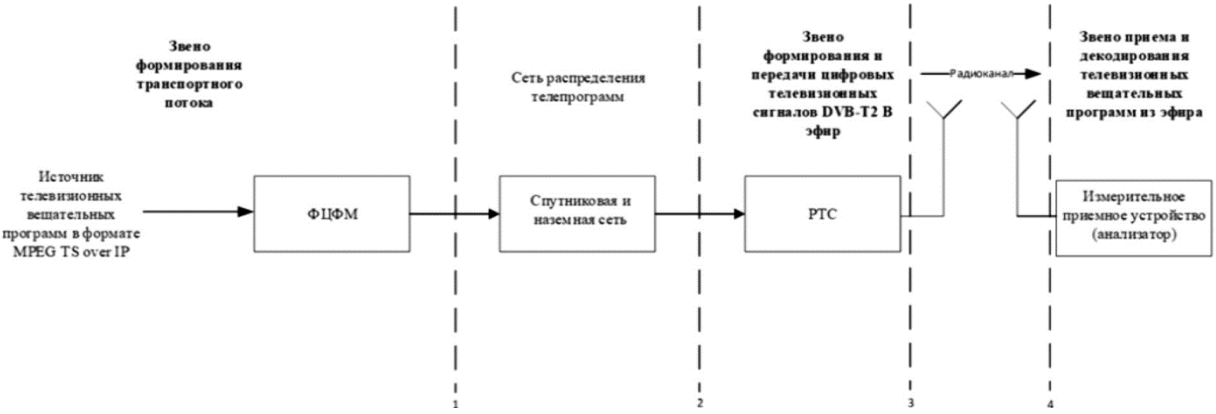


Рис. 2. Контрольные точки

При вводе новых зон обслуживания в эксплуатацию должно проводиться обследование границы зоны в нескольких контрольных точках с целью:

- определения уровня принимаемого сигнала, соотношения сигнал/шум, коэффициента ошибок модуляции MER, коэффициента битовых ошибок BER на выходе фидера приемной антенны в данной точке;
- выбора типа приемной антенны, высоты ее подвеса и ориентации на максимум принимаемого сигнала;
- сравнения измеренных значений с расчетными данными по карте зоны покрытия;
- оценки возможности стабильного качественного приема сигнала в данной точке.

Контрольные точки между звеньями и параметры сигнала сведены в таблицу 2.

В качестве примера в таблице 3 приведены ошибки 1 и 2-го приоритетов, которые оказывают существенное влияние на свойства транспортного потока.

Измерение параметров телевизионного сигнала в выбранной контрольной точке приема производится по схеме, приведенной на рисунке 3.

Перед началом измерений определяют координаты точки приема и ее местоположение на карте зоны покрытия с целью определения азимута на ближайшую РТС. Устанавливают направленную приемную антенну на высоту 3 м в условиях открытой местности и на высоту 10 м в условиях высотной застройки и высокой растительности и ориентируют ее на ближайшую РТС. Настраивают измерительный приемник-анализатор на частоту ТВ канала данной зоны и уточняют ориентацию антенны по максимуму принимаемого сигнала. Если точка приема находится в зоне интерференции (рис. 4), то приемную антенну необходимо ориентировать последова-

тельно на все РТС данной одночастотной зоны для нахождения направления максимального уровня принимаемого сигнала.

Таблица 2

Контрольные точки между звеньями и параметры сигнала

Контрольная точка	Выход оборудования кодирования и мультиплексирования (шлюза T2-MI)	Вход возбудителя цифрового передатчика	Высокочастотный выход цифрового передатчика	Выход абонентской приемной антенны
Цифровой сигнал	Многопрограммный транспортный поток	Многопрограммный транспортный поток	Модулированный радиосигнал DVB-T2	Модулированный радиосигнал DVB-T2
Интерфейс	ASI MPEG TS (ASI T2-MI)	ASI MPEG TS (ASI T2-MI)	RF	RF
Контролируемые параметры	Ошибки 1-, 2-, 3-го приоритетов транспортного потока	Ошибки 1-, 2-, 3-го приоритетов транспортного потока	Выходная мощность, коэффициент ошибок модуляции MER, коэффициент битовых ошибок BER, отклонение центральной частоты канала, ошибки 1-, 2-, 3-го приоритетов транспортного потока	Уровень сигнала, соотношение сигнал/шум, коэффициент ошибок модуляции MER, коэффициент битовых ошибок BER

Таблица 3

Ошибки параметров 1-, 2-го приоритетов

Название ошибки	**Описание ошибки**	**Влияние ошибки на оценку качества транспортного потока**
1-й приоритет		
1.1 TS_sync_loss	Потеря синхронизации транспортного потока	Фатальная ошибка. До восстановления синхронизации измерения и проверки транспортного потока невозможны
1.2 Sync_byte_error	Ошибка приема байта синхронизации транспортного потока	В массовом проявлении, граничащем со срывом синхронизации, может внести существенный вклад в общее ухудшение качества транспортного потока. В единичных случаях не влияет на качество транспортного потока
1.3 PAT_error	Ошибка таблицы соединения программ	Редкие сбои могут привести к задержке декодирования. Постоянный сбой приводит к невозможности декодирования
1.4 Continuity_count_error	Нарушение непрерывности счета	Влияет на декодируемость и помехозащищенность транспортного потока
1.5 PMT_error	Ошибка таблицы структуры программ	Редкие сбои могут привести к задержке декодирования. Постоянный сбой приводит к невозможности декодирования
1.6 PID_error	Ошибка в определении идентификации пакета	Не используется в алгоритме
2-й приоритет		
2.1 Transport_error	Ошибка в транспортном пакете	Влияет на декодируемость транспортного потока
2.2 CRC_error	Ошибка циклического контроля всех таблиц	Влияет на информативность и помехозащищенность транспортного потока
2.3 PCR_error	Ошибка в передаче сигнала синхронизации задающего генератора	Возможны влияние на помехоустойчивость и сбои в декодировании программы или группы программ. Полное отсутствие PCR влечет за собой невозможность декодирования программы или группы программ
2.4 PCR_accuracy_error	Ошибка точности значений PCR более ±500 нс	Возможны влияние на помехоустойчивость и сбои в декодировании программы или группы программ
2.5 PTS_error	Ошибка меток времени представления	Возможны влияние на помехоустойчивость и сбои в декодировании данных
2.6 CAT_error	Ошибка таблицы условного доступа	Редкие сбои могут привести к задержке, а постоянный сбой приводит к невозможности декодирования закрытых программ или группы закрытых программ

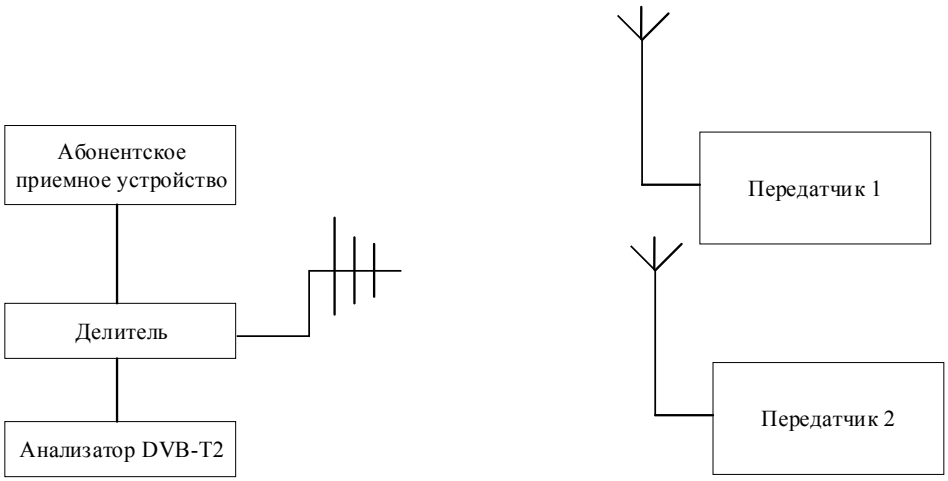


Рис. 3. Схема измерений параметров телевизионного сигнала

Далее замеряют уровень сигнала, соотношение сигнал/шум, параметры MER, BER. На абонентском приемном устройстве фиксируют показания индикаторов «уровень» и «качество» (в процентах) и контролируют наличие квазибезошибочного приема на абонентском приемном устройстве. Критерием квазибезошибочного приема является отсутствие событий срыва изображения или звука, а также известных артефактов («рассыпание», «замораживание») на воспроизводимом изображении. При появлении таких событий испытания производят три раза.

Данные измерений и контролируемых параметров приведены в таблице 4.

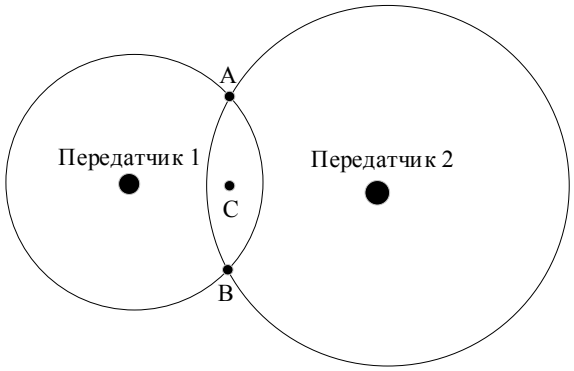


Рис. 4. Точка С в зоне интерференции двух передатчиков

Измеренные значения параметров сравнивают с их расчетными величинами на карте зон покрытия и пороговыми значениями, при которых еще возможен стабильный квазибезошибочный прием (получены опытным путем при проведении полевых натурных испытаний):

Таблица 4

Значения при проведении полевых натурных испытаний

Уровень сигнала, дБм	**MER, дБ**	**BER**	**Показания индикаторов приемного устройства, %**		**Наличие квазибезошибочного приема**
			Уровень	**Качество**	
69,0-70,0	20-21	10^{-4}-10^{-6}	17-18	18-19	Есть

Для гарантированного обеспечения качественного приема необходимо, чтобы запас по показателям уровня и качества приемного устройства составлял не менее 50%.

В зависимости от полученных результатов делаются выводы:

1. Измеренные параметры соответствуют расчетным данным карты зоны покрытия.

2. Возможность качественного приема в данной точке:

качественный стабильный прием в данной точке обеспечивается на направленную антенну высотой 10 м, ориентированную на Передатчик 1.

Описанную методику следует также применять в случаях поступления жалоб от телезрителей на плохое качество приема в отдельных населенных пунктах, кварталах и улицах.

Информация о состоянии параметров сигналов и оборудования в контрольных точках 1 – 4 должна поступать в автоматизированную систему управления и мониторинга сети, которая выполняет следующие функции:

• непрерывный, в режиме реального времени анализ состояния сети в целом и ее отдельных звеньев (формирования телевизионных программ, формирования и передачи цифровых потоков, передачи цифровых телевизионных сигналов и приема телевизионных вещательных программ);

• контроль параметров транспортного потока на входе и выходе цифровых передатчиков DVB-T2;

• контроль высокочастотных параметров передатчиков;

• контроль наличия вводов электроснабжения на входе объекта мониторинга;

• удаленный контроль и управление устройствами электроснабжения, установленными на объекте мониторинга.

Дополнительно система мониторинга может обеспечивать:

• возможность видеонаблюдения за объектами мониторинга при срабатывании датчика движения;

• возможность технологической связи между персоналом аварийно-профилактических групп, выезжающих на объекты мониторинга, и персоналом центра управления, РТС и других объектов мониторинга;

• возможность передачи сигналов охранно-пожарной сигнализации от объектов мониторинга до центра управления.

Поступающая от установленного в контрольных точках измерительного оборудования информация должна быть обработана и интерпретирована таким образом, чтобы дежурные операторы сети могли принять адекватное корректирующее воздействие.

Заключение

Для повышения объективности используемых методов оценки качества принимаемого ТВ сигнала необходимо измерять как можно больше параметров в различных узлах тракта DVB-T2, которые способны влиять на результирующее качество изображения и звука. С учётом этого необходимо модернизировать и использовать систему автоматического контроля радиочастотных параметров цифровых телевизионных передатчиков и параметров приема телевизионного сигнала в зонах обслуживания.

Литература

1. ГОСТ Р 55696-2013 – Передающее оборудование для цифрового наземного телевизионного вещания DVB-T/T2 (Технические требования. Основные параметры. Методы измерений);
2. ГОСТ Р 58912-2020 – Система эфирного наземного цифрового телевизионного вещания второго поколения DVB-T2;
3. *Зеленин С.А., Орлов В.Г.* Развитие технологий телевидения высокой четкости // Фундаментальные проблемы радиоэлектронного приборостроения. 2013. Т. 13. № 5. С. 155-158.
4. ETSI TS 102773 Digital Video Broadcasting (DVB); Modulator Interface (T2MI) for a Second generation digital terrestrial television broadcasting system (DVB-T2). V. 1.3.1. (201212)
5. DVB Document A14-1 Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems; Amendment for T2-MI (Modulator Interface). (2012-07)
6. Балобанов А.В., Балобанов В.Г. Метод сжатия цифрового видеосигнала в прикладном телевидении для управления и контроля БПЛА // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 1. С. 16-21.

ANALYSIS OF THE INFLUENCE ON IMAGE QUALITY OF PARAMETERS AND SIGNAL CHARACTERISTICS IN DIGITAL BROADCAST TELEVISION SYSTEMS

Stanislav G. Dolgov,
Head of the Department of the TPDN, Federal State Unitary Enterprise RTRS, Moscow, Russia,
dolgov.stan@yandex.ru

Andrey V. Balobanov,
Associate Professor of the Department of T&SV, Ph.D., MTUCI, Moscow, Russia,
a.v.balobanov@mtuci.ru

Abstract

The analysis of parameters and characteristics of image signals in digital television systems and their influence on the quality of the transmitted signal, taking into account the specifics of terrestrial television broadcasting systems of the DVB-T2 standard, is presented. The main approaches to monitoring the parameters of the traffic stream and their influence on the quality of the transmitted signal, as well as the presence of distortions and artifacts in the image, are considered. As control points of monitoring, it is advisable to choose points at the joints of the links, where the digital signal is converted.

Key words: *DVB-T2 digital broadcasting system, QoS, QoE, coding and multiplexing equipment output, digital TV transmitter exciter input, RF digital TV transmitter high-frequency output, measuring receiver-analyzer.*

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ OFDM СИГНАЛА В СИСТЕМЕ IoT «СТРИЖ»

Соловьев Александр Сергеевич,
ассистент кафедры МКиИТ, МТУСИ, Москва, Россия,
a.s.solovev@mtuci.ru

Кряжева Кристина Дмитриевна,
студентка МТУСИ, Москва, Россия,
kriazheva.k@gmail.com

Аннотация
В данной работе проведен анализ концепции «Интернет вещей» (IoT). Рассмотрены основные понятия IoT, области применения, технологии передачи, рассмотрен протокол связи XNB, разработанный компанией «СТРИЖ Телематика» на базе технологии LPWAN. В статье рассматривается современная телеметрическая система «СТРИЖ», являющаяся одной из современных разработок для интернета вещей. Целью исследования является определение возможности применения сигнала OFDM в системе интернета вещей «СТРИЖ». Разработана структурная схема модернизированной системы «СТРИЖ» с учетом применения в ней сигнала OFDM. Проведен расчёт основных параметров системы с технологией OFDM, результаты которого позволяют разработать компьютерную имитационную модель рассматриваемой системы «СТРИЖ» с применением сигнала OFDM и реализовать модем данной системы на современной элементной базе.

Ключевые слова: *Интернет вещей, система M2M, сигнал OFDM, система «СТРИЖ», сеть LPWAN, ISM диапазон частот, передача телеметрии, нелицензируемый спектр.*

В наше время в сфере инфокоммуникаций активно развивается «Интернет вещей» (англ. Internet of Things, IoT). В последние годы количество подключённых к сети устройств превысило число пользователей. Концепция «Интернета вещей» (англ. Internet of Things, IoT) заключается в создании взаимодействия между несколькими устройствами или устройствами и окружающей средой с целью более тесной интеграции реального и виртуального миров [8]. Это позволяет разрабатывать приложения для автоматизации, сбора данных и межмашинного взаимодействия (англ. Machine-to-Machine, M2M). Технологии «Интернета вещей» сейчас могут использоваться во многих отраслях: сельское хозяйство, медицина, строительство, городские инфраструктуры (такие как системы ЖКХ), системы безопасности, транспорта и др. Сегодня Интернет вещей состоит из слабо связанных между собою разрозненных сетей, каждая из которых была развернута для решения своих специфических задач. По мере развития Интернета вещей существующие сети будут подключаться друг к другу и приобретать все более широкие возможности в сфере безопасности, аналитики и управления [7].

Для передачи данных в IoT используются как проводные, так и беспроводные технологии. Проводные сети в основном базируются на решении PLC (англ. Power line communication – «Связь через линии электропередачи») – технологии построения сетей по линиям электропередач, и используются для банкоматов, торговых автоматов, контроллеров освещения и др.[8]. В беспроводной передаче данных используются протоколы и технологии ZigBee, Wi-Fi, VSAT, Bluetooth, 2G/3G/4G, LPWAN, NB-IoT.

Для IoT-технологий важны такие параметры как энергозатратность, емкость сети и дальность связи. Технология LPWAN (англ. Low-power Wide-are Network – «энергоэффективная сеть дальнего радиуса действия»), в отличие от других современных беспроводных технологий, способна обеспечить энергоэффективную передачу небольших пакетов данных на дальние расстояния. На базе данной технологии в России была разработана система передачи «СТРИЖ».

Система «СТРИЖ»

Компания-разработчик «СТРИЖ Телематика» начала работу в 2010 году с запуска устройств для беспроводной передачи показаний со счетчиков. В 2014 году эта компания представила свой собственный LPWAN-протокол XNB (Extended Narrowband – расширенный узкополосный).

Система «СТРИЖ» использует топологию сети «звезда». Любой прибор или датчик, подключённый к радиомодему «СТРИЖ», либо прибор с уже интегрированным модемом, напрямую передают пакеты данных на базовую станцию с заданной периодичностью (рис. 1). Базовая станция служит как устройство сбора и передачи данных. Базовые станции «СТРИЖ» построены на LPWAN-технологии, благодаря чему радиус передачи достигает до 10 км, при крайне малом энергопотреблении. Одна базовая станция может обслужить до 2 млн. устройств. Далее с базовой станции данные передаются на сервер для последующей обработки. С сервера данные отправляются к диспетчеру или на компьютер пользователю. Система «СТРИЖ» поддерживает полнодуплексный режим связи. Обратный канал позволяет удаленно управлять приборами.

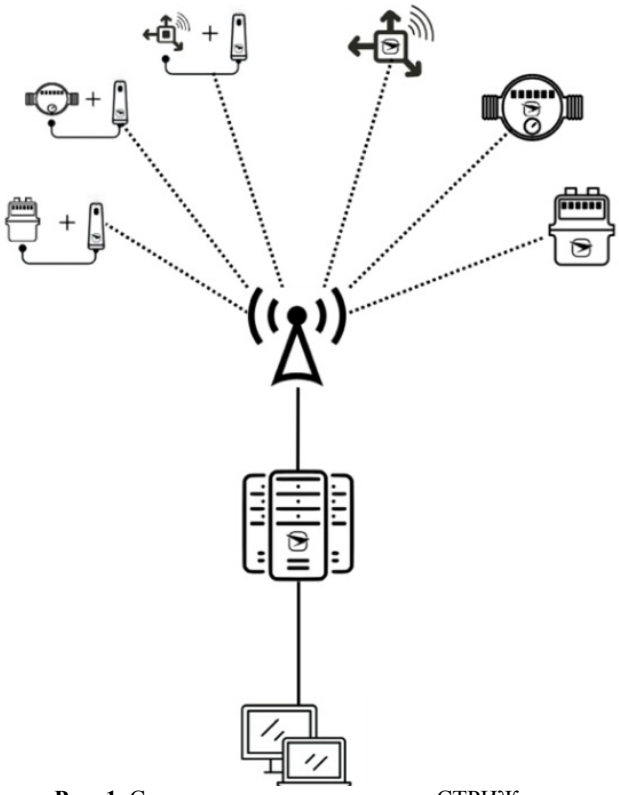


Рис. 1. Структурная схема системы «СТРИЖ»

Абонентское оборудование системы «СТРИЖ»

Компания «СТРИЖ Телематика» представляет на рынке готовые интегрированные plug-and-play устройства (рис. 2). Например, счётчики воды и электроэнергии, теплосчётчики, датчики протечек, датчики открытия со следующими характеристиками:

- До 10 км дальность связи в городе. Опрос показаний в многоквартирном доме без промежуточного оборудования;
- До 10 лет работы от аккумуляторной батареи. Не требует обслуживания в течение всего срока эксплуатации до поверки;
- Датчик несанкционированного оборудования. Оповещает диспетчера в личном кабинете о применении несанкционированного оборудования (магнита);
- Обеспечивает общедомовые нужды. Предотвращает хищения, обратный ток воды, самостоятельно передаёт показания;
- Дистанционное ограничение нагрузки и отключение реле;
- Оповещения о событиях: вскрытие, потеря питания;
- Передача статистики потребления раз в час.

а) б) с)

Рис. 2. Основные элементы системы «СТРИЖ»: счётчик воды СВК (а); однофазный электросчётчик (б); радиомодем «СТРИЖ» (в) [8]

В рассматриваемой системе применяется беспроводной энергоэффективный LPWAN-протокол дальнего радиуса действия XNB. В его основе лежит узкополосный сигнал с относительной двоичной фазовой модуляцией (DBPSK). Сигнал системы «СТРИЖ» представляет собой сигнал с прямым расширением спектра или сложный фазоманипулированный сигнал с применением современных кодовых последовательностей типа М-последовательности, последовательности Голда и др. Это позволяет получить большой энергетический потенциал канала связи до 174 дБм [8] и обеспечивать скорость передачи данных 100 бит/с [9].

Данный протокол XNB имеет ряд преимуществ:

- Дальность передачи сигнала – в городской среде она составляет 10 км, а в условиях открытой местности до 50 км;
- Высокая проникающая способность – возможность размещать устройства в подвалах, там, где не ловит сотовая связь;
- Нелицензируемый ISM-диапазон;
- Низкая мощность передачи.

Используемый системой «СТРИЖ» ISM-диапазон (англ. Industrial, Scientific, Medical – «частоты для индустриального, специального и медицинского оборудования») является радиочастотным спектром общего пользования и не требует лицензирования при условии соблюдения норм, описанных в Решении ГКРЧ № 07-20-03-001 от 07.05 2007 [5]. Использование ISM-диапазона является оптимальным решением для беспроводных систем контроля, управления и сбора данных. Радиоволны данного диапазона хорошо проникают сквозь бетонные и кирпичные стены [4]. Данный диапазон часто является нелицензируемым, то есть абонентам и производителям оборудования системы «СТРИЖ» не нужно тратить время и средства на получение лицензии на использование данного диапазона.

Согласно ГКРЧ №08-24-01-001 [6] в Российской Федерации к ISM-диапазону относят 433 МГц, 868 МГц и 2,4 ГГц. В системе «СТРИЖ» передача данных происходит в диапазоне частот 868,8 МГц при мощности не более 25 мВт при ширине полосы канала передающего устройства равной 100 Гц.

Как правило, системы, использующие ISM-диапазон, отличаются небольшим электропотреблением и низкой скоростью передачи. Но в последнее время видна тенденция к увеличению скорости передаваемых данных, а значит, к увеличению нагрузки на сеть в данном диапазоне частот. На работу беспроводных систем воздействуют помехи, создаваемые другими устройствами и многолучевым распространением сигнала в условиях с различной плотностью застройки местности, что приводит к различным замираниям сигнала. Решением данной проблемы может быть использование OFDM технологии.

Применение OFDM в системе «СТРИЖ»

Ортогональное частотное разделение с мультиплексированием (англ. Orthogonal Frequency Division Multiplexing, OFDM) представляет собой одновременную передачу потока цифровых данных по нескольким частотным каналам. Эта технология позволяет передавать большое количество бит данных с помощью множества сигналов в одном частотном канале [2, 10-21].

Данная технология имеет следующие **преимущества**:

- высокая устойчивость к узкополосным и частотно-селективным замираниям;
- высокая спектральная эффективность;
- простота реализации относительно аналогичных систем и адаптивность;
- и недостатки:
- снижение энергоэффективности, из-за высокого значения пик-фактора;
- высокая чувствительность к смещению частоты и фазы сигнала на приеме;
- низкая спектральная эффективность, из-за использования защитных интервалов;

При использовании технологии OFDM в системе «СТРИЖ» изменится структурная схема рассматриваемой системы. Структурная схема модема системы «СТРИЖ» с применением технологии OFDM представлена на рисунке 3.

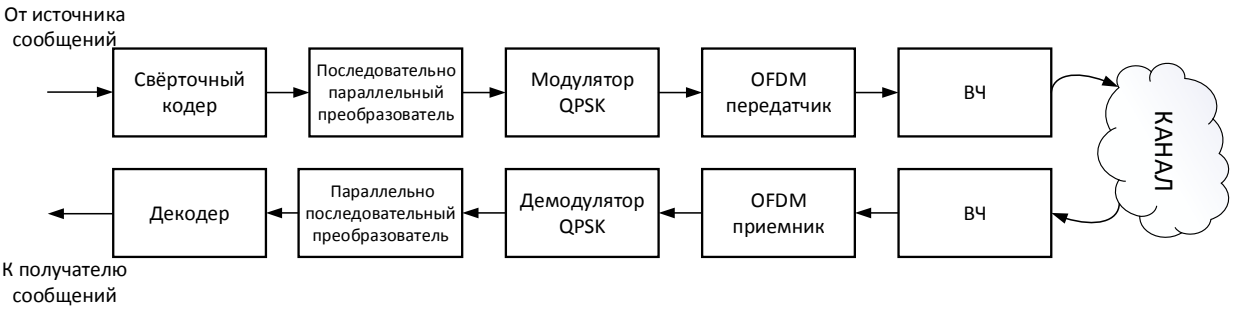


Рис. 3. Структурная схема модема «СТРИЖ» с сигналом OFDM

Структурная схема модема системы «СТРИЖ» с сигналом OFDM повторяет классическую структурную схему модема OFDM. Поток символов передаваемого сообщения с входа модема, поступает на свёрточный кодер, где кодируется помехоустойчивым кодом. Это необходимо для увеличения помехоустойчивость системы. Затем цифровой поток поступает на блок преобразователя последовательного кода в параллельный, где он делится на несколько параллельных подпотоков N. Каждый подпоток модулируется в блоке QPSK модулятора и поступает на блок OFDM передатчика, где выполняется обратное быстрое преобразование Фурье (ОБПФ). С помощью ОБПФ формируются отсчёты комплексной огибающей OFDM-символа:

$$u(t) = \sum_{i=0}^{N-1} d_i \exp\left(-j2\pi \frac{i}{T}(t - t_k)\right), t_k \le t \le (t_k + T), \quad (1)$$

где $i = 0 \dots N-1$, - порядковый номер символа; d_i –модулированный-символ с номером i; T – длительность одного OFDM-символа, который начинается в момент времени t_k.

Далее добавляются отсчёты синхросигналов. Из последних n отсчетов OFDM-символа формируются отсчеты циклического префикса и добавляются спереди к сформированному OFDM-символу. Таким образом, на выходе блока OFDM передатчика получается вектор из $N_{\text{отч}}$ отсчётов с комплексной огибающей OFDM-символа. В блоке ВЧ происходит формирование квадратурных составляющих сигнала и перенос сформированного сигнала на рабочую частоту системы. В блок ВЧ входят блоки формирования квадратурных компонент сигнала, фильтрация сигнала для снижения влияния гармоник высших порядков на соседние диапазоны частот, сложение, цифро-аналоговое преобразование и преобразование частоты сигнала. Затем сигнал передаётся по каналу связи, где подвергается искажению из-за воздействия на него шумов, помех и многолучевого распространения сигнала.

В приёмнике выполняются операции обратные операциям передатчика. В блоке ВЧ, также как и на передающей стороне, производится фильтрация сигнала, усиление, разделение квадратурных компонент сигнала, аналого-цифровое преобразование. Далее сигнал попадает на блок OFDM приёмника, где производится основная операция декомпоновки OFDM-символа – отделение циклического префикса от основного OFDM-символа, вычитание отсчётов синхросигналов, выделение отсчётов передаваемых символов с QPSK модуляцией, последовательно-параллельное преобразование и оценивание QPSK-символов с помощью алгоритма БПФ, производится обработка сигнала в блоке QPSK демодулятора. Параллельно с декомпоновкой OFDM-символа по отсчетам синхросигналов производится оценка параметров канала и компенсация влияния канала на сигнал. Затем формируется последовательный поток в блоке параллельно-последовательного преобразователя и декодируется для получения исходного сигнала и оценки ошибок системы. Вышеупомянутые блоки будут учтены в настоящей структурной схеме для дальнейшего построения имитационной компьютерной модели в Matlab, для оценки помехоустойчивости системы «СТРИЖ» с применением сигнала OFDM и проведена оценка эффективности применения сигнала OFDM для передачи телеметрических данных в ISM диапазоне частот.

Результаты исследования модема системы «СТРИЖ» с сигналом OFDM

В ходе исследования были определены основные параметры системы «СТРИЖ» с применением в ней OFDM сигнала по известной методике описанной в [1-3]. Рассчитанные параметры для данной системы представлены в таблице 1. Полученные в результате расчета параметры исследуемой системы позволяют реализовать систему «СТРИЖ» с применением сигнала OFDM на современной элементной базе.

При сравнении параметров системы «СТРИЖ» и рассчитанных параметров той же системы с OFDM-сигналом видно, что дальность увеличилась с 10 км [9] до 12,6 км, а скорость передачи данных увеличилась более чем в 1,5 раза, с 100 бит/с [9] до 175 бит/с.

Таблица 1

Параметры системы «СТРИЖ»

№	Параметр	Значение
1	Длительность защитного интервала, $T_{защ}$, с	$0{,}2*10^{-3}$
2	Длительность интегрируемой части OFDM-символа, T, с	$5{,}5*10^{-3}$
3	Расстояние между поднесущими Δf, Гц	10 Гц
4	Количество используемых поднесущих в заданной полосе частот, $N_{исп.подн}$	10
5	Метод модуляции	QPSK
6	Количество используемых поднесущих для передачи данных (кодовых бит), $N_{подн.код.бит}$	4
7	Количество поднесущих в одном OFDM-символе, $N_{подн}$	8
8	Количество неиспользуемых (нулевых) поднесущих, N_0	1
9	Интервал дискретизации по времени комплексной огибающей OFDM-символа, Δt,	$1{,}25*10^{-3}$
10	Количество отсчётов огибающей OFDM-символа на защитном интервале, $N_{защ}$	2
12	Длительность OFDM-символа, T_c, с	$5{,}7*10^{-3}$
13	Общее число отсчётов огибающей OFDM-символа, $N_{отсч}$	10
14	Количество кодовых бит на одной поднесущей или в одном модулированном-символе, $N_{битМод}$	2
15	Количество кодовых бит в одном OFDM-символе (блоке), $N_{код.бит.бл}$	8
16	Количество информационных бит в одном OFDM-символе (блоке) на входе кодера, $N_{инф.бит.бл}$	4
17	Выходная мощность передатчика, дБм	14
18	Дальность системы, D, м	12600
19	Скорость передачи данных V, бит/с	175

Построение системы «СТРИЖ» на основе сигналов, сформированных по технологии OFDM, позволяет увеличить скорость передачи данных и снизить время работы в диапазоне частот, что повышает эффективность использования рабочего диапазона частот и снижает влияние системы «СТРИЖ» на другие системы передачи данных, работающие в ISM диапазоне частот. Свойства сигнала OFDM позволяют бороться с влиянием многолучевого канала и применять оборудование в городах с очень плотной застройкой и обеспечивать большую скорость передачи данных и большую дальность связи. Также применение технологии OFDM и переход на цифровую реализацию оборудования системы «СТРИЖ» позволяют реализовать модемы на современной элементной базе, которая поддерживает высокие скорости обработки сигнала и высокие скорости передачи данных. К тому же переход на современные цифровые сигнальные процессоры позволяет облегчить разработку оборудования, его переконфигурирование и модернизацию. Аналоговые элементы оборудования системы «СТРИЖ», такие как фильтры на ПАВ, линии задержки сигналов и корреляторы, можно будет реализовать на цифровых сигнальных процессорах как согласованные с сигналом фильтры и различные считающие автоматы. Это позволит снизить затраты на реализацию модемов, их модернизацию и разработку новых модемов на более эффективных сигналах и методов передачи данных, а также применить методы, обеспечивающие защиту информации и безопасность связи.

Выводы

1. В работе обоснована возможность применения OFDM-сигнала для системы «СТРИЖ».
2. Разработана структурная схема модема, определены основные параметры сигнала и разработана компьютерная имитационная модель современной системы радиодоступа «СТРИЖ» с применением в ней сигнала OFDM.
3. Применение в рассматриваемой системе сигнала OFDM позволило повысить дальность до 12600 м и скорость до 175 бит/с.
4. Разработана структурная схема модема системы «СТРИЖ» с применением OFDM сигнала и определены основные параметры, пригодные для реализации на современной элементной базе.
5. Необходимо произвести исследование помехоустойчивости системы «СТРИЖ» с применением сигнала OFDM с учётом различных моделей канала.
6. Необходимо провести оценку возможности реализации модема рассматриваемой системы «СТРИЖ» с сигналом OFDM на современной элементной базе.

Литература

1. *Бакулин М. Г., Крейнделин В. Б., Шлома А. М., Шумов А. П. и др*. Технология OFDM: учебное пособие для вузов. М.: Горячая линия – Телеком, 2017. 360 с.
2. *Волков Л. Н., Немировский М. С., Шинаков Ю. С.* Системы цифровой радиосвязи: базовые методы и характеристики: учебное Пособие. М.: Эко-Трендз, 2005. 392 с.
3. *Журавлев В. И., Трусевич Н. П.* Методы модуляции-демодуляции радиосигналов в системах передачи цифровых сообщений. М.: Инсвязьиздат, 2009. 312 с.
4. Легализация устройств в ISM диапазоне [Электронный ресурс]: https://eje.short.gy/eBNsKV (дата обращения 07.04.2021).
5. Решение ГКРЧ от 07.05.2007 №07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия», 2007. 10 с.
6. Решение ГКРЧ от 28.04.2008 №08-24-01-001 «О внесении изменений в решение ГКРЧ от 07.05.2007 N 07-20-03-001 " О выделении полос радиочастот устройствам малого радиуса действия", 2008. 5 с.
7. *Эванс Д.* Интернет вещей. Как изменится вся наша жизнь на очередном витке развития Всемирной сети. Официальный документ Группа разработки интернет-решений Cisco для бизнеса (IBSG). 2011. 14 с.
8. *Орлов В.Г., Тюмин С.Г.* Стандарты беспроводной связи для системы умный дом // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 20-28.
9. LPWAN-технология «СТРИЖ» и беспроводной протокол XNB. Описание продуктов и технологии «СТРИЖ» / Системы «СТРИЖ» // ООО «ССРТ». С. 20. [Электронный ресурс]: https://strij.tech/wp-content/download/docs/strij-iot-platforma-strij.pdf?utm_source=robot-auto-answer&utm_medium=email&utm_campaign=download-brochure-iot-platforma-strij&utm_content=brochure-download&utm_term=button-brochure. (дата обращения 17.04.2021).
10. *Бакулин М.Г., Крейнделин В.Б.* Проблема повышения спектральной эффективности и емкости в перспективных системах связи 6G // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 25-31.
11. *Крейнделин В.Б., Григорьева Е.Д.* Модификация метода билинейного преобразования для синтеза цифровых фильтров // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 1. С. 4-9.
12. *Крейнделин В.Б., Григорьева Е.Д.* Реализация банка цифровых фильтров с пониженной вычислительной сложностью // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 7. С. 48-53.
13. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Алгоритмы нелинейной фильтрации двоичной лрп со случайной задержкой и случайной начальной фазой // Системы синхронизации, формирования и обработки сигналов. 2019. Т. 10. № 2. С. 45-51.
14. *Крейнделин В.Б., Резнёв А.А.* Матрица пространственно-временного кода высокой размерности типа "голден" // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 6. С. 34-40.

15. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Анализ пропускной способности канала MIMO в условиях замираний // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 2. С. 13-20.
16. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Методы приема псевдослучайных последовательностей в системах радиосвязи // REDS: Телекоммуникационные устройства и системы. 2018. Т. 8. № 1. С. 108-112.
17. *Крейнделин В.Б., Усачев В.А.* LTE-advanced pro как основа для новых сценариев M2M // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 28-32.
18. *Крейнделин В.Б., Старовойтов М.Ю.* Повышение помехоустойчивости системы связи MIMO с пространственным мультиплексированием методом додетекторного сложения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 4-13.
19. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Исследование вероятностных моделей радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон с помощью компьютерного моделирования // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 1. С. 64-68.
20. *Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К.* Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 24-30.
21. *Крейнделин В.Б., Панкратов Д.Ю.* Вероятностная модель радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 1. С. 103-107.

RESEARCH OF THE POSSIBILITY OF APPLICATION OFDM SIGNAL IN THE IOT SYSTEM "STRIZH"

Alexander S. Soloviev,
Assistant of the Department of MC&IT, MTUCI, Moscow, Russia,
a.s.solovev@mtuci.ru

Kristina D. Kryazheva,
Student of MTUCI, Moscow, Russia,
kriazheva.k@gmail.com

Abstract

This paper analyzes the concept of the Internet of Things (IoT). The basic concepts of IoT, application areas, transmission technologies are considered, the XNB communication protocol, developed by the STRIZH Telematics company based on LPWAN technology, is considered. The article examines the modern STRIZH telemetry system, which is one of the modern developments for the Internet of things. The aim of the study is to determine the possibility of using the OFDM signal in the "STRIZH" Internet of Things system. The structural diagram of the modernized "STRIZH" system has been developed, taking into account the use of the OFDM signal in it. The calculation of the main parameters of the system with the OFDM technology has been carried out, the results of which make it possible to develop a computer simulation model of the considered system "STRIZH" using the OFDM signal and to implement the modem of this system on a modern element base.

Keywords: *Internet of Things, M2M system, OFDM signal, STRIZH system, LPWAN network, ISM frequency range, telemetry transmission, unlicensed spectrum.*

АНАЛИЗ СИСТЕМЫ РАДИОДОСТУПА WI-FI СТАНДАРТА IEEE 802.11AX

Фролов Алексей Андреевич,
старший преподаватель кафедры РТС, к.т.н., МТУСИ, Москва, Россия,
a.a.frolov@mtuci.ru

Литвинов Илья Владимирович,
студент МТУСИ, Москва, Россия,
lighthummer99@gmail.com

Аннотация
В данной работе рассматриваются причины появления нового стандарта и его особенности. Кратко описаны новые технологии, примененные в системе радиодоступа Wi-Fi. Проведен анализ изменений в сигнале, системы радиодоступа стандарта IEEE802.11ax по сравнению с предыдущим стандартом IEEE 802.11ac. Описана структурная схема и принцип работы модема стандарта IEEE 802.11ax. Определены числовые значения параметров модема системы радиодоступа стандарта IEEE802.11ax для последующей его реализации на современной элементной базе.

Ключевые слова: *система Wi-Fi, сигнал OFDM, нелицензируемый спектр, повышение эффективности спектра, стандарт IEEE 802.11ax, стандарт IEEE 802.11ac.*

Общемировая тенденция к росту скорости передачи данных и расширению числа пользователей в сети Wi-FI является основной причиной появления нового стандарта радиодоступа IEEE 802.11ax (Он же Wi-FI 6). Система Wi-FI 6 основана на стандарте 802.11ac, появившемся в 2019 году и являющимся самым современным на данный момент стандартом 802.11. Высокий спрос на такие технологии обусловлен несколькими факторами. Во-первых, появляется всё больше услуг, использующих сети связи, например, услуги записи к врачу или дистанционного обучения. Во-вторых, стремительно увеличивается число пользователей интернета на земле и соответственно количества гаджетов, которыми они пользуются. Также стоит учитывать, что в связи с развитием технологий большинство пользователей имеет даже не по одному, а по несколько устройств, некоторые из которых требуют постоянного подключения к интернету, такие как станции систем умного дома или мультимедиа с искусственным интеллектом. В новом стандарте появилась возможность использования сразу двух диапазонов частот, применяемых в сетях Wi-Fi – диапазона в районе 2,4 ГГц и диапазона 5 ГГц, тем самым увеличив доступный частотный ресурс. Особенностями Wi-Fi 6 являются внедрение технологий: OFDMA, 8x8 MU-MIMO, BSS Color и Beamforming.

Описание системы Wi-Fi

Система радиодоступа Wi-Fi – это технология беспроводной передачи данных, формирующая беспроводную локальную сеть (WLAN). В принцип работы Wi-Fi заложена передача сигналов при помощи модуляции OFDM (Orthogonal Frequency Division Multiplexing, мультиплексирование с ортогональным разделением каналов), которая реализуется на основе быстрого преобразования Фурье. На рисунке 1 изображена структурная схема передатчика и приемника модема системы радиодоступа Wi-Fi 6.

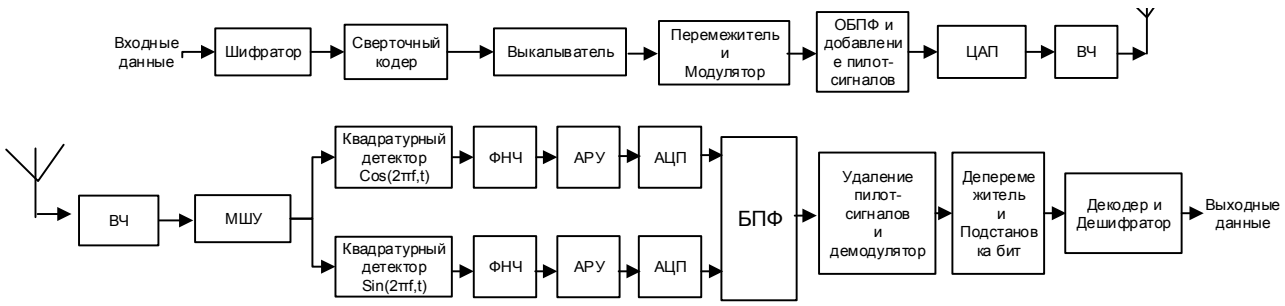


Рис. 1. Структурная схема передатчика и приемника многочастотной системы с OFDM

Структурная схема системы Wi-Fi 6 очень похожа на схему стандартных OFDM модемов. Основные отличия рассматриваемой системы заключаются в функциональных возможностях некоторых блоков структурной схемы. На принцип формирования сигнала системы Wi-Fi 6 эти особенности не оказывают влияния на функ-

циональных возможностях системы. Изменения отражаются лишь на параметрах формируемого OFDM-сигнала.

Принцип работы структурной схемы на рисунке 1 следующий: передаваемое сообщение в передатчике, кодируется в сверточном кодере для повышения помехоустойчивости системы передачи данных. После канального кодирования, в выкалывателе увеличивается скорость передачи данных за счет удаления бит данных по заданному вектору. С помощью выкалывателя скорость следования бит в системе восстанавливается, так как представленные на структурной схеме шифратор и сверточный кодер вносят избыточные биты кода в передаваемое сообщение и снижают скорость следования бит в системе. В перемежителе происходит перестановка бит для повышения помехоустойчивости системы передачи данных. Далее закодированные биты данных модулируются QPSK-модуляцией. Далее, закодированный и промодулированный поток бит данных преобразуется из последовательного в параллельный поток при помощи последовательно/параллельного преобразования, не представленного на рисунке 1, но являющегося неотъемлемой функцией блока «ОБПФ и добавление пилот сигналов».

На следующем этапе формирования OFDM-символа производится операция обратного преобразования Фурье (ОБПФ) и тем самым формируется OFDM-сигнал. Далее добавляются пилотные частоты, и параллельный поток данных преобразуется в последовательный при помощи параллельно/последовательного преобразования. Затем к OFDM-символу добавляется префикс, сформированный из N последних отчетов OFDM-символа, позволяющий противостоять влиянию многолучевого канала. Затем сигнал преобразуется в аналоговый посредством ЦАП (цифро-аналогового преобразования). Блок ВЧ переносит передачу данных в высокочастотную область рабочих частот.

Сигнал с антенны передатчика поступает в канал связи, где за счет многолучевого распространения радиоволн претерпевает некоторые изменения. Измененный каналом сигнал, перемешанный с шумом, поступает на вход приемника.

Находящийся на входе приемника блок ВЧ исследуемой системы состоит из антенного предусилителя, входного фильтра и преобразователя частоты. Входной фильтр выделяет из всего спектра частот рабочую полосу системы и сглаживает выбросы, которые возникают в сигнале, снижает уровень паразитных гармоник и уменьшает уровень шума. Отфильтрованный сигнал с помощью преобразователя частоты переносится в область частот обработки сигнала процессором. Далее отфильтрованный сигнал усиливается в малошумящем усилителе (МШУ), так как сигнал, попадая из канала на приемную антенну имеет слишком малую мощность,. Для лучшей различимости сигнала на фоне шумов и получения информации, которую переносит сигнал необходимо увеличить уровень его мощности.

Сигнал OFDM на выходе передатчика, представляет собой сумму ортогональных сигналов (квадратур) каждый из которых несет в себе полезную информацию. Для разделения сигнала на квадратуры на следующем этапе обработки сигнала в приемнике применяется квадратурный детектор. После детектирования принятый сигнал разделяется на квадратурные компоненты. Каждая из них проходит через фильтр нижних частот (ФНЧ), систему АРУ (автоматической регулировки усиления) и АЦП (аналого-цифрового преобразование) [2, 8-16].

Далее последовательный поток отсчетов аналогового сигнала преобразуется в параллельный, после чего производиться БПФ (быстрое преобразование Фурье) и расформирование OFDM-символа, включающее удаление циклического префикса и пилот-поднесущих, а также параллельно/последовательное преобразование.

Следующим шаг – деперемежение и подстановка бит по заданному вектору. На следующем этапе преобразований в работу включается декодер и дешифратор, которые из закодированного и зашифрованного сообщения извлекает полезную информацию.

Технология OFDMA

Как известно системы Wi-Fi построены на основе технологии OFDM. Для увеличения количества абонентов применяется технология OFDMA («Orthogonal Frequency Division Multiple Access» множественный доступ с ортогональным частотным разделением каналов). Технология OFDMA позволяет обеспечить радиодоступ нескольким абонентам одновременно в одном частотном канале. Для этого частотный ресурс разделяется между этими абонентами, то есть выделенное для организации канала связи количество поднесущих разделяется между абонентами, и отдельному абоненту выделяется определенное количество поднесущих, которые являются «ресурсными единицами» или «ресурсными блоками» (Resource Units, RU). Эта функция в стандарте 802.11ax, позволяет, кроме распределения радиочастотного ресурса, оценивать трафик и важность запросов радиочастотного ресурса. Пример распределения ресурсных блоков между клиентами представлен на рисунке 2.

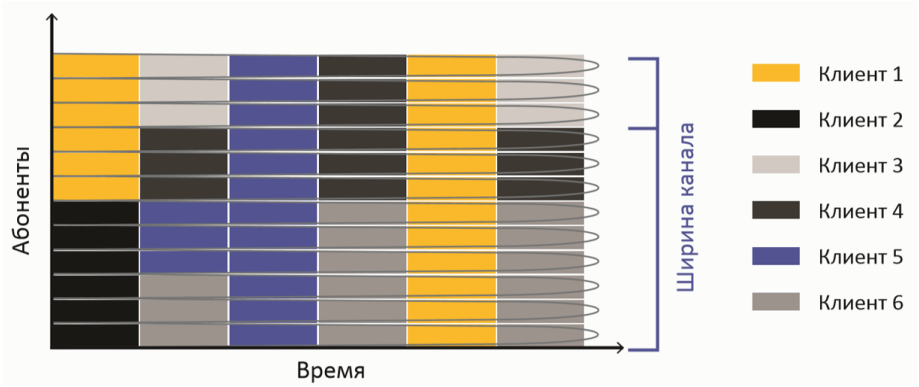


Рис. 2. Пример работы OFDMA [4]

Технология MU-MIMO

Следующей технологией, из применяемых для повышения эффективности системы в системе Wi-Fi 6, является технология MU-MIMO. Технология MU-MIMO (Multi User – Multiple Input Multiple Output, многопользовательская система MIMO) является технологией разнесенного приема/передачи данных, реализуемая на основе многоантенной технике. Данная технология является модернизированной технологией MIMO и позволяет улучшить качество приема/передачи сигнала в сложных помеховых условиях в канале, а также повысить спектральную эффективность системы Wi-Fi 6. В отличие от технологии MIMO, усовершенствованная технология MU-MIMO позволяет одновременно работать с несколькими абонентами, тем самым увеличивая спектральную эффективность системы Wi-Fi 6. В рассматриваемой системе применяется многоантенные системы, позволяющие обеспечивать до 8 разнесенных каналов приема/передачи сигнала (рис. 3).

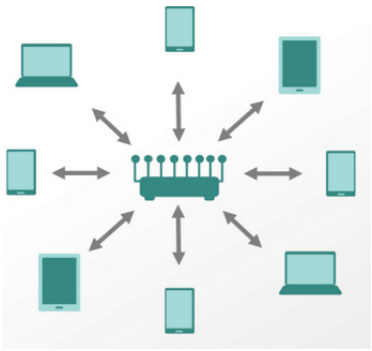


Рис. 3. Пример применения MU-MIMO 8x8

Технология Beamforming

Дополняющая технологию MU-MIMO, технология Beamforming применяется в устройствах стандарта IEEE 802.11 ac и в устройствах стандарта IEEE 802.11 ax. Эта технология дополняет предыдущую технологию, повышает помехоустойчивость и вероятность правильного приема в использующих её устройствах. Технология Beamforming – это технология формирования используемой антенной решеткой (несколькими антеннами) индивидуального луча с узкой диаграммой направленности для каждого абонента. Многоантенное устройство, применяющееся в модеме (точке доступа) Wi-Fi 6, при использовании данной технологии формирует отдельный луч для каждого абонента. Это обеспечивается с помощью полученной от абонента информации о мощности принятого сигнала, его фазе, о характере затуханий в канале и других параметрах сигнала, после осуществления регистрацию абонента в сети. На основе полученных данных, модем, выступающий в качестве точки доступа, адаптирует параметры излучаемого сигнала на основе вычисленных разностей мощности переданного сигнала и принятого, фазы, задержки, угла прихода ответного сигнала и др. В качестве адаптируемых параметров выступают углы места и азимута приходящего ответного сигнала, мощность, задержка ответного сигнала и др. Подстраивая диаграмму направленности, технология Beamforming позволяет адаптировать диаграмму антенны, мощность сигнала и фазу сигнала и, как следствие, скорость передачи данных для тех или иных абонентов, расположенных в разных точках пространства. Это делает передаваемый сигнал адресным в пространстве, повышает помехоустойчивость радиолинии для каждого абонента и увеличивает вероятность правильного приема сигнала, а следовательно, увеличивает скорость передачи сообщения адресованного конкретному абоненту в сложных помеховых условиях канала с многолучевым распространением радиоволн. Таким образом, данная технология повышает эффективность системы передачи данных Wi-Fi 6 для каждого абонента.

Технология BSS Coloring

В настоящее время Wi-Fi сети получили максимальное распространение. В связи с переходом операторов связи от макросот к микро и пикосотам стала достаточно распространенной ситуация наличия на предприятии или в торговом центре нескольких одновременно работающих сетей Wi-Fi разных провайдеров. Каждая такая Wi-Fi сеть создает соседним сетям помехи (рис. 4).

В системе Wi-Fi 6 применяется технология BSS Coloring (Base Station System Coloring), позволяющая разделить сигналы различных сетей и снизить их влияние друг на друга. Технология BSS Coloring – это метод разделения потоков данных нескольких точек доступа, которые основаны на «раскрашивании» потоков данных от той или иной точки доступа. В соответствии с этим методом каждая точка доступа системы Wi-Fi 6 вносит в поток данных специализированные метки, по которым устройства, зарегистрированные в сети, определяют к какой точке доступа относятся данные. По меткам BSS Coloring абонентские устройства принимают решение принимать или не принимать сообщения от конкретной точки доступа. Данное «раскрашивание» потоков данных осуществляется как на линии вверх, так и на линии вниз. Абонентские устройства получают оригинальную «цифровую подпись» от точки доступа при регистрации в сети. Таким образом, снижается влияние соседних сетей радиодоступа на сигнал рабочей сети Wi-Fi 6.

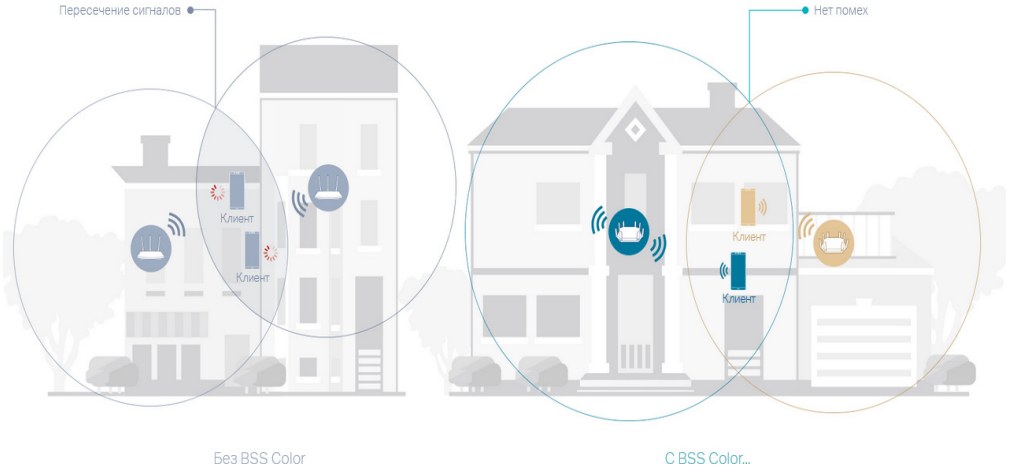


Рис. 4. Модемы без применения BSS Color и с его использованием [3]

Изменения в структуре передачи информации в многопользовательском режиме

Изменения в структуре сигнала системы Wi-Fi 6 коснулись в основном его параметров. Особенно заметны эти изменения сигнала для физического уровня сигнала при взаимодействии описанных выше технологий, применяемых в системах стандарта IEEE 802.11 ax. Основными адаптивно изменяющимися параметрами являются количество поднесущих различного назначения, зависящие от ширины канала. Регулирование этих параметров происходит за счет включения или отключения «ресурсных блоков» (resource unit, RU), описанных выше.

В Wi-Fi 6 временно-частотные ресурсные блоки предусмотрены для работы на необходимом количестве поднесущих. Точка доступа назначает ресурсные блоки фиксированным частотам в канале (например, 20, 40, 80, 80+80 или 160 МГц). Каждый ресурсный блок может использовать свою схему модуляции, скорость кодирования и уровень мощности [1].

Нововведения в сигнале OFDM нового стандарта IEEE 802.11 ax

Первое нововведение в сигнал предыдущего стандарта IEEE 802.11ac – это применения модуляции 1024 QAM вместо 256 QAM в предыдущем стандарте [5]. Для этого не потребуется больше ресурсов спектра или большее количество антенн, и возможна реализация на уже существующих решениях предыдущего стандарта IEEE 802.11ac.

Вторым нововведением является переход от фиксированных параметров сигнала к адаптивным. В предыдущем стандарте IEEE 802.11 ac значение длительности передаваемого символа была равна 3,2 мкс, а значения длительности циклического префикса равнялось 0,4мкс и постфикса – 0,8 мкс. В стандарте IEEE 802.11 ax рассматриваемые параметры имеют несколько значений, например: длительность префикса и постфикса имеют значения 0,8 мкс; 1,6 мкс; 3,2 мкс; длительность символа увеличилась до 12,8 мкс.

Кроме того, в стандарте IEEE 802.11 ax один символ OFDM стал плотнее за счёт 980 информационных поднесущих со временем работы 13,6 мкс в канале 80 МГц, в сравнении с 234 поднесущими и временем работы 3,6 мкс в таком же канале стандарта 802.11ac.

Третьим нововведением является расширенный диапазон частот. В стандарте IEEE 802.11ax используется два диапазона частот: диапазон 2,4 ГГц характерный для ранних стандартов Wi-Fi, а также диапазон частот

5 ГГц, используемый предыдущим стандартом IEEE 802.11 ac. Данное совмещение диапазонов позволило увеличить скорость передачи данных в диапазоне частот 2,4 ГГц и поддерживать высокую скорость передачи данных в диапазоне частот 5 ГГц [5].

Параметры, определенные в рамках выполненных исследований

В связи с тем, что стандарт IEEE 802.11 ax достаточно новый и не все основные параметры системы Wi-Fi 6 известны, в ходе исследований были определены параметры сигнала системы радиодоступа Wi-Fi 6 для используемой ширины полосы частот 20 МГц в диапазоне частот 5,15 – 5,35 ГГц. В таблице 2 представлены основные параметры сигнала системы Wi-Fi 6.

Таблица 2

Параметры системы системы Wi-Fi 6

Название параметра	Значение
Диапазон частот, ГГц	5,150-5,350
Центральная частота сигнала f_0, ГГц	5,250
Число пилот-поднесущих $N_{\text{пилот}}$	4
Длина защитного интервала $T_{\text{защ}}$, мкс	0,32
Длительность OFDM-символа, мкс	1,28
Расстояние между поднесущими, кГц	0,78
Количество используемых поднесущих, $N_{\text{исп подн}}$	26
Количество кодовых бит, $N_{\text{код бит}}$	21
Число поднесущих, $N_{\text{подн}}$	32
Число нулевых поднесущих, N_0	6
Интервал дискретизации по времени комплексной огибающей OFDM-символа, Δt, мкс	0,05
Число отсчетов огибающей OFDM-символа на защитном интервале	6
Общее число отсчетов огибающей OFDM-символа	32
Число кодовых бит на одной поднесущей	10
Число кодовых бит в одном OFDM-символе	210
Число информационных бит в одном OFDM-символе	158
Расчетное значение дальности связи, м	65
Расчетное значение скорости передачи сообщений, Мбит/с	40

Реализация модема системы радиодоступа Wi-Fi 6 на современной элементной базе.

В рамках данной работы была проведен анализ возможности реализации модемов Wi-Fi 6 на современной элементной базе. В результате анализа было выявлено, что исследуемую систему можно реализовать на уже производящихся современных цифровых сигнальных процессорах, (рис. 5 и 6).

Процессор Broadcom BCM43684 [7]

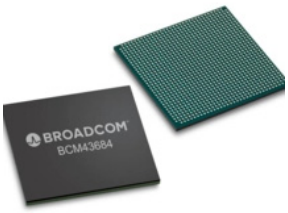


Рис. 5. Внешний вид процессора Broadcom BCM43684

- Поддерживает до 4 потоков данных 802.11ax
- Максимальная ширина канала 160 МГц
- Модуляция 1024 QAM
- Uplink и Downlink OFDMA
- MU-MIMO
- Полное соответствие спецификациям IEEE и WFA 802.11ax

Процессор Qualcomm QCA6390 [6]

Рис. 6. Внешний вид процессора Qualcomm QCA6390

- Поддерживает до 8 потоков данных 802.11ax
- Максимальная ширина канала 160 МГц
- Модуляция 1024 QAM
- Uplink и Downlink OFDMA
- MU-MIMO
- Target Wake-up Time (TWT)
- Полное соответствие спецификациям IEEE и WFA 802.11ax

Рассмотренные цифровые сигнальные процессоры имеют практически одинаковые характеристики. Они позволяют с высокой скоростью обрабатывать и формировать сигналы систем стандарта IEEE802.11ax. Эти процессоры позволяют реализовать несколько операций с передаваемыми сообщениями.

Таким образом, на данных процессорах возможна реализация «системы на кристалле» практически без применения дополнительных процессоров. Однако, для обеспечения высокой скорости передачи (до 11 Гбит/с) и большого числа потоков данных в подсистеме MIMO (до 8), больше подходит цифровой сигнальный процессор Qualcomm QCA6390.

Выводы

1. На данный момент стандарт WLAN IEEE 802.11ax является самым совершенным и использующим новые технологий, позволившие увеличить скорость передачи информации, оптимизировать использование доступного частотного спектра и увеличить число одновременно обслуживаемых клиентов.

2. Разработанные. в ходе исследований структурная схема модема и компьютерная имитационная модель современной системы радиодоступа стандарта IEEE 802.11ax позволили определить основные параметры сигнала: расчётную скорость 40 Мбит/с, которая является минимальной для передачи данных в одном пространственном потоке одного ресурсного блока, и расчётную дальность действия системы в условиях плотной городской застройки 65 м.

3. Для технической реализации модема рассматриваемой системы радиодоступа Wi-Fi 6 предпочтительнее сделать выбор в пользу процессора фирмы Qualcomm, так как на основе возможна реализация устройства с 8 потоками данных единовременно. Это позволит получить высокую пропускную способность системы и снизить затраты потребляемой электроэнергии.

Литература

1. *Новосёлов В., Особенности* Wi-Fi 6 / *В. Новосёлов* // Беспроводные технологии. 2019. №3 (56). С. 6-9. [Электронный ресурс]: https://wireless-e.ru/standarty/wi-fi-6/ (дата обращения 5. 03.2021).
2. *Казаков Л.Н., Кукушкин Д.С.* Синхронизация в системах радиосвязи с ортогональным частотным разделением. – Ярославль, 2012. 161 с. [Электронный ресурс]: http://www.lib.uniyar.ac.ru/edocs/iuni/20120705.pdf.
3. Шестое поколение Wi-Fi [Электронный ресурс]: сайт компании “TP-Link CO., LTD” https://www.tp-link.com/ru/wifi6/ (дата обращения 8. 03.2021).
4. Что такое 802.11ax – обзор нового стандарта Wi-Fi 6 [Электронный ресурс]: сайт компании “Ситком” https://www.sit-com.ru/802-11ax-review-wifi6.html#history (дата обращения 10. 03.2021).
5. IEEE 802.11ax: The Sixth Generation of Wi-Fi White Paper [Электронный ресурс]: сайт компании “Cisco Systems, Inc.” https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.html (дата обращения 15. 02.2021).
6. Техническое описание процессора Qualcomm FastConnect 6800 [Электронный ресурс]: сайт компании “Qualcomm.” https://www.qualcomm.com/products/fastconnect-6800 (дата обращения 21. 03.2021).
7. Техническое описание процессора BCM43684 [Электронный ресурс]: сайт компании “Broadcom Inc.” https://www.broadcom.com/products/wireless/wireless-lan-infrastructure/bcm43684 (дата обращения 21. 03.2021).
8. *Бакулин М.Г., Крейнделин В.Б.* Проблема повышения спектральной эффективности и емкости в перспективных системах связи 6G // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 25-31.
9. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Анализ пропускной способности канала MIMO в условиях замираний // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 2. С. 13-20.
10. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Методы приема псевдослучайных последовательностей в системах радиосвязи // REDS: Телекоммуникационные устройства и системы. 2018. Т. 8. № 1. С. 108-112.
11. Крейнделин В.Б., Старовойтов М.Ю. Повышение помехоустойчивости системы связи MIMO с пространственным мультиплексированием методом додетекторного сложения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 4-13.
12. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Исследование вероятностных моделей радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон с помощью компьютерного моделирования // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 1. С. 64-68.
13. *Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К.* Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 24-30.
14. *Крейнделин В.Б., Панкратов Д.Ю.* Вероятностная модель радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 1. С. 103-107.
15. *Фролов А.А.* Оценка эффективности совместного использования радиочастотного спектра многочастотными сверхширокополосными системами радиодоступа и WIFI // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 10. С. 21-26.
16. *Фролов А.А.* Исследование многочастотной сверхширокополосной системы радиодоступа с совмещением технологий OFDM и кодового разделения абонентов // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 1. С. 77-83.

ANALYSIS OF THE IEEE 802.11AX WI-FI RADIO ACCESS SYSTEM

Alexey A. Frolov,
Senior Lecturer of the Department of RTS, Ph.D., MTUCI, Moscow, Russia,
a.a.frolov@mtuci.ru

Ilya V. Litvinov,
Student MTUCI, Moscow, Russia,
lighthummer99@gmail.com

Abstract

This paper discusses the reasons for the emergence of a new standard and its features. The new technologies used in the Wi-Fi radio access system are briefly described. The analysis of changes in the signal of the radio access system of the IEEE802.11ax standard in comparison with the previous IEEE 802.11ac standard is carried out. The block diagram and principle of operation of the IEEE 802.11ax standard modem are described. The numerical values of the parameters of the modem of the radio access system of the IEEE802.11ax standard are determined for its subsequent implementation on a modern element base.

Keywords: *Wi-Fi system, OFDM signal, unlicensed spectrum, increased spectrum efficiency, IEEE 802.11ax standard, IEEE 802.11ac standard.*

СРАВНИТЕЛЬНЫЙ ОЦЕНОЧНЫЙ АНАЛИЗ КЛЮЧЕВЫХ ХАРАКТЕРИСТИК ТЕХНОЛОГИЙ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ СВЯЗИ

Лебедев Дмитрий Александрович,
студент МТУСИ, Москва, Россия,
blooddiman@mail.ru

Сорокин Александр Степанович,
доцент кафедры СиСРТ, к.т.н., доцент МТУСИ,
a.s.sorokin@mtuci.ru

Аннотация

Подчёркивается актуальность развития технологии самоорганизующихся сетей связи (СОСС) и приводится уточненные понятия классификации и назначения СОСС. Кратко рассмотрены и проанализированы характерные достоинства и недостатки основных видов СОСС. Приводится и рассматривается перечень ключевых характеристик и параметров СОСС, с учетом которых авторами на основе метода эвристического логико-числового анализа (ЭЛЧА) с помощью определения численных рейтинговых оценок выполнен сравнительный анализ ключевых характеристик (КХ) и ключевых параметров (КП) основных стандартов технологий СОСС. По результатам сравнительного анализа КХ сформулированы адекватные используемому методу анализа (ЭЛЧА) научно-обоснованные выводы.

Ключевые слова: *самоорганизующиеся сети связи, ключевые характеристики, ключевые параметры, топология сетей связи, AdHoc-сеть, Mesh-сеть, технология мобильной связи, рейтинг технологии мобильной связи, эвристический логико-числовой анализ, эффективность сети мобильной связи, эффективность функционирования самоорганизующейся сети связи, 3GPP.*

Актуальность работы обусловлена возрастающей в настоящее время роли технологий СОСС и перспективностью её дальнейшего развития [1]. На СОСС возлагаются большие надежды в плане качественного обслуживания огромного объема абонентского трафика вследствие более высокой эффективности функционирования СОСС по сравнению с сетями связи, построенными на основе традиционных технологий. Вместе с тем в настоящее, вопросы теоретического анализа работы СОСС в научно-технической литературе освещены недостаточно полно, в особенности в части обобщенности анализа КХ, важность которого становится все более значимой из-за постоянного усложнения алгоритмов функционирования СОСС. Это приводит к тому, что СОСС приобретают новое качество - становятся фактически мобильными и динамически масштабируемыми. Для поддержки, контроля и регулировки этих качеств/свойств необходимо иметь математический аппарат анализа эффективности функционирования СОСС и, в качестве его основы – количественный критерий оптимальности используемой технологии построения СОСС.

Цель работы (на текущем этапе) состоит в составлении адекватной методологии прогностического анализа эффективности функционирования СОСС в условиях отсутствия (на настоящий момент) её полного математического описания (МО), и выполнение на основе такой методологии сравнительного оценочного анализа существующих стандартизованных технологий СОСС. Актуальность указанной методологии обусловлена ее применением на обязательном этапе эвристического анализа и отбора исходных параметров СОСС в процессе выполнения процедур оптимизации.

О современном определении СОСС
(“как вы яхту назовете, так она и оплывет”)

Необходимо отметить два известных понятия и определения СОСС:

- определение 1: СОСС – это децентрализованная беспроводная сеть, не имеющая постоянной/фиксированной структуры;

- определение 2: СОСС – это радиосеть связи, которой не нужна никакая дополнительная инфраструктура, кроме самих основных сетевых элементов (СЭ) в виде абонентских станций (АС) [3].

Оба эти определения являются абсолютно эквивалентными при условии правильного понимания информации умолчания, содержащейся в терминах “децентрализованная беспроводная” и “никакая дополнительная инфраструктура”. Можно отметить, что определение 2 является более конкретным и понятным, но все же представляется, что оно слишком категорично на настоящий момент.

В стандартах технологий мобильной связи (ТМС) *4G* и *5G* понятие СОСС получило расширенное толкование, несколько отличное от рассмотренных выше. Главным отличием является то, что на настоящий момент, по крайней мере, оно не предполагает обязательное наличие децентрализованной структуры и, соответственно, дополнительной инфраструктуры. Это обстоятельство можно расценивать как некий “откат” в развитии технологий СОСС, но, если рассматривать с точки зрения ТМС *4G/5G*, то это все же шаг вперед, но достаточно осторожный и оправданный с учетом высокого уровня ответственности обеспечиваемого ими информационного обмена по сравнению с другими стандартами ТМС, такими как *WiFi* или *ZigBee.*

На рисунке 1 показана типовая топология сотовой сети мобильной связи (СМС) с фиксированной структурой.

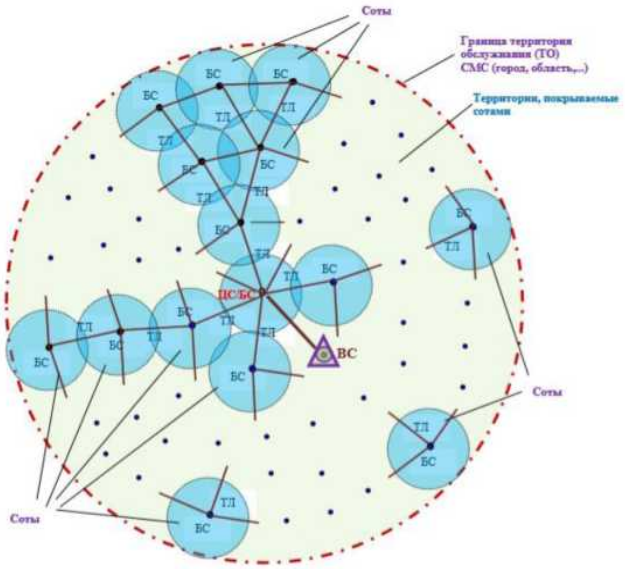


Рис. 1. Типовая топология сотовой СМС с фиксированной структурой

Как известно, структура сотовой СМС состоит из ряда фиксированных СЭ и подвижных (нефиксированных) СЭ. К числу фиксированных СЭ относятся: базовые станции (БС), центральная станция (ЦС), центр управления (ЦУ), центр эксплуатации и обслуживания (ЦЭО), соединительные линии (СЛ) на основе волоконно-оптических линий связи (ВОЛС) или радиорелейных линий (РРЛ).

Подвижными СЭ в сотовой СМС являются только АС. На рисунке 1 показаны только БС, ЦС и СЛ в предположении, что ЦУ и ЦЭО обычно территориально объединены с ЦС и что АС могут занимать произвольное положение в пределах территории обслуживания (ТО) СМС.

Можно отметить, что ЦС, ЦУ, ЦЭО, БС и СЛ образуют дополнительную инфраструктуру и с точки зрения идеальной технологии СОСС являются излишними, если все функции, выполняемые этими СЭ возложить на АС. Теоретически это возможно, но при практической реализации, пока, имеются существенные ограничения.

На рисунке 2 в качестве примера приведены три варианта самоорганизации топологии СОСС, состоящей из 10 АС.

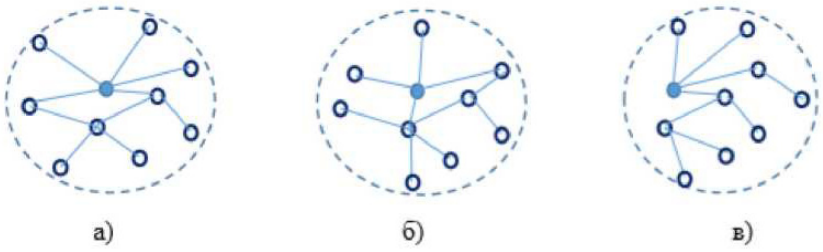


Рис. 2. Пример трех вариантов самоорганизации топологии СОСС

Отметим, что рисунки 2а, б и в отображают вид “мгновенной” топологии в различные моменты времени работы СОСС. Здесь закрашенным кружком показан условно фиксированные СЭ для обозначения значения примерного расположения геометрического центра ТО (пунктирная окружность), а не закрашенными кружками - подвижные СЭ. На рисунке 2в изображено состояние СОСС, при котором произошло смещение ТО относительно ее положения, показанного на рисунке 2а.

В реальной ситуации топология СОСС будет изменяться по мере необходимости таким образом, чтобы поддерживалась оптимальность своей работы. При этом число вариантов самоорганизации может быть доста-

точно велико (это и хорошо и плохо) и их будет тем больше, чем больше число АС, входящих в структуру СОСС. Это обстоятельство является весьма проблематичным и требует тщательного и надежного учета (будет рассмотрено далее).

Сказанное выше о современном понятии сущности СОСС позволяет сформулировать уточненное и, что немало важно, обобщенное, определение СОСС следующим образом: **СОСС – это сеть связи с возможностью автоматической оптимизации показателей функционирования (ПФ) в заданном диапазоне изменения условий работы сети.**

О достоинствах и недостатках СОСС

Использование СОСС имеет преимущества в сравнении с беспроводными сетями традиционной архитектуры с фиксированной топологией за счет возможности расширенной адаптации характеристик и параметров инфраструктуры в соответствии с определенными алгоритмами их управления таким образом, чтобы поддерживались оптимальными ПФ СОСС в целом. Очевидно, что внедрение расширенных процедур адаптации связано с усложнением алгоритмов функционирования и некоторым удорожанием оборудования СОСС.

Следует особо отметить проблематику пониженной информационной безопасности (ИБ) СОСС, которая обусловлена рядом дополнительных информационных уязвимостей. Однако, проблема обеспечения ИБ является общей для систем радиосвязи, но представляется, что в недалекой перспективе она должна исчезнуть или, по крайней мере, не будет столь актуальной, как в настоящее время.

В таблице 1 приведены основные преимущества и недостатки СОСС по сравнению с сетями, основанными на традиционных технологиях с фиксированной структурой.

Таблица 1

Основные преимущества и недостатки СОСС

Преимущества	**Недостатки**
Снижение затрат на построение и эксплуатацию системы	Повышенное энергопотребление координирующих станций
Повышение спектральной эффективности	Существенное усложнение алгоритма функционирования
Улучшение радиопокрытия территории обслуживания	Увеличенные риски информационной безопасности
Повышение пропускной способности системы	Более высокие требования к техническим характеристикам абонентских станций
Отсутствие необходимости в предустановленной инфраструктуре	
Устойчивость к негативным изменениям в структуре сети	
Простота и малое время развертывания	

В качестве комментария к таблице 1 следует заметить, что перечень приведенных преимуществ СОСС не является абсолютным в смысле их обязательного наличия. Это, как бы, потенциальные преимущества, которые надо уметь реализовать практически. Вместе с тем указанные в таблице 1 недостатки СОСС являются в большей степени академическими (теоретическими) и при решении поставленных в данной работе задач ими можно пренебречь.

Основные виды существующих технологий СОСС

Основная идея разработки СОСС, определяющая ее назначение - улучшение/повышение технических и технико-экономических ПФ системы связи и ее эффективности в целом за счет встраивания в ее структуру высокоинтеллектуальных средств управления и контроля на основе компьютерных технологий.

В настоящее время СОСС реализуются на основе трех самостоятельных технологий: *AdHoc-технологии, Mesh-технологии* и гибридной технологии *(ГТех)* [5,7].

AdHoc-сеть – децентрализованная беспроводная сеть, не имеющая постоянной структуры (рис. 3).

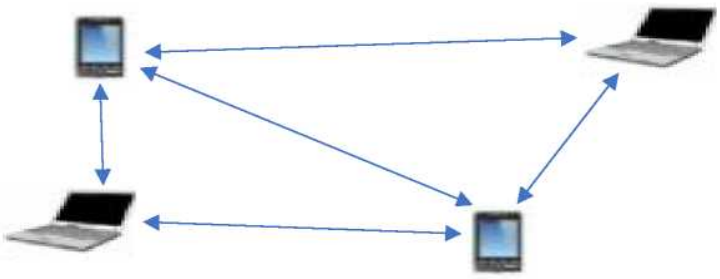


Рис. 3. Топология комбинированной *AdHoc-сети*

В такой сети информационный обмен (ИО) происходит между двумя станциями, то есть попарно, как показано стрелками на рисунке 3. При этом возможность связи и качество ИО между отдельными станциями зависит от условий распространения радиоволн между ними. В целом следует отметить, что алгоритм работы *AdHoc-сетей* является простейшим, что и является их главным преимуществом.

Mesh-сеть (ячеистая топология) - сетевая топология, построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны выполнять роль коммутатора для остальных участников. Пример топологии такой структуры представлен на рисунке 4.

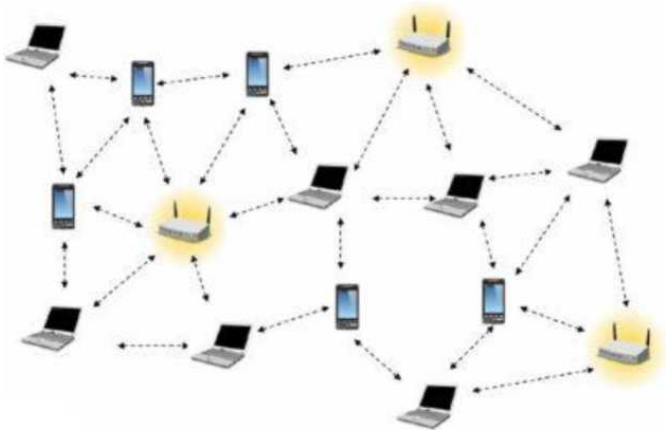


Рис. 4. Фрагмент Mesh-сети

В Mesh-сети ИО осуществляется, как правило, между смежными СЭ непосредственно, а между удаленными СЭ за счет ретрансляции сигналов через промежуточные СЭ. В результате такого построения каналов связи Mesh-сети обладают потенциально более высокой масштабируемостью по сравнению с сетями *Ad-Hoc,* но при этом имеют более сложный алгоритм управления.

Сеть ГТех представляет собой совокупность традиционных технологий построения сети с фиксированной структурой и элементов технологий *AdHoc-сетей* и *Mesh-сетей*, что расширяет возможности структуры связи за счёт возрастания достоинств и уменьшению влияния недостатков свойственных отдельным сетям. При этом вид топологии *ГТех-сети* практически не будет отличаться от показанной на рисунке 1.

Основные алгоритмы функционирования СОСС

Базовый алгоритм управления

Базовый алгоритм управления (БАУ) основан на технологии пакетной передачи в сочетании с временным уплотнением (ТППВУ) целевых сигналов управления и контроля всех СЭ данной СОСС, реализуемой в виде покадровой временной структуры группового цифрового сигнала (ГЦС), то есть бесконечной последовательности однотипных кадров, обеспечивающих выполнение всех необходимых функций управления [6]. На рисунке 5 в качестве примера показана типовая покадровая структура ГЦС СОСС Mesh-сети стандарта *WiMAX.*

Рис. 5. Пример структуры кадра СОСС

Каждый кадр ГЦС состоит из двух субкадров: субкадра управления сетью и субкадра данных. Субкадры управления сетью включают интервалы для подключения к сети новых устройств. “Сетевой вход” и следующие за ними интервалы “Конфигурация сети”, содержат всю необходимую информацию о составе сети: списки соседей каждого узла, удаленность соседей для каждого узла, номера каналов связи с соседями и пр. Кроме того, в интервалах “Конфигурация сети” с заданной периодичностью вещается дескриптор сети в виде таблицы с полным описанием параметров сети. Управляющий субкадр в зависимости от реализуемой функции может быть двух типов: управления сетью и управления очередностью доступа к каналам связи, структура которого показана в нижней части рисунка 5. В субкадрах управления всегда используется наиболее помехоустойчивая модуляция вида 2-ФМ или 4-ФМ с максимальной скоростью помехоустойчивого кодирования [6].

Следует отметить, что БАУ во всех используемых в настоящее время технологий СОСС примерно идентичны и оперируют аналогичными данными, описывающими доступные сетевые ресурсы в виде соответствующих таблиц, которые формируются на каждом узле сети и периодически обновляются [1, 3]. На основании совокупности этих данных и происходит управление сетью.

Специфические алгоритмы СОСС

Данные алгоритмы реализуют специальные функции самоорганизации структуры связи, суть которых состоит в автоматическом контроле и управлении всеми параметрами сети с целью поддержания оптимальности ее работы при минимальном вмешательстве в этот процесс человека-оператора. Это позволяет улучшать качество обслуживания абонентов, повышать надежность работы структуру и существенно снижать издержки на ее эксплуатацию. Общей особенностью данных алгоритмов является то, что они не имеют единой стандартизации, хотя в целом, в используемых в настоящее время технологиях СОСС они не имеют существенного различия.

Данные алгоритмы условно подразделяются на три группы [1, 2].

Специфические алгоритмы СОСС **первой группы о**беспечивают автоматическую конфигурацию *(dynamic plug-and-play configuration)* вновь развернутых СЭ. При этом СЭ самостоятельно настраивает свой физический идентификатор, частоту передачи и мощность, что обеспечивает более быстрое планирование и развертывание структуры СОСС.

Вторая группа специфических алгоритмов СОСС включает в себя алгоритмы оптимизации покрытия, пропускной способности, хэндовера и внутрисистемных помех. В набор этих алгоритмов входят: алгоритм балансировки нагрузки мобильности; алгоритм оптимизации мобильности; алгоритм координации внутрисистемных помех; алгоритм оптимизации канала доступа; алгоритм оптимизации радиопокрытия и пропускной способности; алгоритм оптимизации энергопотребления [10] .

Специфические алгоритмы СОСС **третьей группы** обеспечивают автоматическое восстановление работоспособности структуры в случаях: сбоев программного обеспечения (ПО) сетевых элементов (СЭ); физических отказов аппаратуры СЭ; отключения СЭ с целью энергосбережения.

Алгоритмы маршрутизации

Все типовые алгоритмы маршрутизации (Марш) делятся на три группы: проактивные, реактивные и гибридные. Проактивные алгоритмы Марш предполагают постоянное обновление полных списков адресов назначения и маршрутов до них. Реактивные алгоритмы Марш выполняют построение маршрута по необходимости, т.е. при наличии трафика, предназначенного определенному адресату, с помощью опросов соседних узлов и алгоритмов обнаружения соседей. Гибридная Марш реализуется сочетанием элементов проактивной и реактивной Марш путем хранения таблицы некоторых адресатов, и последующего их опроса по требованию по мере необходимости построения иных маршрутов [7] .

Наиболее распространенными типовыми алгоритмами (протоколами) Марш являются: *AODV* и *HWMP* [4,6]. Протокол *AODV (AdHoc On-demand Distance Vector)* является реактивным протоколом, устанавливающим маршрут по требованию на основе дистанционно-векторного алгоритма Марш. Протокол *HWMP (Hybrid Wireless Mesh Protocol)* - гибридный протокол радиосетей с ячеистой структурой. Он основан на протоколе *AODV* и древовидном алгоритме Марш, и может работать как в проактивном, так и в реактивном режимах Марш.

Вопрос применения того или иного протокола Марш в СОСС является открытым, то есть решается по усмотрению разработчика. Довольно часто используются так называемые фирменные протоколы (ФП), например, в стандарте *Bluetooth,* стандартах *LTE* и *5G.*

Ключевые характеристики СОСС

Все характеристики СОСС можно подразделить на обобщенные характеристики (ОХ) и ключевые характеристики (КХ). КХ являются теми из общего числа характеристик СОСС, которые наиболее существенно влияют на ОХ. Можно отметить, что основной ОХ всех динамических систем, к которым относятся современные СОСС, является эффективность функционирования (ЭФ).

Все КХ СОСС целесообразно для достижения целей данной работы подразделить на две группы: полуобобщенные КХ (ПКХ) и частные КХ (ЧКХ).

СОСС обладает следующими ПКХ [1, 2]:

1. Самоконфигурация (СКон) - свойство/функция автоматического определения и регистрации в сети вновь подключаемых СЭ. При этом другие СЭ сети автоматически корректируют свои параметры (например, мощность излучения, наклон антенны и т.д.) в соответствии с алгоритмом СКон;

2. Самооптимизация (СОпт) – свойство/функция адаптации параметров СЭ при изменении параметров сети таких как: количество пользователей, уровень принимаемого сигнала, уровень внешних помех и др.;

3. Самовосстановление (СВос) – свойство/функция автоматического обнаружения и устранения сбоев или выхода из строя (физического отказа) аппаратуры СЭ путем включения резервного оборудования и/или перераспределения функций между ними для устранения отказа (аварии).

К ЧКХ относятся наиболее влияющие технические характеристики системы такие как: диапазон рабочих частот (ДРЧ), максимальная мощность передатчика, скорость передачи сигналов, дальность связи и пр.

Как и любая характеристика КХ специфицируются индивидуальными параметрами, которые можно также называть ключевыми параметрами (КП). Каждая КХ имеет свой набор КП, причем он относится и к ПКХ и к ЧКХ.

На рисунке 6 показана упрощенная модель взаимосвязи ОХ, ПКХ и ЧКХ.

Как можно видеть из рисунка 6, он отображает весьма сложную картину взаимодействия ОХ, ПКХ и ЧКХ. Суть такой сложности состоит с одной стороны в объемности процессов взаимодействия, а с другой - в отсутствии их адекватного МО. Следует отметить, что в настоящее время вопрос разработки МО СОСС пытаются решить на основе применения технологии нейросетей, но ,вероятно, до положительного исхода еще очень далеко [8].

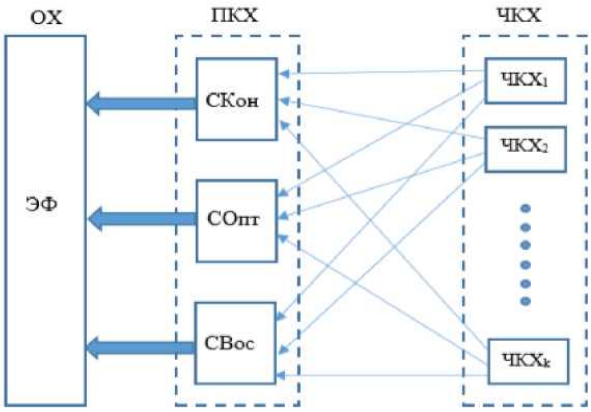


Рис. 6. Модель взаимосвязи ОХ и КХ СОСС

Методология реализации ЭЛЧА

В указанных выше условиях неопределенности, по сути, единственной возможностью решения поставленной в данной работе цели является применение метода ЭЛЧА, проверенного и надежного инструмента человеческого мышления.

ЭЛЧА в данной работе реализован способом эвристического определения относительных рейтинговых оценок/рейтингов ЧКХ (РЧКХ) рассматриваемых технологий СОСС и последующего определения на их основе осредненных относительных рейтингов технологий (ОРТ) СОСС. Очевидно, что рейтинги должны определяться в эквивалентных условиях применения рассматриваемых технологий СОСС. Об этих условиях сравнения будет конкретно сказано ниже.

ОРТ *t-ой* технологии СОСС *(rtit)* при равновесном влиянии ЧКХ рассчитывается по формуле,

$$rtit = [(rtiti + rti\ t2 + rtit3 + ... + rti\pm)/k], \quad (1)$$

где *t* – номер технологии СОСС (t=1, 2, ..., k); *k* – число рассматриваемых ЧКХ; rti_ti – рейтинг t-ой технологии СОС по ЧКХ №1; rtit2 – рейтинг t-ой технологии СОС по ЧКХ №2 и т.д. до rtitk – рейтинг t-ой технологии СОС по ЧКХ №k; [•] – знак округления до меньшего целого.

Отметим, что анализ технологий СОСС при учете неравновесного влияния ЧКХ предполагается выполнить на следующем этапе работы.

По полученным ОРТ делается логико-числовой анализ, суть которого заключается в том, чтобы логически обосновать преимущества и недостатки каждой из рассматриваемых технологий СОСС. На основании этого анализа формулируются значимые выводы (на настоящий момент и на перспективу).

Результаты выполнения ЭЛЧА

Как указывалось выше, РЧКХ в данной работе для каждой рассматриваемой технологии СОСС определяются эвристически на основании логико-числового анализа основных технических характеристик соответствующего стандарта ТМС, в котором применяется данная технология СОСС. На первом этапе такого анализа проводится формирование списка ЧКХ из значительного числа технических характеристик, которые могут

быть у объекта. В качестве ЧКХ выбираются те, влияние которых на ОХ признается (на основании технического опыта и интуиции) достаточно существенным.

В таблице 2 приведены основные технические характеристики и параметры основных стандартов ТМС, в которых используются технологии СОСС.

Примечания к таблице 2:

1. ТТ - топология “Точка-точка”; ТМТ - топология “Точка-много-точек”.
2. * Кратность MIMO - степень числа 2m, при которой значение этого числа равно числу пар приемо-передающих MIMO-антенн.

Пример: если число пар антенн равно 8, то имеем m=3, т.е. трехкратная MIMO.

*** Плюсы учитываются в рейтингах в виде некоторого их повышения; несколько “+” , соответственно, в зависимости от их числа будут в большей или меньшей мере повышать рейтинг соответствующей ЧКХ и, таким образом, влиять на ОРТ.

Определение конкретных РЧКХ и ОРТ проводилось в эквивалентных условиях, предполагающих возможность применения каждой из рассматриваемых технологий СОСС для построения сети на большой ТО со значительным числом абонентов и с достаточно высокими требованиями к параметрам абонентского трафика.

Для определения РЧКХ использовалась шкала рейтинговых оценок, приведенная в таблице 3.

В таблице 4 приведены рейтинговые оценки определенных путем логико-числового анализа ЧКХ и рассчитанные на их основе ОРТ шести технологий СОСС.

Таблица 2

Основные характеристики и параметры ТМС, использующие технологии СОСС

Стандарт ТМС Характеристика	802.15.4 *ZigBee*	802.15.1 *Bluetooth*	802.11 *WiFi*		802.16 *WiMAX*	*LTE*	5G
Виды передаваемого трафика	Мониторинг управление, сети датчиков	Голос, данные	Данные, голос, видео, IP		Соединение, данные, голос, видео, IP	Данные, голос, видео, IP	Управление, данные, голос, видео, IP
Стоимость	низкая	низкая	низкая		средняя	Высокая	высокая
Качество обслуживания	не гарантир.	не гарант.	не гарант.		Гарантир.	гарантир.	гарантир.
Надежность	высокая	средняя	средняя		Средняя	Высокая	высокая
Типичный размер ТО	средний	малый	малый		не огранич.	не огранич.	не огранич.
Масштабируемость	низкая	низкая	низкая		Средняя	Высокая	высокая
ДРЧ, ГГц	0,8	0,9	2,4	5,2	3,5	0,8.2,6	0,8.5,2
Агрегация спектра	Нет	нет	нет	нет	Нет	+	++
Максимальная скорость передачи, Мбит/с	0,02	0,04	300	1000	300	До $1*10^3$	До $20*10^3$
Выходная мощность АС, мВт	1	1; 2,5; 100	100		200	200	200
Максимальный радиус соты, м	100	100	100		$5 \cdot 10^4$	10^5	500
Время работы батареи АС на 1 заряде, дней	○ ○ ○	1..7	0,5…5		3	3	2
Поддержка IP-технологий ***)	+	нет	+		+	+	+
Виды топологий	ТТ ТМТ *Mesh*	ТТ ТМТ, *Scattetner*	ТТ; ТМТ *AdHoc* *Mesh*		ТТ ТМТ *Mesh*	Много-сотовая	Много-сотовая
Алгоритм маршрутизации	*AODV*	ФП	*HWMP*		*HWMP*	ФП	ФП
Кратность *MIMO* *	Нет	нет	2.4		<3	<4	>4
BeamForming **)	Нет	нет	+		+	+	++
Задержка доставки сообщений, мс	30	15	25		30	20	1
Мобильность, км/ч	10	10	10		120	100	500
Число видов трафика	1	2	3		5	15	20

Таблица 3

Шкала рейтинговых оценок, используемых для ЭЛЧА

Значение рейтинга	Содержание рейтинга
0	отсутствует
1	низкий
2	ниже среднего
3	средний
4	выше среднего
5	хороший
6	высокий

Таблица 4

Рейтинговые оценки (рейтинги) КХ и осредненные рейтинги основных технологий СОСС

Технология СОСС		*AdHoc*		*Mesh*			ГТех
Стандарт ТМС		*WiFi*	*Bluetooth*	*WiFi*	*ZigBee*	*WiMAX*	4G/5G
№	ЧКХ			Рейтинги			
1	Алгоритм СКон	4	5	4	5	4	6
2	Алгоритм СОпт	2	4	2	2	3	6
3	Алгоритм СВос	2	2	3	2	3	5
4	Алгоритм Марш	3	4	5	6	5	4
5	*MIMO*	3	0	6	0	5	6
6	*BeamForming*	2	0	2	0	0	4
7	Дальность связи АС	2	1	2	3	5	6
8	Энергосбережение АС	2	3	2	6	5	5
9	Задержка сообщений	3	3	2	3	4	6
10	Мобильность	2	2	2	1	4	6
11	Мультисервисность *	2	3	3	1	3	6
Осредненный рейтинг технологии СОСС		**2,4**	**2,5**	**3**	**2,6**	**3,7**	**5,4**

Примечание:

Мультисервисность определяется числом видов трафика, которые могут передаваться в системе связи.

Как видно из данных в таблице 4 наибольшим из рассматриваемых технологий СОСС рейтингом обладает сеть *ГТех*, используемая в стандартах ТМС *LTE/5G.* Представляется, что преимущества сети *ГТех* обусловлены применением гибридной технологии СОСС, которую на настоящий момент можно считать оптимальной, вследствие, прежде всего использования обобщенного алгоритма используемых технологий. Это в значительной степени повышает эффективность и одновременно значительно упрощает функционирование данной сети в сравнении с сетями на основе технологии *Mesh* и соответственно, обеспечивает более высокую надёжность. Можно предположить, что данное утверждение является взвешенным и соответствует традициях разработчиков международного партнерства 3 *GPP,* начиная с разработки технологии *GSM.*

Выводы

1. Наиболее высоким рейтингом по результатам ЭЛЧА обладает гибридная технология СОСС, используемая в структуре стандартов LTE/5G.
2. Mesh-технология СОСС, применяемая в стандарте WiMAX и ZigBee, позиционируется на основе полученного рейтинга несколько ниже, чем гибридная технология СОСС, используемая в стандартах LTE/5G.
3. Наиболее низкий рейтинг имеет технология СОСС, используемая в AdHoc-сетях WiFi и Bluetooth.
4. На основании положений, указанных выше в пп. 1, 2 и 3, можно сделать вывод о более высокой эффективности гибридной технологии СОСС по сравнению с рассмотренными альтернативными технологиями СОСС AdHoc-сетей и Mesh-сетей.
5. Разработанная методология применения ЭЛЧА и выполненный для ее проверки рейтинговый анализ КХ технологий СОСС показал ее работоспособность, что является подтверждением заявленной в работе цели. Вместе с тем целесообразно дальнейшее совершенствование методологии ЭЛЧА с целью разработки на ее основе адекватного математического описания функционирования СОСС [9].

Литература

1. *Nohrborg M.* Self-Organizing Networks. 3GPP, 2020.
2. *Тихвинский В.О. и др.* Автоматическое управление сетями 4G/5G с использованием технологий и алгоритмов *SON* // Последняя миля, №3, 2019. С. 78-87.
3. Самоорганизующиеся сети SON // www.ru.nec.com.
4. *Хоров Е.М.* Знакомство с современными беспроводными технологиями. Многошаговые беспроводные сети: принципы построения и открытые задачи [Электронный ресурс] www.mipt.ru.
5. *Проскочило А.В. и др.* Анализ и перспективы развития самоорганизующихся сетей // Научные ведомости, №19, 2015. [Электронный ресурс] www.cyberleninka.ru.
6. *Гусс С.В.* Самоорганизующиеся Mesh-сети для частного применения // Математические структуры и моделирование, №4, 2016. С. 102-115.
7. *Орлов В.Г., Фадеев А.Н.* Протоколы маршрутизации в мобильных ad-hoc-сетях // Фундаментальные проблемы радиоэлектронного приборостроения. 2012. Т. 12. № 6. С. 208-212.
8. *Польщиков К.А.* Оценка вероятностно-временных характеристик доставки в беспроводной самоорганизующейся сети [Электронный ресурс] (Дата обращения 03.05.2021).
9. О технологии связи 6G // www.d-russia.ru.
10. *Орлов В.Г., Литвяков В.С.* Схемы и процедуры взаимодействия инфраструктурных узлов сетей мобильной связи разных поколений // Телекоммуникации и информационные технологии. 2020. Т. 7. № 1. С. 42-50.

COMPARATIVE EVALUATION ANALYSIS OF KEY CHARACTERISTICS TECHNOLOGIES OF SELF-ORGANIZING COMMUNICATION NETWORKS

Dmitry A. Lebedev,
Student MTUCI, Moscow, Russia,
blooddiman@mail.ru

Alexander St. Sorokin,
Associate professor of SiSRT department, Ph. D., MTUCI, Moscow, Russia,
a.s.sorokin@mtuci.ru

References

Of self-organizing communication networks (SOSS) is emphasized and a refined definition of the definition and purpose of SOSS is given. The characteristic advantages and disadvantages of the main types of SOS are briefly considered and analyzed. A list of the key characteristics and parameters of the SOSS is given and considered, taking into account which the authors, based on the method of heuristic logical-numerical analysis (ELCA) by determining numerical ratings , performed a comparative analysis of the key characteristics (KX) and key parameters (KP) of the main standards of SOSS technologies. Based on the results of the comparative analysis of the CC, scientifically-based conclusions are formulated that are adequate to the analysis method used (ELCA)

Keywords: *self-organizing communication networks, key characteristics, key parameters, topology of communication networks, network element, network node, AdHoc network, Mesh network, mobile communication technology, mobile communication technology rating, heuristic logical-numerical analysis, mobile communication network efficiency, self-organizing communication network functioning efficiency, 3GPP.*

АНАЛИЗ ВОЗМОЖНОСТЕЙ СИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ «LORA» НА ОСНОВЕ СИГНАЛА OFDM

Фролов Алексей Андреевич,
старший преподаватель кафедры РТС, к.т.н., МТУСИ, Москва, Россия,
a.a.frolov@mtuci.ru

Тамбовцева Алёна Александровна,
студентка МТУСИ, Москва, Россия,
tambovceva1999@mail.ru

Аннотация

В работе представлены основные результаты исследования возможности применения сигнала OFDM в системе интернета вещей «LoRa». В данной работе рассматривается основная концепция интернета вещей. Также описан ее принцип действия и наиболее распространенная область применения. Исследуются архитектура системы «LoRa» и структурные элементы сети. Представлено обоснование возможности применения нестандартного для системы «LoRa» сигнала OFDM. Определены преимущества и недостатки предлагаемого для применения в рассматриваемой системе сигнала OFDM в сравнении со стандартным ЛЧМ сигналом с прямым расширением спектра, применяющимся в системе «LoRa». Приведена структурная схема модема системы «LoRa» на основе сигнала OFDM и основные параметры модема, позволяющие разработать имитационную компьютерную модель данной системы для реализации модема на современной элементной базе.

Ключевые слова: *Интернет вещей, система M2M, сигнал OFDM, система LoRa, сеть LoRaWAN, ISM диапазон частот, передача телеметрии, нелицензируемый спектр.*

Концепция «Интернета вещей» (Internet of Things, IoT) – это интеграция объектов и устройств, которые выполняют функции анализа и преобразования параметров окружающей среды в понятном для цифровой техники формате для обеспечения доступа к публичной сети. Системы Интернета вещей являются системами передачи данных между датчиками и центрами обработки данных, т.е. практически полностью автономными системами межмашинного взаимодействия (Mashine to Mashine, M2M). Такие системы бывают как проводными, так и беспроводными. В настоящее время, наиболее распространенные системы Интернета вещей базируются на технологиях передачи данных, использующих радиоканал. Широко известны и часто применяются в качестве основы сетей Интернета вещей системы и сети ZigBee, Bluetooht, WiFi, WiMAX, сотовые системы второго, третьего и четвертого поколения, а также системы 5G. Основной информацией, передаваемой по сетям IoT, является телеметрическая информация, полученная с датчиков. В большинстве случаев, физические параметры среды, которые оценивает и преобразует в передаваемое сообщение датчик, меняются достаточно медленно, и нет смысла постоянно контролировать измеряемые параметры [14-23]. Системы IoT отличаются от других систем передачи данных достаточно низкой скоростью передачи данных и редким опросом датчиков (от нескольких раз в час до нескольких раз в день). Таким образом, одной из главных особенностей систем IoT является малое энергопотребление. Чтобы улучшить данный параметр разработчиками IoT-систем были определены наиболее эффективные параметры, описанные в группе стандартов систем, относящихся к IoT. Также, на современной энергоэффективной элементной базе разрабатываются устройства IoT обеспечивающие низкое энергопотребление.

1. История появления технологии LoRa

В рамках концепции «Интернет вещей» LoRa Alliance в 2015 г. вместе с ETSI (European Telecommunications Standards Institute Европейский институт по стандартизации в области телекоммуникаций) разработали и выпустили стандарт для сетей межмашинного взаимодействия с малым энергопотреблением LPWAN (Low Power Wide Area Networks). В соответствии со стандартом сети LPWAN поддерживают технологию LoRa (Long Range) – технологию межмашинного взаимодействия большой дальности. Основой данной технологии является открытый энергоэффективный протокол LoRaWAN, разработанный исследовательским центром IBM Research совместно с Semtech Corporation. С помощью этого протокола можно организовать передачу данных на большие расстояния и развернуть сеть M2M [8].

Технология LoRaWAN основана на открытом энергоэффективном протоколе, разработанном специально для сетей большой емкости с большим радиусом действия. С помощью применения сетевого протокола технологии LoRaWAN система обеспечивает большой радиус действия (до 15 км) и большую емкость сети (около 1

млн. устройств), а также позволяет разрешить противоречие между обеспечением необходимой скорости передачи данных и сроком работы устройства при электропитании от аккумулятора.

Сеть LoRaWAN состоит из телекоммуникационного оборудования, абонентских оконечных устройств, абонентских управляющих устройств и устройств обработки данных. В качестве телекоммуникационного оборудования выступают приемо-передающее и коммутационное оборудование, и линии системы связи, реализующие эффективную передачу и прием телеметрических данных от датчиков до абонентов системы «Интернета вещей» LoRa. Абонентскими оконечными устройствами являются датчики и исполнительные устройства. Датчики это устройства, преобразующие внешние физические воздействия в цифровые сигналы, применяемые в качестве передаваемых сообщений по сети. В качестве исполнительных устройств используются электромеханические устройства, позволяющие выполнять механические действия над физическими объектами по сигналу пришедшему с управляющего устройства, датчика или телекоммуникационного устройства [11] . Абонентскими управляющими устройствами являются персональные и управляющие компьютеры, различные гаджеты и устройства отображения показателей и индикации работы оборудования системы «Интернета вещей», позволяющие абоненту управлять системой. В качестве устройств обработки данных выступают серверы и системы сбора и обработки телеметрических данных, на которых установлены программное обеспечение и приложения, позволяющие обрабатывать данные с датчиков и управлять исполнительными и телекоммуникационными устройствами [7, 8].

2. Описание системы LoRa

Системой передачи телеметрических данных, построенной по технологии LoRaWAN, является система передачи данных LoRa (от англ. Long Range – длинный диапазон). Особенность сигнала системы LoRa в том, что в нём используются ЛЧМ сигнал и принцип передачи с прямым расширением спектра. Таким образом, получается, что передача данных в системе LoRa осуществляется посредствам ЛЧМ сигнала с прямым расширением спектра, то есть последовательностью ЛЧМ импульсов, которая сформирована по принципам формирования М-последовательностей. Сигнал системы LoRa можно представить в виде математического выражения (рис. 1) [1].

$$S(t) = A_0 \cos\left(\omega_0 t + \frac{2F_{дев}}{T_c} t^2\right), \quad 0 < t < T_c$$

$F_{дев}$ – девиация частоты;

ω_0 – центральная частота сигнала;

$T_c = \dfrac{2^{SF}}{F_{дев}}$ – длительность сигнала;

SF – коэффициент расширения спектра

$B = F_{дев} T_c = 2^{SF}$ – база сигнала

Рис. 1. Основные соотношения, описывающие стандартный сигнал системы LoRa

Скорость передачи данных в системе LoRa, в основном, определяется значением коэффициента расширения спектра сигнала. Также от этого параметра зависят помехоустойчивость и дальность действия системы. При этом скорость передачи данных адаптируется с учтём выполняемых задач и зависит от требуемой дальности и помехоустойчивости системы.

Сеть LoRaWAN оптимизирует длительность сигнала для обеспечения необходимой скорости передачи данных и для минимизации потребляемой электроэнергии. Исходя из сравнения с другими устройствами семейства LPWAN с помощью системы LoRa можно добиться снижения энергопотребления примерно в 100 раз.

В России на основании Решения Государственной комиссии по радиочастотам (ГКРЧ) № 08-24-01-001 от 28.04.2008 и № 07-20-03-001 от 07.05.2007 для передачи телеметрических данных отведены частотные диапазоны 433,075-434,750 МГц и 868,7-869,2 МГц, являющиеся нелицензируемыми. Сеть LoRaWAN использует диапазон частот 868 МГц с мощностью до 25 мВт и поэтому не требует оформления разрешения на использование радиочастот от ГКРЧ [4,5].

3. Применение в системе LoRa сигнала OFDM

По сравнению со стандартным ЛЧМ сигналом с прямым расширением спектра, применяющимся в системе LoRa, который является сигналом с аналоговой модуляцией, сигнал с ортогональным мультиплексированием и частотным разделением OFDM (Orthogonal frequency-division multiplexing), минимизирует влияние многолучевого замирания в канале и увеличивает эффективность использования радиочастотного спектра.

В отличие от стандартного сигнала ЛЧМ системы LoRa сигнал OFDM позволяет экономить спектр и использовать его более эффективно. Применение сигнала OFDM обеспечивает передачу данных на нескольких узкополосных поднесущих одновременно. На каждой поднесущей передаются с небольшой скоростью несколько бит данных. Таких поднесущих, как минимум, вдвое больше, чем ЛЧМ импульсов, которые передаю только один бит данных в сигнале с расширением спектра. Однако при этом, возникает проблема большого

пик-фактора сигнала и эта проблема до сих пор актуальна для исследования и поиска технических решений, которые разрабатываются и предлагаются в настоящее время.

3.1. Структурная схема системы LoRa

В стандартной реализации системы LoRaWAN применяется сигнал с ЛЧМ модуляцией. Структурная схема в этом случае содержит модулятор ЛЧМ сигнала и демодулятор, основанный на экстракторе, что усложняет реализацию модема. Такой подход к построению модема дает следующие преимущества: устойчивость к отклонению частоты от номинального значения, снижение требований к тактовому генератору, обеспечивает компенсацию сосредоточенных помех при помощи экстрактора, [1]**.** Однако, данная конструкция модема имеет достаточно малую скорость передачи данных. С ростом количества абонентов сетей радиодоступа и сетей сотовой связи скорость передачи данных систем кратно возрастает. С появлением сетей 5G концепция «Интернета вещей» получила «вторую жизнь» и реализация данной концепции стала доступна практически каждому, а преимущества данной технологии стали очевидны широкому числу современных абонентов. В настоящее время система LoRa с ЛЧМ сигналом уже не отвечает требованиям скорости передачи данных и в данной работе предлагается применение OFDM сигнала в системе LoRa.

Особенность технологии передачи LoRa состоит в том, что в ней совмещены расширение спектра за счёт помехоустойчивого кодирования и применение сложных сигналов.

На рисунке 2 представлена структурная схема системы LoRa с применением технологии OFDM.

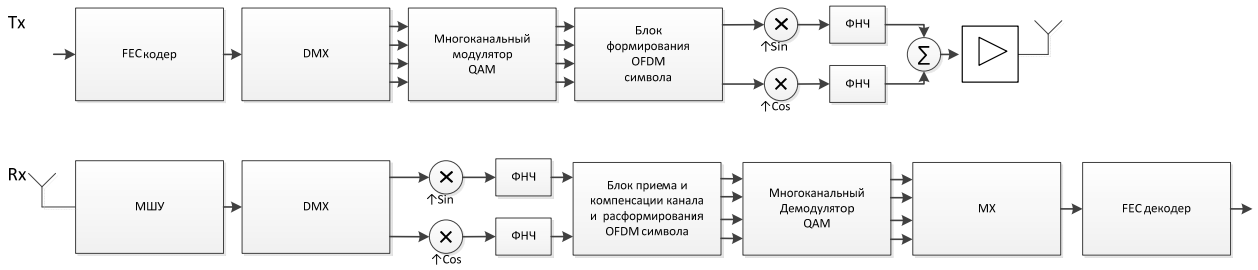


Рис. 2. Структурная схема системы LoRa с применением технологии OFDM

Передаваемая последовательность бит данных в передатчике, кодируется в FEC-кодере для снижения влияния многолучевого канала. Коды, корректирующие ошибки методом упреждения (Forward Error Correction) позволяют повысить устойчивость к импульсным помехам и увеличить вероятность правильного приема передаваемого сообщения.

Далее закодированный поток бит данных преобразуется из последовательного в параллельный при помощи последовательно-параллельного преобразования. После канального кодирования закодированные биты данных модулируются с использованием QAM-модуляции, в результате чего сигнал принимает вид QAM созвездия. На следующем этапе формирования OFDM символа производится операция ОБПФ. В результате выполнения следующего преобразования

$$\dot{S}_k = \frac{1}{N}\sum_{n=0}^{N-1}\dot{A}_n e^{j\frac{2\pi}{N-1}nk}, \quad k = 0,..,N-1, \tag{1}$$

где N – порядок ОБПФ, равный общему числу поднесущих OFDM символа; $\dot{A}_n$ – блок промодулированых QAM символов; $k = 0,..,N-1$ – номер отсчета комплексной огибающей формируемого основного блока отсчетов OFDM символа; $n = 0,..,N-1$ – номер поднесущей.

В блоке формирования OFDM символа, после ОБПФ, параллельный поток данных преобразуется в последовательный и далее к нему добавляются пилотные частоты и защитный префикс. Сформированный OFDM символ ВЧ генератор переносит в высокочастотную область. Сигнал с выхода передатчика поступает в канал связи, где за счет многолучевого распространения радиоволн претерпевает некоторые изменения.

Приемник выполнен по принципу преобразования сигнала в обратном порядке. Смесь сигнала с шумом поступает на малошумящий усилитель (МШУ), где малый уровень сигнала усиливается и, далее разделяется на квадратурные составляющие. Основным блоком приемника, в котором происходит преобразование сигнала, является «Блок приема и компенсации канала и расформирования OFDM символа». В нём производиться расформирование символа OFDM: удаление циклического префикса, удаление синхросимволов, а также выполняется быстрое преобразование Фурье. Одновременно с преобразованием сигнала по синхросимволам производиться оценка влияния канала и подстройка характеристик сигнала. На следующем этапе сигнал демодулируется в демодуляторе QAM. В итоге получается поток битов равный потоку, который передал передатчик с FEC-

кодера. Далее в FEC-декодере происходит декодирование сигнала, и поток данных поступает к получателю сообщений.

Особенностью схемы приемника, представленного в [1] является экстрактор, который компенсирует сосредоточенные узкополосные помехи. Экстрактор позволяет работать совместно с современными сотовыми системами связи в диапазоне ISM. Однако, данная схема является низкоскоростной, так как для передачи данных и компенсации помех использует весь выделенный частотный канал. При применении сигнала OFDM передача данных и оценка принятого сигнала производится по нескольким частотным субканалам. Такой подход позволяет: увеличить скорость передачи; точнее оценить помеховую обстановку в выделенном частотном канале; определить положение сосредоточенной помехи в частотном субканале и исключить влияние этой помехи путем отключения соответствующей поднесущей сигнала OFDM или фильтрации её с помощью режекторного фильтра. При этом обеспечивается возможность передачи данных с большой скоростью и экономное расходование ресурса питающего аккумулятора [2].

3.2. Параметры системы LoRa с применением OFDM сигнала

В данной работе были определены параметры сигнала системы LoRa при использовании для формирования сигнала технологи OFDM.

Основные параметры LoRa с применением OFDM сигнала представлены в таблице 1.

Применение технологии OFDM для формирования сигнала системы LoRa позволяет повысить спектральную эффективность системы передачи телеметрических данных, увеличить скорость передачи, по сравнению со стандартной системой LoRa и увеличить количество абонентских устройств в сети.

Расчетная дальность действия модема системы LoRa составляет 5,7 км. Одной из особенностей рассматриваемой системы является большая дальность действия, которая достигается за счет построения системы на основе технологии LPWAN (в случае со стандартным сигналом), а также за счет применения сигнала OFDM и его проникающей способности, позволяющей вести эффективную передачу данных на различных частотах и эффективно использовать частотный спектр системы. Соотношение мощности сигнала, и его длительности при применении OFDM сигнала, обеспечивающего равномерность распределения мощности в рабочей полосе частот, позволяют не только эффективно передавать данные на большие расстояния, но и осуществлять энергоэффективную передачу данных, а также и работать автономно с использованием аккумуляторной батареи в течении продолжительного время (от года до нескольких лет) [11,12].

Таблица 1

Параметры сигнала системы LoRa с применением OFDM сигнала

№	Параметр	Значение
1.	Диапазон рабочих частот, МГц	868
2.	Длительность защитного интервала, $T_{защ}$, с	$160*10^{-9}$
3.	Длительность интегрируемой части OFDM-символа, T_{OFDM}, с	$640*10^{-9}$
4.	Расстояние между поднесущими, Δf, Гц	1562
5.	Метод модуляции	QPSK
6.	Количество используемых поднесущих в заданной полосе частот, Nисп подн	80
7.	Количество поднесущих, используемых для передачи данных (кодовых бит), $N_{подн}$ код бит	71
8.	Число поднесущих Nподн в одном OFDM-символе, Nподн	64
9.	Число неиспользуемых (нулевых) поднесущих, Nисп подн	7
10.	Интервал дискретизации по времени комплексной огибающей OFDM-символа, Δt, с	$10*10^{-9}$
11.	Число отсчетов огибающей OFDM-символа на защитном интервале, $N_{защ}$	16
12.	Длительность защитного интервала, $T_{защ}$, с	$160*10^{-9}$
13.	Длительность OFDM-символа, T_c	$800*10^{-9}$
14.	Общее число отсчетов огибающей OFDM-символа, $N_{отсч}$	80
15.	Число кодовых бит на одной поднесущей или в одном КАМ-символе, $N_{бит}$ КАМ	2
16.	Число кодовых бит в одном OFDM-символе (блоке), $N_{код}$ бит бл	142
17.	Число информационных бит в одном OFDM-символе (блоке) на входе кодера, $N_{инф}$ бит бл	71
18.	Выходная мощность передатчика, дБм	20
19.	Расчетная дальность системы	5732 м
20.	Расчетная скорость передачи данных	5,6 кбит/с

4 Характеристики оборудования LoRa

В настоящее время на рынках Европы и США представлены готовые решения для организации сети LoRa в диапазонах 868 МГц и 902 МГц. Готовые модемы системы LoRa построены на элементах аналоговой СВЧ-техники, что увеличивает стоимость реализации сети.. Переход к цифровой технике позволяет обеспечивать высокие скорости передачи данных и обработки сигналов и снизить стоимость оборудования сети [9].

Одним из основных решений для рынка систем M2M/IoT является семейство радиомодемов SX127x производства компании Semterch. Данные модемы работают в диапазоне 860-1000 МГц с сигналами системы LoRa.

В таблице 2 представлены основные характеристики модемов семейства SX127x [2, 10].

Чипсеты серии SX127x является универсальным. Используя их можно реализовать модемы как со стандартным сигналом LoRa. так и модемы для системы LoRa с сигналом OFDM.

Таблица 2

Основные характеристики RF-трансиверов семейства SX127x

Наименование	SX127x
Диапазон работы частот, МГц	860-1020
Выходная мощность, дБм	+20
Ширина полосы пропускания, кГц	125-500
Доступные типы модуляции	FSK, GFSK, MSK, GMSK, OOK, LoRa
Скорость передачи при использовании модуляции LoRa, кбит/с	0,24-37,5
Чувствительность передатчика, дБм	-117…-137

Заключение

1) Технология LoRa перспективна для построения сетей IoT и позволяет повысить эффективность этих сетей.
2) Использование нелицензируемого диапазона ISM позволяет снизить затраты на развертывание сетей IoT на основе системы LoRa, так как не требуется лицензия на использование данного частотного диапазона.
3) Система LoRa с OFDM сигналом обеспечивает дальность не менее 5,5 км в условиях городской застройки и скорость передачи данных примерно 5,6 кбит/с.
4) Большой интерес для дальнейшего исследования представляет моделирование системы LoRa с применением OFDM технологии в условиях многолучевого канала и различных моделей канала.
5) В рамках продолжения работы необходимо оценить возможность реализации системы LoRa с сигналом OFDM на основе использования современных цифровых сигнальных процессоров.

Литература

1. *Болдина В.И., Фролов А.А.* Современная сверхузкополосная система передачи данных LoRa // Фундаментальные проблемы радиоэлектронного приборостроения / Материалы Международной научно-технической конференции «INTERMATIC – 2017». М.: МГТУ МИРЭА - ИРЭН РАН. 2017. Часть 4. С. 1142-1146.
2. *Верхулевский К.* «Технология LoRa компании Semtech: новый импульс развития «Интернета вещей» // Беспроводные технологии. 2015. № 3. С.8-14.
3. *Сикарев А.А., Лебедев О.Н.* Микроэлектронные устройства формирования и обработки сложных сигналов. М.: Радио и связь, 1983. 216 с.
4. Решение ГКРЧ от 07.05.2007 №07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия», 2007. 10 с.
5. Решение ГКРЧ от 28.04.2008 №08-24-01-001 «О внесении изменений в решение ГКРЧ от 07.05.2007 N 07-20-03-001 " О выделении полос радиочастот устройствам малого радиуса действия", 2008. 5 с.
6. *Фролов А.А.* Влияние узкополосных и широкополосных помех на многочастотную импульсную СШП-систему радиодоступа // Электросвязь. 2014. № 7. С. 32-35.
7. *Josh Blum*. LoRa modem with LimeSDR. Blog on MYRIADRF,10.6.2016, [Электронный ресурс]: https://myriadrf.org/blog/lora-modem-limesdr/. (Дата обращения 21.03.2021)
8. LoRa-Alliance, „LoRaWAN 101 – A Technical Introduction“, [Электронный ресурс]: https://www.lora-alliance.org/What-Is-LoRa/Technology, May 2017.
9. RC232 user manual. [Электронный ресурс]: https://www.radiocrafts.com (Дата обращения 12.04.2021)
10. SEMTECH, “LoRa Modulation Basics“, Application Note AN1200.22,May 2015.
11. *Орлов В.Г., Тюмин С.Г.* Стандарты беспроводной связи для системы умный дом // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 20-28.
12. Интернет ресурс: [Электронный ресурс]: https://habrahabr.ru/company/rtl-service/blog/304312/ (Дата обращения 28.09.2017).
13. Интернет ресурс: [Электронный ресурс]: http://lorawan.lace.io/faqs/lora/ (Дата обращения 28.09.2017).
14.*Орлов В.Г., Шаврин С.С.* Беспроводные мобильные приложения в системах мониторинга и диспетчеризации технологических служб // Фундаментальные проблемы радиоэлектронного приборостроения. 2008. Т. 8. № 1. С. 247-251.
15. *Бакулин М.Г., Крейнделин В.Б.* Проблема повышения спектральной эффективности и емкости в перспективных системах связи 6G // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 25-31.
16. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Анализ пропускной способности канала MIMO в условиях замираний // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 2. С. 13-20.
17. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Методы приема псевдослучайных после-довательностей в системах радиосвязи // REDS: Телекоммуникационные устройства и системы. 2018. Т. 8. № 1. С. 108-112.
18. *Крейнделин В.Б., Старовойтов М.Ю.* Повышение помехоустойчивости системы связи MIMO с пространственным мультиплексированием методом додетекторного сложения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 4-13.

19. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Исследование вероятностных моделей радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон с помощью компьютерного моделирования // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 1. С. 64-68.

20. *Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К.* Эффективность методов обработки сиг-налов в системах MU-MIMO высоких порядков // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 24-30.

21. *Крейнделин В.Б., Панкратов Д.Ю.* Вероятностная модель радиоканала MIMO с учетом вза-имной корреляции передающей и приемной сторон // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 1. С. 103-107.

22. *Фролов А.А.* Оценка эффективности совместного использования радиочастотного спектра многочастотными сверхширокополосными системами радиодоступа и WIFI // T-Comm: Телеком-муникации и транспорт. 2019. Т. 13. № 10. С. 21-26.

23. *Фролов А.А.* Исследование многочастотной сверхширокополосной системы радиодоступа с совмещением технологий OFDM и кодового разделения абонентов // REDS: Телекоммуникаци-онные устройства и системы. 2017. Т. 7. № 1. С. 77-83.

ANALYSIS OF THE POSSIBILITIES OF THE INTERNET OF THINGS "LORA" BASED ON THE OFDM SIGNAL

Frolov A. Alexey,
Senior Lecturer of the Department of RTS, Ph.D., MTUCI, Moscow, Russia,
a.a.frolov@mtuci.ru

Alena A.Tambovtseva,
Student MTUCI, Moscow, Russia,
tambovceva1999@mail.ru

Abstract

The paper presents the results of the possibility of using the OFDM signal in the "LoRa" Internet of Things system. In this paper, the basic concept of the Internet of Things. Its principle of operation and the most common area of application are also described. The architecture of the "LoRa" system and the structural elements of the network are investigated. The substantiation of the possibility of using an OFDM signal, which is not standard for the "LoRa" system, is presented. The advantages and disadvantages of the OFDM signal proposed for use in the system are determined in comparison with the standard chirp signal with direct signal extension used in the "LoRa" system. The block diagram of the modem of the LoRa system based on the OFDM signal and the main parameters of the modem are presented, which make it possible to present a simulation computer model of this system for the implementation of a modem on a modern element base.

Keywords: *Internet of Things, M2M system, OFDM signal, LoRa system, LoRaWAN network, ISM frequency range, telemetry transmission, unlicensed spectrum.*

МОДЕРНИЗАЦИЯ ЛАБОРАТОРИИ ПО ИЗУЧЕНИЮ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Маликова Елена Егоровна,
доцент кафедры ССиСК, к.т.н., МТУСИ, Москва, Россия,
emalikova@gmail.com

Канищева Маргарита Геннадьевна,
магистрант МТУСИ, Москва, Россия,
margo.kan@list.ru

Шишкин Дмитрий Витальевич,
магистрант МТУСИ, Москва, Россия,
draknem@gmail.com

Аннотация

В статье приводится описание процесса, расширения лабораторного комплекса по изучению мультисервисных сетей связи. Для объединения используется оборудование виртуального облака, включающего два сервера. Рассматриваются способы подключения нового оборудования ведущего российского производителя Eltex к программной телефонной станции Asterisk. Представлена новая схема подключения имеющегося лабораторного оборудования. Приведено описание нового лабораторного практикума для студентов бакалавриата и магистратуры кафедры «Сети связи и системы коммутации» (ССиСК) МТУСИ.

Ключевые слова: *мультисетвисная сеть связи, концепция виртуализации, гипервизор, язык лабораторный комплекс, программная телефонная станция Asterisk, оборудование Eltex, операционная система Linux, виртуальная машина.*

Введение

В 2011 году организацией ITU-T было объявлено о новой концепции развития инфокоммуникаций – «Будущие сети (Future Networks – FN)». В этом же году вышли рекомендации серии Y.3000 [1]. В основе концепции Будущих сетей лежат методы и средства искусственного интеллекта, технологии виртуализации, также такие новые технологии, как обработка больших объёмов данных, облачные и туманные технологии, технологии беспроводной связи, Интернет вещей и др.

На сегодняшний день существует высокая потребность в инженерах связи, которые способны в кротчайшие сроки организовать связь на современных инфокоммуникационных сетях. При этом они должны сделать это самым оптимальным способом, быстро, качественно и недорого.

Статья посвящена исследованию и постановке лабораторных работ по изучению современных мультисервисных сетей. Особое значение уделено программной телефонной станции Asterisk.

Описание мультисервисной сети связи на кафедре СС и СК

На кафедре СС и СК располагается лабораторный комплекс по изучению мультисервисных сетей связи [6-9]. Данный комплекс включает в себя оборудование нескольких лабораторий кафедры. В лаборатории Л-402 находятся стенды по изучению программной телефонной станции Asterisk, а также оборудования Eltex [2]. Помимо этого, в мультисервисную сеть лаборатории входят: АТС типа Coral (Л-409), станция SI3000 IMS фирмы Iskratel (Л-411), а также учрежденческая производственная станция Definity (Л-404).

Большая часть лабораторных работ проходит на оборудовании, посвященном изучению программной телефонной станции Asterisk (рис. 1), на котором создано 20 рабочих стендов. Каждый стенд включает в себя рабочую станцию, виртуальную машину (*Virtual Machine* - VM), на которой установлена IP-АТС Asterisk, а также коммутатор и два SIP-телефона. У студентов есть доступ к правам суперпользователя для выполнения привилегированных операций со станцией. Так, например, они могут снять трафик с сетевого интерфейса помощью программы-анализатора трафика Wireshark на сетевом интерфейсе или перезапустить станцию. Каждый стенд полностью независим от любого другого, также действия одной бригады студентов никак не влияют на работу остальных бригад [3].

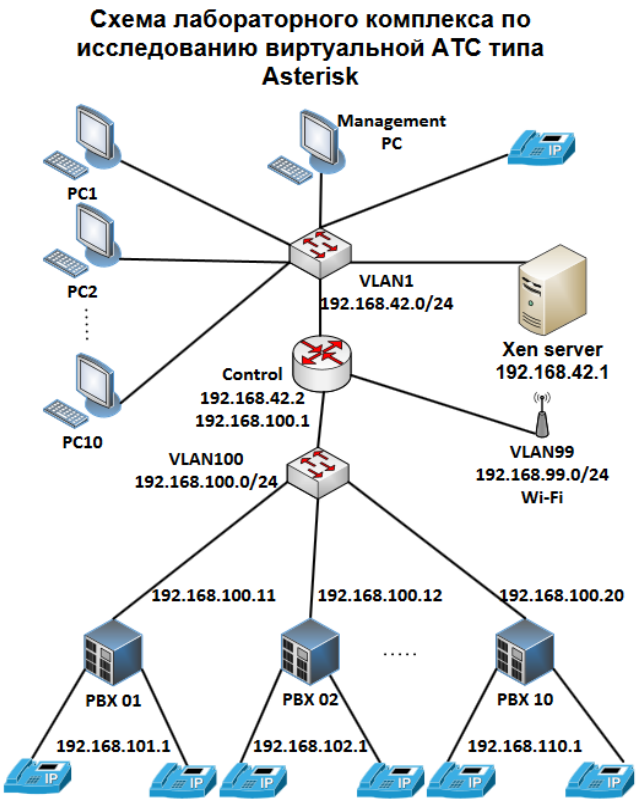


Рис. 1. Схема лабораторного комплекса по изучению виртуальной станции Asterisk

Для хранения данных и управления всеми стендами было создано виртуальное облако, которое состоит из двух серверов. Каждый сервер включает в себя жесткий диск (*HDD – Hard Disk Drive*), оперативную память (*RAM – Random Access Memory*) и набор центральных процессоров (*CPU – Central Processing Unit*). Также у серверов имеются сетевые интерфейсы, которые подключаются к коммутаторам (рис. 2).

В серверах данного типа процессоры, оперативная память и жесткие диски объединены в общее логическое устройство.

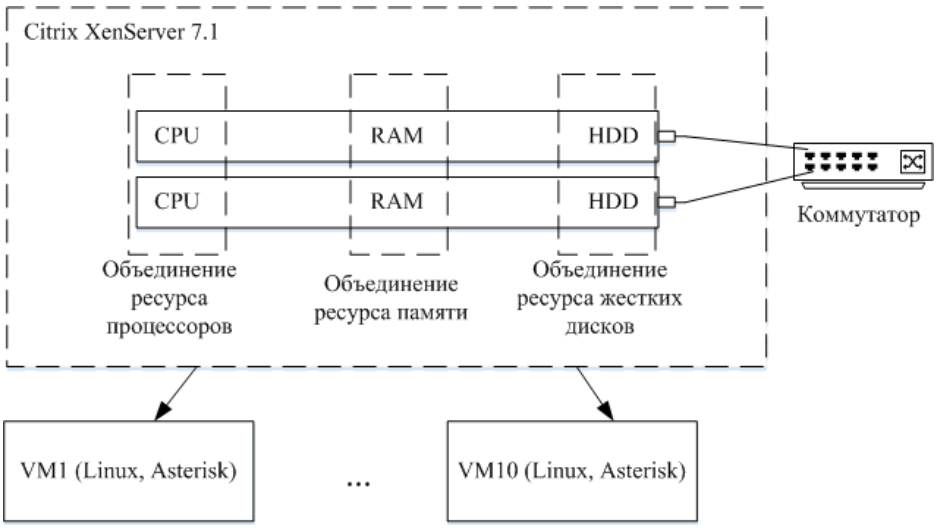


Рис. 2. Создание виртуальных машин на серверном оборудовании

При объединении общих ресурсов двух серверов появилась возможность организовать виртуальные машины. В качестве системы виртуализации был выбран гипервизор *Citrix XenServer* 7.1. Он позволяет из всех объединенных ресурсов выделить часть ресурса для каждой виртуальной машины. Так, первая *VM* использует несколько центральных процессоров из общего набора, а также определенные области оперативной памяти и жестких дисков. Для остальных *VM* аналогичным образом производится выделение других ресурсов.

Всего организуется 10 виртуальных машин по числу рабочих стендов на лабораторном комплексе. На каждой виртуальной машине устанавливаются операционная система *Linux* и программный пакет *Asterisk*.

Виртуальные машины необходимо подключить к физическим ресурсам сети. Для этого используется коммутатор фирмы *Cisco*, к которому от каждого рабочего места в соответствующие порты подключаются два телефона и *IP*-АТС каждой бригады студентов (рис. 3).

Телефонные порты выделены в отдельные *VLAN*. Сервер подключается в специально выделенный порт коммутатора. Порт является транковым и через него идут все соединения *VLAN* на коммутаторе. Внутри сервера *VLAN* разбиваются на виртуальные интерфейсы. Через физический интерфейс сервера идет подключение к виртуальному интерфейсу машины, который соответствует номеру *VLAN*. Также в лабораторном комплексе присутствует главная *IP*-АТС, к которой подключены все виртуальные машины через интерфейс 100.

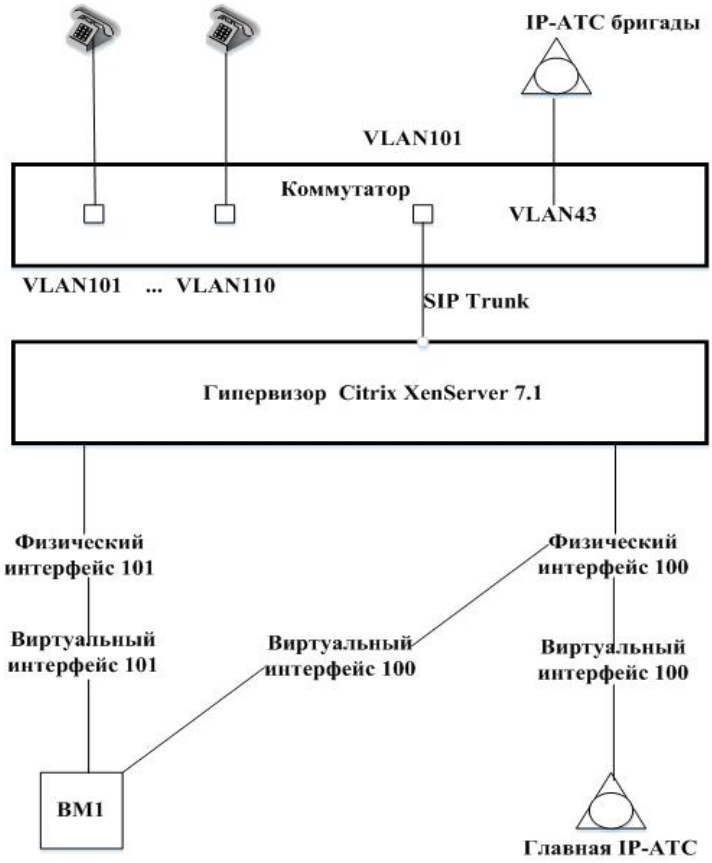


Рис. 3. Сетевое подключение серверного оборудования

Описание нового оборудования для лабораторного комплекса

Для расширения комплекса лабораторных работ было задействовано новое оборудование предприятия Eltex, которое является ведущим российским разработчиком и производителем телекоммуникационного оборудования [4]. Для лабораторного стенда был использовано следующее оборудование:

1.Коммутатор MES3124. Внешний вид данного коммутатора представлен на рисунке 4. Он имеет 24 порта 10/100/1000 Base-T. Для коммутаторов данной серии характерно наличие значительного запаса производительности, так как они имею универсальные интерфейсы, которые работают на скоростях 1 Гбит/с и 10 Гбит/с.

Рис. 4. Внешний вид коммутатора MES3124

2. Транковый шлюз SMG-1016M (рис. 5).

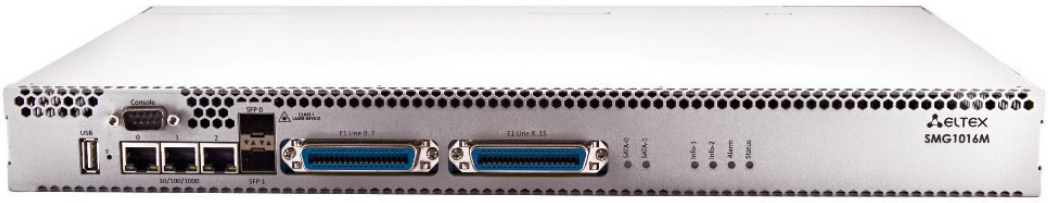


Рис. 5. Транковый шлюз SMG-1016M

SMG-1016M представляет собой транковый шлюз, который может применяться для соединения сигнальных и информационных потоков сетей с коммутации каналов и коммутации пакетов. Также данное устройство может выполнять функции IP-АТС. При этом поддерживаются функция СОРМ, а также различные дополнительные виды обслуживания (ДВО). Данное устройство применяется для построения современных мультисервисных сетей связи.

3. Абонентский маршрутизатор RG 2402 G-W (рис. 6).

Рис. 6. Абонентский маршрутизатор RG-2402G-W

Машрутизатор поддерживает услугу передачи речи поверх протокола IP (VoIP). В него могут включаться как SIP-телефоны, так и аналоговые телефонные аппараты. Имеется Wi-Fi модуль для подключения мобильных абонентов.

Описание лабораторной работы «Организация связи межу оборудованием Eltex и Asterisk»

Целью работы является изучение принципов маршрутизации на современной мультисервисной сети. Предварительно необходимо выполнить следующие действия:

1. Настроить программную телефонную станцию Asterisk;
2. Настроить оборудование Eltex;
3. Организовать телефонную связь между оборудованием Eltex и станцией Asterisk. Для выполнения данной задачи нужно произвести настройку маршрутизаторов между оборудованием;
4. Снять трассировки сигнального обмена при установлении телефонного вызова между лабораторным оборудованием.

На рисунке 7 представлена схема соединения между лабораторными стендами Asterisk и Eltex и указаны IP-адреса всех устройств.

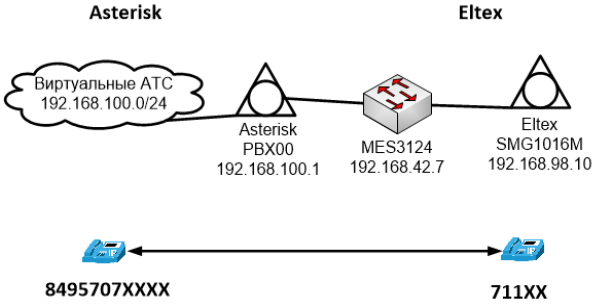


Рис. 7. Схема соединения между оборудованием Asterisk и Eltex

Для данной лабораторной работы был разработан общий план нумерации абонентов всего лабораторного комплекса. На рисунке 8 приведена подробная структурная схема соединения между лабораторными стендами Asterisk и Eltex с указанием IP-адресов. У всех абонентов прописывается десятизначная нумерация с префиксом 495.

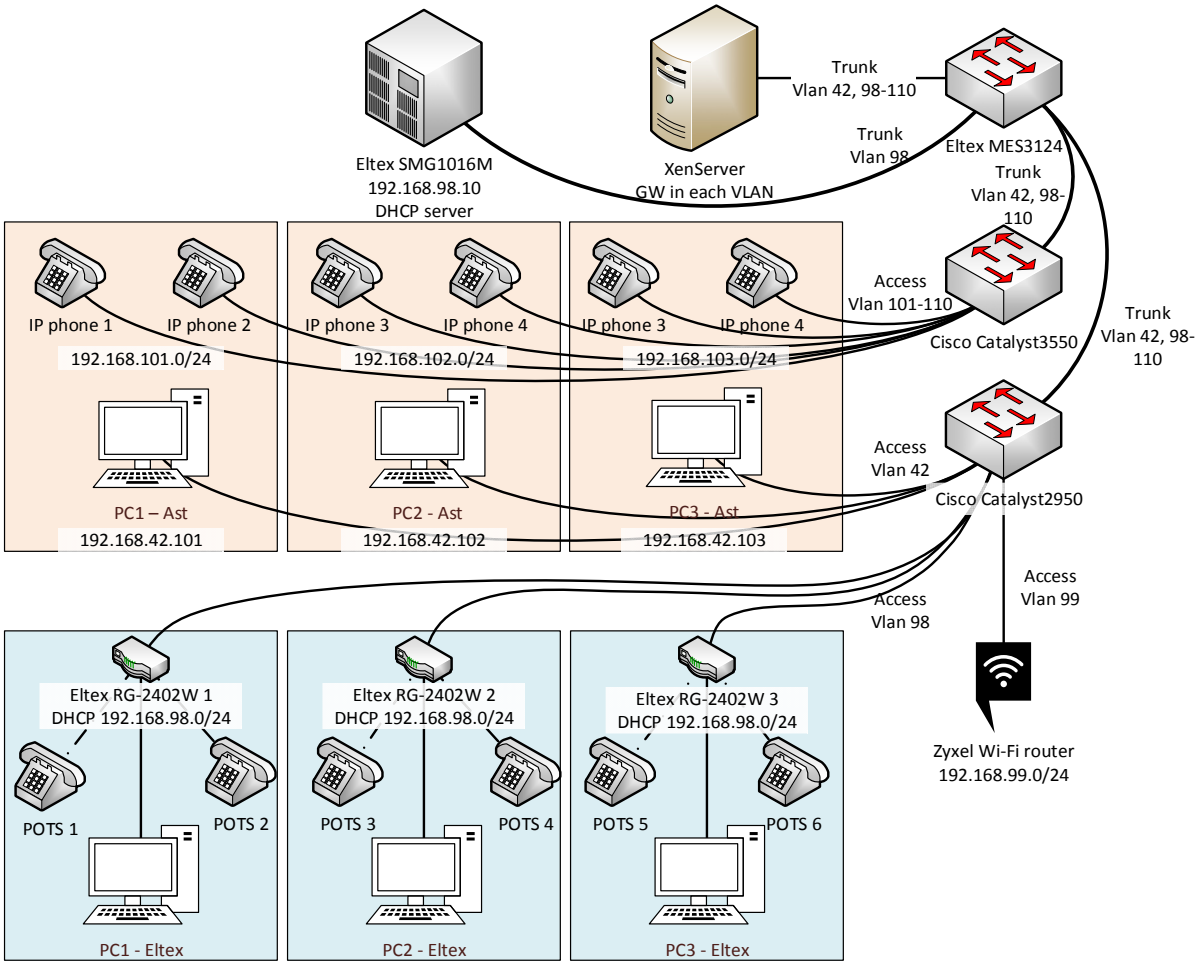


Рис. 8. Схема соединения между оборудованием Asterisk и Eltex

Для соединения всех абонентов была произведена коммутация оборудования на серверной стойке (рисунок 9).

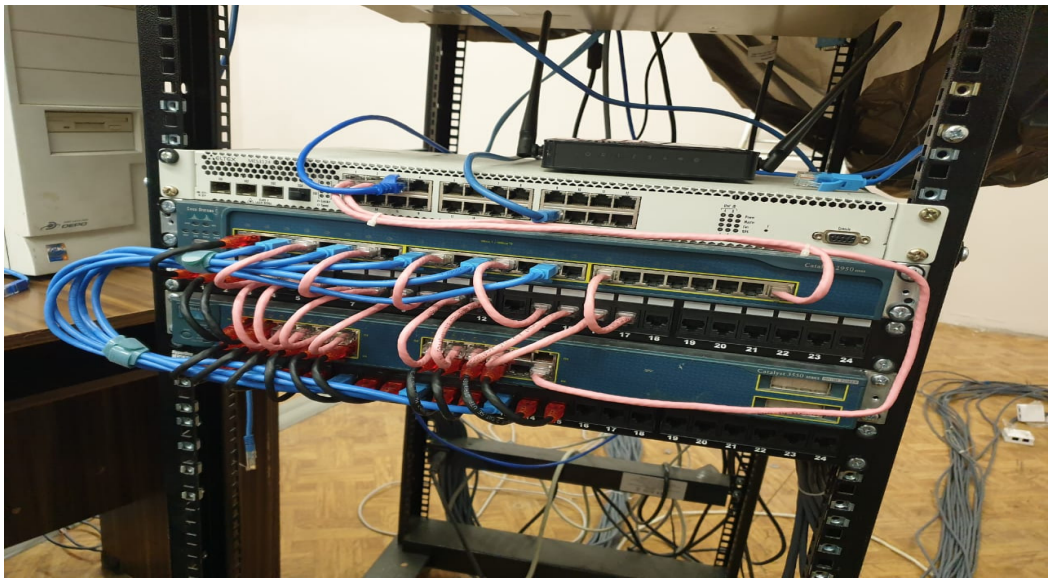


Рис. 9. Серверная стойка с оборудованием

На первом этапе выполнения работы необходимо настроить телефонную станцию Asterisk и прописать всех абонентов [5].

Далее производится настройка оборудования Eltex (рис. 10), для этого необходимо:

- открыть браузер и в адресной строке набрать адрес IP-терминала:
- ввести логин и пароль для входа в WEB-интерфейс.

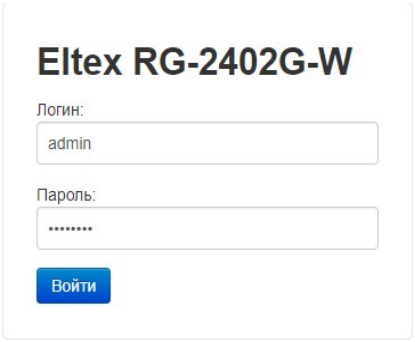


Рис. 10. Настройка оборудования Eltex

В разделе IP-телефония во вкладке «Линия 0» нужно ввести данные пользователя, выданные преподавателем (рис. 11): телефонный номер, логин и пароль.

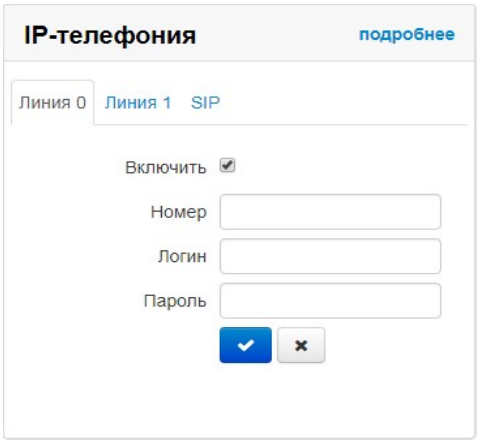


Рис. 11. Ввод данных пользователя

В этом же разделе (IP-телефония) необходимо произвести настройку SIP-сервера, перейдя на вкладку «SIP». Каждой бригаде необходимо заполнить все поля значениями, которые заданы преподавателем, и зарегистрировать IP- абонентов (рис. 12):

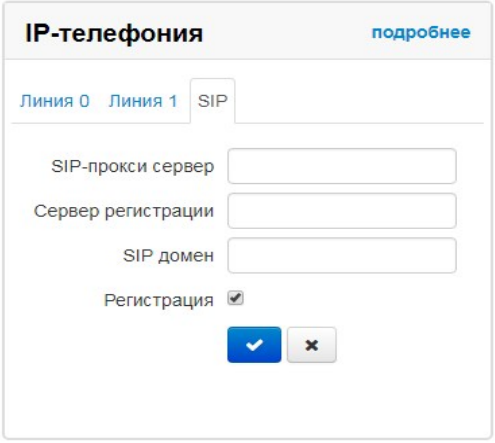


Рис. 12. Выполнение регистрации на оборудовании Eltex

Далее нужно организовать связь между абонентами, включенными в оборудование Asterisk и Eltex и произвести разговор.

После настройки маршрутизатора с помощью программы Wireshark выполняется захват трафика соединения между лабораторными стендами Asterisk и Eltex (рис. 13).

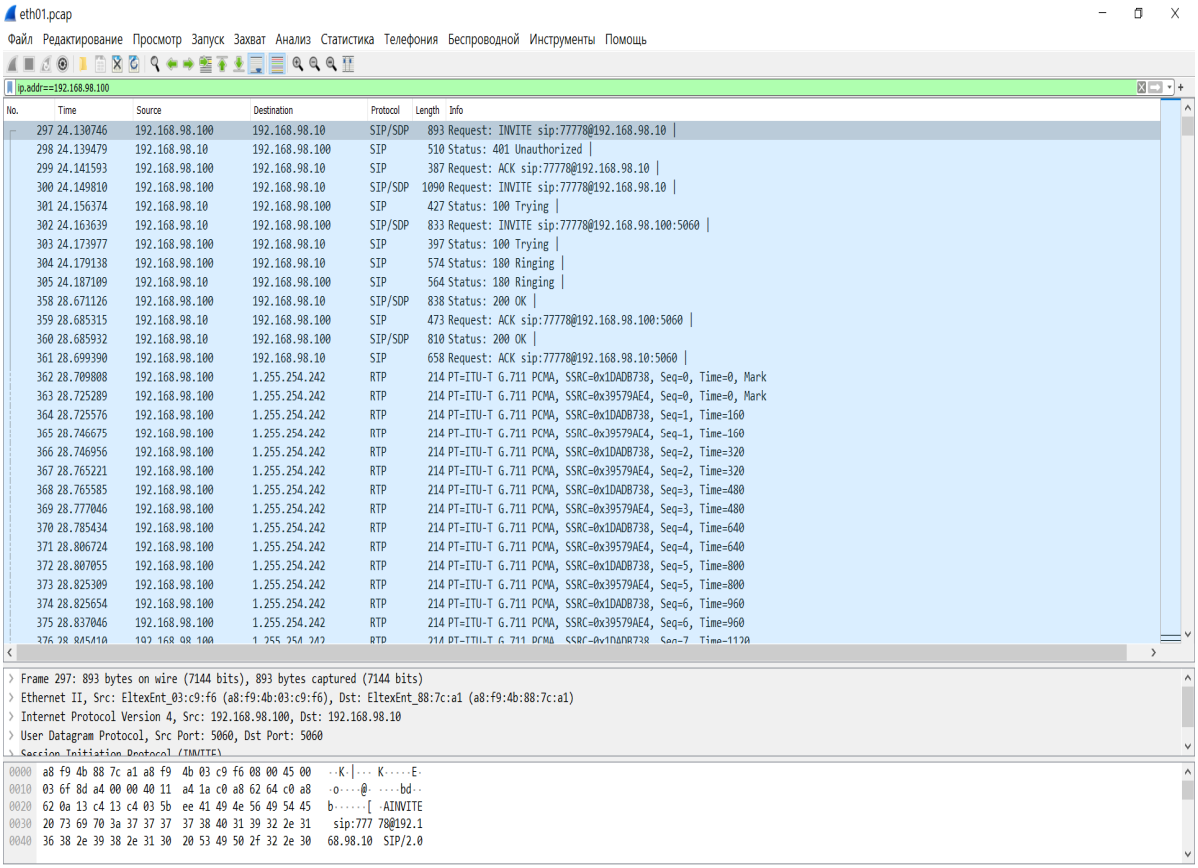


Рис. 13. Захваченный трафик с помощью программы WireShark

На рисунке 14 приведен пример визуализации голосового потока между абонентами телефонных станций, из которого видно, что большую часть в разговоре составляют паузы.

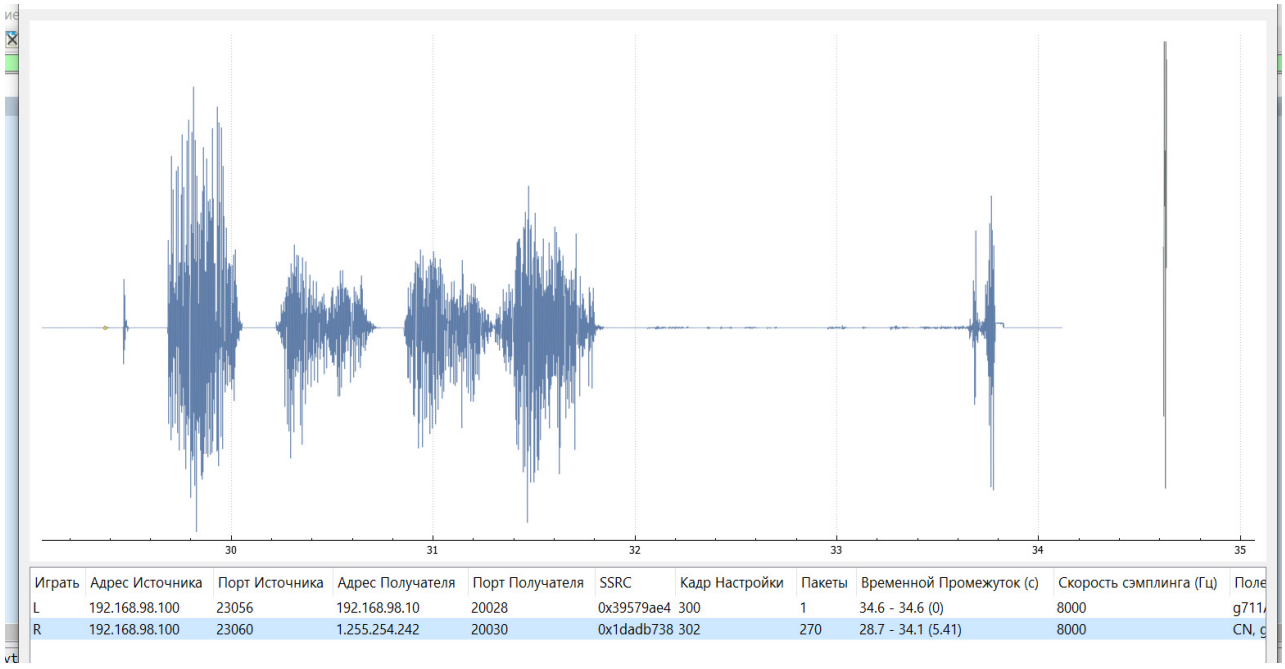


Рис. 14. Пример проигрывания голосового потока

Выводы

Технология виртуализации, которая была использована на лабораторном комплексе по изучению технологий мультисервисных сетей, является одной из ключевых технологий в концепции Будущих сетей. Новые лабораторные работы, выполняемые на данном комплексе, помогают организовать современный учебный процесс, при котором у студентов формируются навыки работы на современном инфокоммуникационном оборудовании. При выполнении работ студенты учатся самостоятельно создавать абонентов на виртуальных IP-АТС, прописывать для них план набора, изучать принципы нумерации и маршрутизации на современных мультисервисных сетях, анализировать прохождение сигнального и информационного трафика с помощью программы-анализатора трафика Wireshark. Все это мотивирует студентов к самостоятельному исследованию современных средств организации связи.

Литература

1. Рекомендации МСЭ-Т Y.3000 (05/2011). Серия Y: Глобальная информационная инфраструктура, аспекты протокола интернет и сети последующих поколений. Сети последующих поколений – Будущие сети.
2. *Меггелен Дж., Мадсен Л., Смит Дж.* Asterisk^{EM} : будущее телефонии, 2-е издание. Пер. с англ. СПб: Символ-Плюс, 2019. 656 с.
3. *Канищева М.Г., Железов Д.Б., Маликова Е.Е* Разработка лабораторных работ по изучению и исследованию мультисервисных сетей связи //Телекоммуникационные информационные технологии, №2, 2019. С. 82-87.
4. https://eltexsl.ru/products/oborudovanie/ (Дата обращения 05.04.2021).
5. *Канищева М.Г., Маликова Е.Е., Пелевин И.И., Пшеничников А.П.* Основы работы с виртуальной телефонной станцией IP-АТС Asterisk: учебное пособие. М.: Медиа Паблишер, 2021. 100 с.
6. *Маликова Е.Е., Пшеничников А.П.* Особенности преподавания перспективных инфокоммуникационных технологий на кафедре сети связи и системы коммутации в МТУСИ // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2018. Т. 7. № 3. С. 35-42.
7. *Маликова Е.Е., Пшеничников А.П.* Особенности формирования компетенций по направлению подготовки "инфокоммуникационные технологии и системы связи" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 2. С. 23-25.
8. *Антонова В.М., Богомолова Н.Е., Маликова Е.Е.* О новом лабораторном практикуме по изучению виртуальной телефонной станции IP-АТС ASTERISK // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 3. С. 20-22.
9. *Антонова В.М., Маликова Е.Е.* Использование программы технических расчетов MATLAB для постановки новых лабораторных курсов на кафедре "сети связи системы коммутации" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2016. Т. 5. № 3. С. 9-10.

MODERNIZATION OF THE STUDY LABORATORY MULTISERVICE NETWORKS

Elena E. Malikova.
Associate professor of NCaSC department, PhD., MTUCI, Moscow, Russia,
emalikova@gmail.com

Margarita G. Kanishcheva,
Graduate MTUCI, Moscow, Russia,
margo.kan@list.ru

Dmitry V. Shishkin,
Graduate MTUCI, Moscow, Russia,
draknem@gmail.com

Abstract

The article describes the process of expanding the laboratory complex for the study of multiservice communication networks. The equipment of a virtual cloud, which includes two servers, is used for unification. Methods of connecting new equipment of the leading Russian manufacturer Eltex to the Asterisk software telephone exchange are considered. A new scheme for connecting the existing laboratory equipment is presented. A description of a new laboratory practice for undergraduate and graduate students of the Department of Communication Networks and Switching Systems (CCiSK) of MTUCI is given.

Keywords: *multiservice network, virtualization concept, hypervisor, laboratory language, Asterisk software telephone exchange, Eltex equipment, Linux operating system, virtual machine.*

АНАЛИЗ ОСОБЕННОСТЕЙ ИСПОЛЬЗОВАНИЯ РАЗЛИЧНЫХ ВИДОВ МОДУЛЯЦИИ В ГИДРОАКУСТИЧЕСКОМ КАНАЛЕ

Куприков Олег Дмитриевич,
магистрант МТУСИ, Москва, Россия,
Kod808@yandex.ru

Шаврин Сергей Сергеевич,
профессор кафедры МТС, д.т.н., МТУСИ, Москва, Россия,
sss@mtuci.ru

Аннотация
Рассматривается проблема передачи информации в водной среде по гидроакустическому каналу. Приводится сравнение и анализ передачи данных в воздушной и водной среде с учётом их особенностей. Основная цель работы – выбор наилучшего метода модуляции сигналов для гидроакустического канала.

Ключевые слова: *гидроакустика, гидроакустический канал связи, подводная связь, параметры водной среды, МСИ, межсимвольная интерференция, OFDM, Orthogonal Frequency Division Multiplexing.*

Подводная связь

На сегодняшний день существует множество различных видов передачи информации. Развитие связи началось с проводной связи, а со временем были изобретены радиосвязь, мобильная и спутниковая связь. Кроме того, в наши дни существует и подводная связь, которая также играет огромную роль в технике передачи информации, но при этом не получила должного развития. Данный тип связи позволяет передавать информацию в подводном пространстве океанов, морей и любых водоемов. Существует и давно применяется стационарная подводная связь. Данный вид подводной связи использует адаптированные для подводной среды средства наземной проводной связи. Так, например, подводные кабели должны обладать стойкостью к воздействию воды, щелочей, а также высокого давления. Они имеют дополнительную изоляцию из полиэтилена, майларовой пленки и обладают вспомогательным армированием. Стационарная подводная связь имеет ряд недостатков из числа, которых прежде всего стоит выделить дороговизну оборудования, сложность установки и обслуживания, так как кабели часто могут прокладываться на глубине до 8-ми километров, а также невозможность повсеместного использования в связи с особенностями рельефа дна или глубиной прокладки.

Данные проблемы можно решить посредством применения беспроводной подводной связи. Беспроводная подводная связь также открывает новые возможности для исследования и оперативного мониторинга подводного пространства.

Гидроакустика

Изначально для беспроводной передачи информации применялась радиосвязь, акустика и оптическая связь. Изучая вопрос эффективной передачи информации в водном пространстве, можно сделать вывод, что единственным подходящим способом передачи является использование гидроакустического канала связи. Как известно радиоволны в лсновном не передаются в водной среде за исключением сверхдлинных ($\lambda > 10км$) волн, которые характеризуются очень низкой скоростью передачи информации. Оптические волны хорошо передаются в водной среде, но обладают сильной зависимостью возможности передачи от состояния среды, так как при помутнении воды передача оптического сигнала становится невозможной. Наиболее приемлемым способом приёма-передачи звуковых волн в водной среде является гидроакустический способ, так как звук может распространяться в жидкости на значимое расстояние. Это связано с тем, что акустические волны передаются путем распространения механических возмущений, которые возможны благодаря наличию упругих связей между частицами среды.

Один из возможных вариантов схемы совместного использования радиосвязи в комбинации с гидроакустическим каналом для подводной связи представлен на рисунке 1.

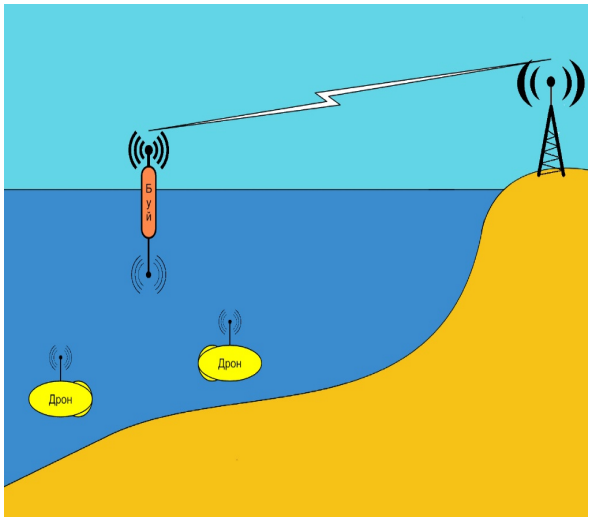


Рис. 1. Связь неподвижного буя с подводными дронами по гидроакустическому каналу

Проблемы гидроакустического канала связи

Основная задача исследования возможности построения системы подводной связи заключается в поиске подходящего метода модуляции для гидроакустического канала, так как он обладает специфичными характеристиками, отличающимися от типовых характеристик радиоканалов. В связи с этим, в первую очередь, необходимо исследовать основные параметры среды распространения, а именно водной среды [2]. .

Основным параметром среды является скорость распространения сигнала, и в случае использования гидроакустического канала – скорость распространения звука в жидкостях:

$$\upsilon = \sqrt{\frac{K}{\rho}}\, м/с, \tag{1}$$

где: υ – скорость звука, K – модуль всестороннего сжатия (коэффициент пропорциональности между напряжением и изменением объема), ρ – плотность среды.

Данный параметр не постоянен, так как значения модуля всестороннего сжатия и плотности могут изменяться в зависимости от температуры и давления водной среды. Среднее значение скорости звука в воде составляет примерно 1500 м/с, что является очень низким показателем в сравнении со скоростью распространения радиоволн в воздушной среде ($3 \cdot 10^8\ м/с$).

Следующий рассматриваемый параметр – задержка сигнала во времени. Задержка сигнала во времени возникает из-за конечной скорости распространения гидроакустических волн, которая в свою очередь, как было показано, зависит от параметров среды. Таким образом, задержка сигнала в водной среде составляет приблизительно 67 мс на 100 м расстояния в соответствии с выражением:

$$T = \frac{S}{\upsilon} мс, \tag{2}$$

где: T – задержка сигнала, S – расстояние от передатчика до приемника (100 м), υ – скорость распространения ($\approx 1500 м/с$).

Следует отметить, что данное значение справедливо только для прямых лучей, а для отраженных от дна и поверхности лучей задержка будет еще больше.

Также необходимо учитывать такой параметр, как затухание сигнала, который характеризует снижение амплитуды сигнала на выходе канала связи. Для наиболее точного расчета затухания для гидроакустического канала необходимо учитывать такие параметры, как соленость, температура, глубина и водородный показатель. Все эти параметры учитываются в формуле Франсуа-Гаррисона:

$$a(f) = \frac{A_1 P_1 f_1 f^2}{f_1^2 f^2} + \frac{A_2 P_2 f_2 f^2}{f_2^2 f^2} + A_3 P_3 f\ дБ/км, \tag{3}$$

где: $a(f)$ – затухание сигнала, A – коэффициент, зависящий от водородного показателя, P – коэффициент, зависящий от глубины, f – центральная частота канала, f_1, f_2 – частоты релаксации.

Так, в условиях Черного моря (водородный показатель 8, средняя температура воды 10°С, соленость 17‰) при использовании центральной частоты 56 кГц значение затухания будет соответствовать величине 9,47дБ/км [1].

Четвертый параметр среды – это шумы в канале связи. Для сигнала в среднем частотном диапазоне, передаваемого по гидроакустическому каналу связи, наибольшее влияние оказывают шумы, возникающие вследствие движения поверхности воды под воздействием ветра.

Кроме этого в гидроакустическом канале связи учитываются: перемещение приемника и передатчика в водной среде друг относительно друга и многолучевое распространение волн вследствие наличия множества лучей от передатчика до приемника из-за их отражения от дна, поверхности воды и водных объектов [5].

Межсимвольная интерференция

Определившись с методом передачи сигналов в водной среде и исследовав проблемы, присущие данному методу, необходимо решить задачу выбора метода модуляции сигнала для эффективной передачи по гидроакустическому каналу.

При приеме сигнала, наибольшее воздействие на искажение сигнала оказывает межсимвольная интерференция, возникающая за счет откликов на более ранние символы. Существует два типа межсимвольной интерференции.

Первый тип возникает вследствие спектрального состава передаваемого сигнала и борьба с ним производится простым способом, а именно с помощью добавления фильтра из «приподнятого косинуса», который в результате изменит форму импульса. Второй тип возникает из-за многолучевого распространения волн в водной среде (рис. 2). Данный тип межсимвольной интерференции нельзя нейтрализовать привычными методами в связи с невозможностью заранее предсказать результат интерференции при многолучевом распространении волн, вследствие которого в среде возникает бесчисленное множество её вариантов.

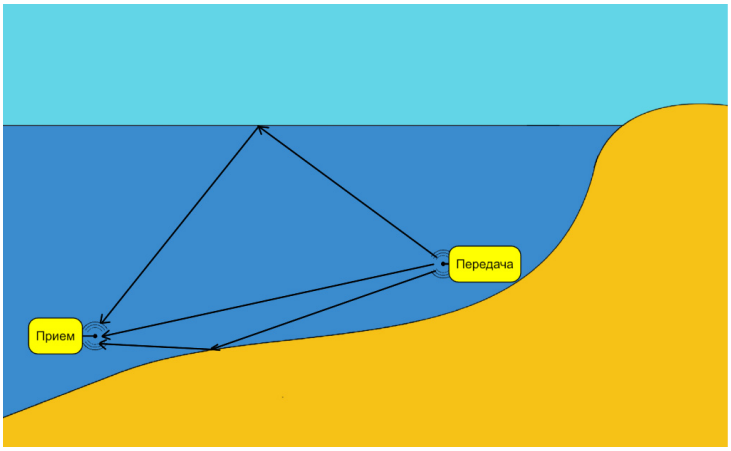


Рис. 2. Многолучевое распространение волн в водной среде

На рисунке 3 изображен принцип воздействия межсимвольной интерференции (МСИ) на передаваемые данные в приемной части.

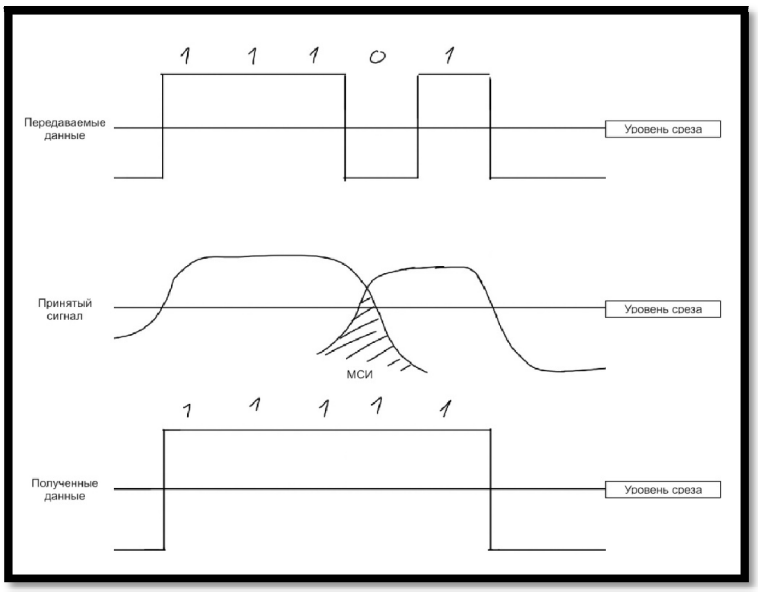


Рис. 3. Воздействие МСИ на передаваемый сигнал

Мультиплексирование с ортогонально-частотным разделением каналов

В связи с тем, что межсимвольная интерференция оказывает наибольшее воздействие на передаваемый сигнал, основной задачей является её подавление. Наиболее эффективным способом борьбы с межсимвольной интерференцией, возникающей вследствие многолучевого распространения волн, явилось применение многочастотной модуляции, а именно OFDM.

OFDM (Orthogonal frequency-division multiplexing) – мультиплексирование с ортогонально-частотным разделением каналов представляет собой вид модуляции, использующий обратное преобразование Фурье для формирования OFDM сигнала. Основной особенностью данного метода является передача информации одновременно на множестве поднесущих на разных частотах. На рисунке 4 представлен итоговый сигнал (3) образованный путем сложения множества поднесущих в частотной области (1) [3,4].

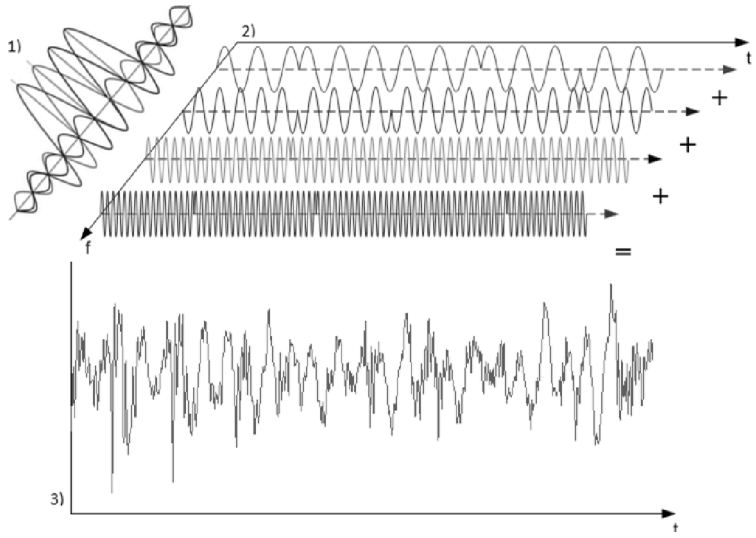


Рис. 4. Формирование OFDM сигнала

С помощью модуляции OFDM можно решить основную проблему передачи информации по гидроакустическому каналу - воздействие межсимвольной интерференции на передаваемый сигнал. В данном случае, из-за наличия множества поднесущих информация передается параллельно на разных частотах. В результате, длительность каждого символа увеличивается пропорционально количеству этих поднесущих [4]. Благодаря увеличению длительности каждого символа OFDM снижается влияние межсимвольной интерференции на передаваемый сигнал. На рисунке 5 представлены поступающие на приемник символы с модуляцией на одной несущей. В данном случае межсимвольная интерференция охватывает три символа.

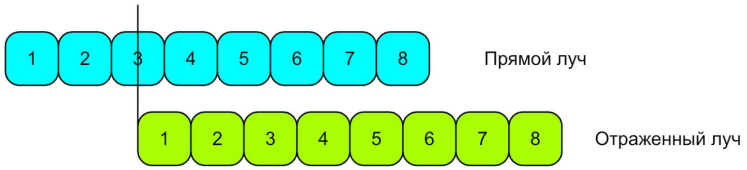


Рис. 5. Влияние МСИ со стандартной модуляцией

На рисунке 6 также представлены поступающие на приемник символы, но уже с модуляцией на множестве поднесущих. В данном случае межсимвольная интерференция охватывает только 30% одного символа.

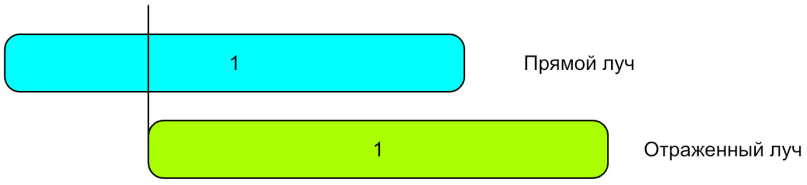


Рис. 6. Влияние МСИ с OFDM модуляцией

При использовании модуляции OFDM уровень влияния межсимвольной интерференции будет зависеть от числа поднесущих. Так как увеличивается число поднесущих, увеличивается и длительность каждого символа и снижается скорость передачи, но в случае с использованием гидроакустического канала с относительно низкой скоростью распространения волны данный недостаток не оказывает существенного влияния.

OFDM модулятор

Упрощенная схема модулятора OFDM представленная на рисунке 7.

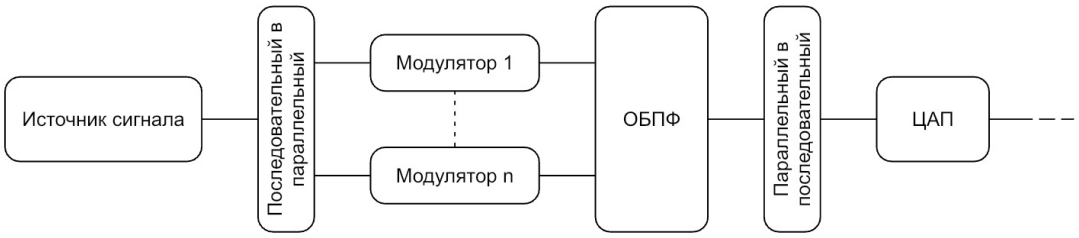


Рис. 7. Упрощенная схема OFDM модулятора

Метод OFDM использует одновременно и модуляцию, и мультиплексирование составных частей одного сигнала [3]. Так, сначала, последовательный код, приходящий от источника сигнала преобразуется в параллельный. Образовавшиеся группы бит определяют амплитуду и фазу каждой поднесущей, после чего для поднесущих выбирается отдельный тип модуляции в зависимости от условий и поставленной задачи. На начальном этапе была выбрана модуляция QPSK в качестве модуляции поднесущих, так как она позволяет сузить спектр сигнала в два раза. Далее, каждая параллельная линия поступает на блок ОБПФ (Обратного Быстрого Преобразования Фурье) с n входами и n выходами, чтобы из значений поднесущих в частотной области получить значения во временной области. После этого полученные поднесущие объединяются в сложный сигнал OFDM, который проходит стандартное цифро-налоговое преобразование в блоке ЦАП для передачи по гидроакустическому каналу связи.

Заключение

Использование гидроакустического канала связи оказалось наиболее подходящем методом беспроводной подводной связи, так как радиоволны не передаются в водной среде за исключением сверхдлинных волн, а оптические волны не передаются в мутной воде.

Наиболее подходящим видом модуляции сигнала для передачи информации по гидроакустическому каналу связи является OFDM. Благодаря модуляции на множестве поднесущих метод OFDM удовлетворяет требованиям по обработке сигнала, позволяя нейтрализовать эффект межсимвольной интерференции. В тоже время недостатком метода OFDM является чувствительность к эффекту Доплера, воздействие которого может приводить уже к межканальной интерференции, также влияющей передаваемый сигнал. С учётом этого внедрение данного вида модуляции для передачи информации по гидроакустическому каналу связи потребует дополнительного исследования.

Литература

1. *Душин С. В., Алешин В. С., Шаврин С. С., Фархадов М. П., Куров И. Ю.*«Использование среднего частотного диапазона акустических волн для передачи информации в поверхностных водах // Вестник Томского государственного университета 2021. №54. С. 38-47.
2. *Кудрявцев В. И.* Гидроакустика рыбохозяйственная. М.: Изд-во ВНИРО, 2018. 460 с.
3. *Феер К.* Беспроводная цифровая связь. Методы модуляции и расширения спектра. Пер. с англ. /Под ред. В. И. Журавлева. М.: Радио и связь, 2000. 520 с.
4. *Лайонс Р.* Цифровая обработка сигналов. Пер. с англ. М.: ООО «Бином-Пресс», 2006. 656 с.
5. *Душин С. В., Фархадов М.П., Шаврин С. С., Алешин В. С.* Тенденции и перспективы развития беспроводной подводной связи // DSPA: Вопросы применения цифровой обработки сигналов, 2020. №2. С. 11-18.

ANALYSIS OF THE FEATURES OF USING DIFFERENT TYPES OF MODULATION IN A HYDROACOUSTIC CHANNEL

Oleg D. Kuprikov,
Graduate MTUCI, Moscow, Russia,
Kod808@yandex.ru

Shavrin S. Sergeevich,
Professor of the Department of MTS, Doctor of Technical Sciences, MTUCI, Moscow, Russia,
sss@mtuci.ru

Abstract

The problem of information transmission in an aquatic environment through a hydroacoustic channel is considered. Comparison and analysis of data transmission in air and water environment and consideration of their features are given. The main goal is to select the best signal modulation method for the hydroacoustic channel.

Keywords: *hydroacoustics, hydroacoustic communication channel, underwater communication, parameters of the aquatic environment, ISI, intersymbol interference, OFDM, Orthogonal Frequency Division Multiplexing.*

ПРОБЛЕМЫ НАСТРОЙКИ И АДМИНИСТРИРОВАНИЯ МАРШРУТИЗАТОРОВ CISCO СЕРИИ ASR

Базаев Антон Евгеньевич,
студент МТУСИ, Москва, Россия,
anton.bazaev@mail.ru

Докучаев Владимир Анатольевич,
заведующий кафедрой СИТиС, д.т.н., профессор, МТУСИ, Москва, Россия,
v.a.dokuchaev@mtuci.ru

Аннотация

Корпоративные сети на базе маршрутизаторов CISCO широко используются в центрах обработки данных и в некорпоративных информационно-телекоммуникационных сетях крупных компаниях. Эти маршрутизаторы стабильны, имеют долгий срок службы и оснащены мощными и качественными внутренними составляющими. Однако из-за проблем в настройке, унификации и администрировании этих маршрутизаторов часть компаний и ЦОД переходят к использованию оборудования конкурентов. С целью сохранения конкурентных преимуществ оборудования CISCO необходимо рассмотреть особенности настройки оборудования и предложить рекомендации по их оптимизации.

Ключевые слова: *оборудование Cisco, маршрутизатор ASR серии 1000, маршрутизатор ASR серии 9000, протокол NAT, прошивка маршрутизатора, протоколы маршрутизации, уязвимости.*

Введение

В последнее время активно развиваются сетевые технологии *SDN – Software Defined Networking*, так же известная как программно–определяемая сеть. В данной сети, уровень управления которой отделён от устройств передачи данных и реализован программно, происходит виртуализации вычислительных ресурсов. Хотя данная технология позволяет частично отказаться от сетевого оборудования, но всё же ключевой частью сети является маршрутизатор, обладающий высокой вычислительной мощностью. Маршрутизатор является сетевым устройством, принимающим решения о пересылке пакетов сетевого уровня между различными сегментами сети на основании информации о топологии сети и определённых правил. Основная функция маршрутизаторов состоит в маршрутизации трафика сети. Как оборудование L3 маршрутизатор функционирует на сетевом уровне и служит для организации связи между сетями. Помимо этого, маршрутизатор необходим для обеспечения защиты информации и контроля за путями передачи, а также для связи сетей с несовместимой архитектурой, объединения локальных сетей и предоставления доступа в интернет.

В сетевых технологиях ЦОДа на май 2020 в лидерах, по мнению аналитической компании *Gartner,* находятся три производителя сетевого оборудования. Это международныи компании *Cisco, Arista Networks* и *Juniper Networks*, которые благодаря своим сетевым технологиям являются лидерами по продажам оборудования на международном рынке (рис. 1).

Среди российских производителей оборудования для гражданского назначения выделяются такие компании как *Zelax, НАТЕКС, Eltex, Qtech*. Они разрабатывают и производят отечественное сетевое оборудование, в состав которого так же входят и маршрутизаторы [4,5] .

В сентябре 2020 года *TAdviser* составил рэнкинг офисов иностранных ИТ-компаний в России на основе объема их выручки. Cisco заняла 10 строчку списка всех иностранных ИТ компаний, увеличив в 2019 году свою выручку до 33,4 миллионов рублей. Стоит отметить, что в данном списке учитывается выручка по продажам всего оборудования. Так на первом месте стоит компания *Samsung Electronics.*

Одной из самых популярных компаний на российском рынке по продаже маршрутизаторов остаётся *Cisco*. С 2018 года их бизнес в России вновь начал расти после спада популярности. Большинство компаний доверяют их оборудованию, но в России постепенно происходит замена оборудования *Cisco* на оборудование конкурентов.

Рис. 1. Лидеры сетевых технологий ЦОДа на май 2020

На рисунке 2 представлена гистограмма выручки *Cisco* в России.

Рис. 2. Гистограмма выручки *Cisco* в России

Настройка оборудования *Cisco* и возможные проблемы

Рассмотрим настройку маршрутизатора *Cisco ASR* серии 1000 в филиале корпоративной сети. Данная сеть типична для современных российских компаний и в ней есть основной офис с территориально удаленными от него филиалами. Вся связь и информация проходят через головной офис. Подключенный маршрутизатор в филиале должен выполнять минимальные функции, а именно иметь связь с главным офисом, обеспечивать филиал доступом в Интернет и быть ядром локальной сети. Получив от провайдера доступ в Интернет, необходимо настроить *NAT*, поднять сервер *DHCP* и настроить туннель до центрального офиса [1-3].

Приобретя маршрутизатор *Cisco*, администратор уже сталкивается с первой проблемой. В комплекте отсутствует провод для подключения к консоли через *COM* порт или *com-to-usb*. От провайдера идёт оптоволокно, поэтому необходимо закупить оптический трансивер. Если взять трансивер другой фирмы, даже если он заработает, маршрутизатор будет специально подавлять скорость с 40 Гбайт/с до 1 Гбайт/с , так как устройство будет не сертифицировано. Данное оборудование у конкурентов имеет схожие характеристики и качество, но ниже по цене в несколько раз и не имеет данных проблем.

Подключившись к провайдеру, следующим шагом необходимо наладить связь с главным офисом. При использовании стека протоколов *IPsec* отсутствуют проблемы в настройке туннеля, так как *Cisco* создал удобную

настройку *VPN* через стек протоколов при условии нахождения маршрутизаторов на обоих концах тоннеля. Это не только удобно в настройке, но и обеспечивает высокую степень защиты, так как используются разработанные *Cisco* протоколы шифрования. Так же, используя маршрутизаторы *Cisco* на обоих концах туннеля, пропускной способности канала хватит для поддержания любого обмена информации между филиалом и центральным офисом.

Подключив сервер *DHCP*, возможно, разделив пользователей на несколько *VLAN,* получить рабочую локальную сеть. У маршрутизаторов *Cisco ASR* серии 1000 есть много проблем с технологией *NAT*. Так, самая обычная команда "*clearing ip nat translations*" приводит к тому, что «падает» какой-то из сервисов в зависимости от настройки, если запросить состояние *NAT* командой "*show ip nat translations*". На официальном сайте *Cisco* в *Bug Search Tool* стоит рекомендация: «*Wait for 20 sec after clear is issued, then issue show ip nat translations*». Официальный ответ *Cisco* на решение данной проблемы – это не запрашивать "*show ip nat translations*" в течение 20 секунд после очистки.

Зачастую происходит засорение памяти при работе с *NAT*, из-за чего необходимо раз в месяц перезагружать оборудование для освобождения памяти. Данная проблема имеет место только на отдельных прошивках. При смене прошивки эта проблема может уйти, но возможна неправильная работа *ALG* в режиме *NAT overload,* или что-то иное. При этом, неизвестно какие ещё проблемы могут возникнуть при смене прошивки.

В режиме *NAT* overload *PPTP* работает не корректно: периодически управляющая *TCP* сессия транслируется на порт в белый адрес, а *GRE* туннель в другой *IP* адрес. Белые адреса периодически сканируются из внешней сети на предмет уязвимости, вследствие чего на любой белый адрес поступает пакет, остающийся в пуле, так как тайм аут больше, чем периодичность поступающих пакетов. Трансляции не закрываются и белые адреса не освобождаются. Когда пул белых адресов исчерпывается, новые сессии *PPTP* перестают работать. При работе с прошивкой 3.13.4 включение или отключение *PPTP ALG* не помогает. Если перейти на прошивку 3.10.5 проблема снимается. Для очистки всех не использующиеся белых адресов можно периодически полностью очищать пул, при этом все абоненты отключатся, либо необходимо перезагружать сам маршрутизатор, что приведет к тому же результату.

Проблемы с переполнением пула или памяти невозможно предвидеть, так как на разных прошивках оборудование ведет себя по-разному. Чтобы произошло переполнение, необходима бесперебойная работа в реальной сети на протяжении нескольких недель. Это замедляет настройку оборудования.

При переходе протоколов в разные режимы работы, они могут работать не корректно. Совмещение предшествующего и текущего режимов работы может привести к сбою, при котором предугадать поведение маршрутизатора невозможно. Поэтому, сразу после изменения режима следует перезагрузить оборудование с сохранением конфигурации. При настройке дефолтного *NAT*, если в настройке *access-list* прописывать *IP* а потом адрес, *NAT* будет работать не корректно – внутри сети фиксируется незапрашиваемый трафик из Интернета. Для решения данной проблемы, необходимо вместо *IP* дублировать добавление в *access-list* нужные протоколы с одинаковым адресом вместо *permit ip 10.1.0.0 0.0.255.255 any* нужно прописать:

permit tcp 10.1.0.0 0.0.255.255 any
permit udp 10.1.0.0 0.0.255.255 any
permit icmp 10.1.0.0 0.0.255.255 any

При выполнении данной команды пакеты не будут посылаться на не включённые протоколы. При выборе *IP* будет происходить засорение трафика из-за спама на выключенные протоколы. Данная проблема присутствует на различных версиях прошивок в разных моделях серии *ASR* 1000.

При настройке *NAT* на оборудовании *Cisco* на большинстве прошивок существуют ошибки в разных функциях данного протокола, либо при взаимодействии с другими протоколами [1,2].

У более новых маршрутизаторов *Cisco ASR* серии 9000 так же имеются свои проблемы. Правда, даже самые большие из них имеют пути решения, даже если они не исправлены в новой прошивке. Так, в протоколе связующего дерева (*STP*) существует проблема при использовании нескольких разновидностей *STP*: порты коммутатора спонтанно переключаются между блокированием и пересылкой.

Рассмотрим топологию соединения изображенного на рисунке 3.

Рис. 3. Топология

Предположим, что используется *MST* на коммутаторе 1 и на интерфейсе router, который приводит к коммутатору 1, но при этом используется *PVST* + на коммутаторе 2. *PVST* + *BPDU* проходят через домен моста и доходят до коммутатора 1. Затем коммутатор 1 распознает как пакеты *BPDU MST* от *router*, так и *PVST* + *BPDU* от коммутатора 2, и это приводит к тому, что связующее дерево на порту коммутатора 1 постоянно переключается с блокирования на не блокирование, что, в свою очередь, приводит к потере трафика.

Предлагается три варианта решения этой проблемы:

1. Настроить *MST* на коммутаторе 2 и включить *MST* на интерфейсах роутера к коммутаторам 1 и 2.
2. Использовать список доступа сервисов *Ethernet* на роутере для отбрасывания *PVST + BPDU* либо во входящем потоке от коммутатора 2, либо в исходящем потоке к коммутатору 1.
3. Запустить шлюз доступа к связующему дереву *VLAN (PVSTAG)* на интерфейсе *router* в направлении к коммутатору 2, что заставит router использовать *PVST + BPDU* от коммутатора 2.

Так же ПО *Cisco* не идеально: так в банке данных угроз безопасности информации ФСТЭК существует длинный список выявленных уязвимостей, от минимальной до максимальной опасности по шкале *CVSS*. Для решения проблем с данным типом угроз ФСТЭК ссылается на официальный сайт *Cisco*.

У маршрутизаторов *ASR* серии 9000 была уязвимость с идентификатором *CVE-2019-1710*, она набрала 9,8 баллов по шкале *CVSS* из 10 возможных. Данная уязвимость связана с неправильной изоляцией вторичного интерфейса управления от внутренних приложений системного администратора. Злоумышленник может воспользоваться этой уязвимостью, подключившись к одному из прослушивающих внутренних приложений. Успешный эксплойт может привести к нестабильным условиям работы, включая как отказ в обслуживании, так и удаленный не аутентифицированный доступ к устройству. В течение двух дней после обнаружения данной уязвимости *Cisco* выпустила обновления программного обеспечения, которые устраняют эту уязвимость. Так же на своем официальном сайте *tools.cisco.com* было выпущено описание уязвимости, способ её обнаружения и устранения [2,4] .

Из числа более новых существует уязвимость *BDU:2020-04605*: уязвимость в программном обеспечении *Cisco IOS XE ROM Monitor (ROMMON)* для маршрутизаторов интегрированных служб *Cisco* серии 4000; маршрутизаторов агрегационных служб *Cisco ASR* серии 920; маршрутизаторов агрегационных служб *Cisco ASR* серии 1000 и конвергентных широкополосных маршрутизаторов *Cisco cBR-8*. Эта уязвимость может позволить не аутентифицированному физическому злоумышленнику разорвать цепочку доверия и загрузить скомпрометированный образ программного обеспечения на пораженное устройство. Уязвимость связана с наличием опции конфигурации отладки в уязвимом программном обеспечении. Злоумышленник может воспользоваться этой уязвимостью, подключившись к уязвимому устройству через консоль, принудительно переведя устройство в режим *ROMMON* и написав вредоносный шаблон с использованием этой конкретной опции на устройстве. Успешный эксплойт может позволить злоумышленнику разорвать цепочку доверия и загрузить скомпрометированный образ программного обеспечения на пораженное устройство. Скомпрометированный образ программного обеспечения — это любой образ программного обеспечения, который не был подписан цифровой подписью *Cisco*. *Cisco* выпустила обновления программного обеспечения, которые устраняют эту уязвимость. Обходных путей, устраняющих эту уязвимость, не существует.

В марте текущего года была выявлена уязвимость с *CVSS 5.3 BDU:2021-01246*. Уязвимость в процессе *ipsecmgr* программного обеспечения *Cisco ASR* серии 5000 (*StarOS*) может позволить не аутентифицированному удаленному злоумышленнику вызвать состояние отказа в обслуживании (*DoS*). Эта уязвимость связана с недостаточной проверкой входящих пакетов *Internet Key Exchange* версии 2 (*IKEv2*). Злоумышленник может воспользоваться этой уязвимостью, отправив специально искаженные пакеты *IKEv2* на пораженное устройство. Успешный эксплойт может позволить злоумышленнику вызвать перезапуск процесса *ipsecmgr*, что нарушит текущие переговоры *IKE* и приведет к временному состоянию *DoS*. Cisco выпустила обновления программного обеспечения, которые устраняют эту уязвимость. Обходных путей, устраняющих эту уязвимость, не существует.

При обнаружении всех уязвимостей компания *Cisco* оперативно устраняет проблемы, чтобы злоумышленник не смог получить доступ к оборудованию или вызвать отказ в его работе. Администратору сети необходимо регулярно проверять новости о появлении новых угроз и методах их устранения [2].

Когда системный администратор меняет оборудование на более мощное, либо изменяет прошивку, он не может быть уверен в прежней бесперебойной работе маршрутизатора при точном дублировании всех прежних настроек. При загрузке конфигурации с другой прошивки или использовании другого маршрутизатора оборудование может не загрузиться из-за различий в унификаций конфигурации.

При том, что компания *Cisco* выпускает всё новые прошивки для оборудования, исправляющие баги, одновременно с этим могут проявляться новые ошибки. В связи с этим большинство администраторов тщательно проверяют новое оборудование и запрашивают информацию на форумах, чтобы в случаи использования обновленной прошивки не возникли непредвиденные неисправности. При этом необходимо своевременно обновлять прошивку на устройстве, так как в новых версиях предусмотрено устранение уязвимостей системы.

Компания *Cisco* может перестать обслуживать старые модели и выпускать для них обновление в прошивке. Тем самым при покупке старой модели следует понимать, что её безопасность будет только уменьшаться и баги, которые присутствовали в последней версии прошивки, не будут исправлены.

Когда требуется заменить маршрутизатор C*isco* на новую модель, системный администратор. как правило, стремится скопировать со старого оборудования конфигурацию и загрузить её на новое оборудование, настроив только новые возможности модели следующего поколения. Компания C*isco* такую функцию не предусмотрела. Так, например, имея в распоряжении настроенную модель *ASR* 1001 и закупив *ASR* 1002 необходимо все настройки производить заново. Хотя эти два маршрутизатора из одной серии, но у них нет унифицированной системы конфигурации.

Заключение

Оборудование *Cisco* широко распространено в центрах обработки данных и в некорпоративных информационно-телекоммуникационных сетях крупных компаний. Чтобы переход к новому оборудованию у клиентов происходил быстрее и проще компании *Cisco* стоит задуматься о создании унификационной системе переноса конфигурации, что обеспечит более активные закупки её новых продуктов.

Cisco следует изготавливать более качественные новые прошивки, после выпуска которых не потребуется ждать долгие месяцы для подтверждения их качества и, помимо этого, обеспечить поддержку своей старой продукции, безопасность которой снижается со временем.

В комплекте поставок оборудования не предусмотрен консольный порт и некоторые модули. С учётом заявок заказчиков *Cisco* могла бы при закупки оборудования включать требуемые узлы в итоговую комплектацию и поставлять их уже встроенными в оборудование.

Литература

1. «Руководство по установке аппаратного обеспечения маршрутизаторов Cisco ASR 9001 и Cisco ASR 9001-S». Штаб-квартира в США Cisco Systems: 2014, 184 с.
2. *Бен Пайпер [Ben Piper]* Администрирование сетей CISCO: освоение за месяц. Санкт-Петербург: ДМК-Пресс, 2018.
3. *Алан Леинванд [Leinwand Allan]* «Конфигурирование маршрутизаторов Cisco», 2-е изд. Москва: Вильяме, 2015.
4. Поиск багов [Элекстронный ресурс]. Режим доступа: https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvn49911.
5. *Золотухин М.С.* Межсетевая операционная система для оборудования cisco // современные научные исследования и инновации. 2020, вып 5 (109). С. 6.

CONFIGURATION AND ADMINISTRATION PROBLEMS OF CISCO ASR SERIES ROUTERS

Anton E. Bazaev,
Student MTUCI, Moscow, Russia,
anton.bazaev@mail.ru

Anatolyevich D. Vladimir,
Head Department of CITiS, Doctor of Technical Sciences, Professor, MTUCI, Moscow, Russia,
v.a.dokuchaev@mtuci.ru

Abstract

Corporate networks based on CISCO routers are widely used in data centers and non-corporate information and telecommunication networks of large companies. These routers are stable, have a long lifespan and are equipped with powerful and quality internals. However, due to problems in configuring, unifying and administering these routers, some companies and data centers are switching to using competing equipment. In order to maintain the competitive advantages of CISCO equipment, it is necessary to consider the specifics of setting up the equipment and offer recommendations for their optimization.

Keywords: *Cisco, ASR 1000 series router, ASR 9000 series router, NAT protocol, router firmware, routing protocols, vulnerabilities.*

МЕТОД АУТЕНТИФИКАЦИИ В МОБИЛЬНЫХ СЕТЕВЫХ СТРУКТУРАХ ДЛЯ АВИОНИКИ

Щёголев Роберт Андреевич,
студент МТУСИ, Москва, Россия,
vannetis@yandex.ru

Зуйкова Татьяна Николаевна,
старший преподаватель кафедры МТС, МТУСИ, Москва, Россия,
t.n.zuikova@mtuci.ru

Аннотация

Представлен анализ особенностей функционирования мобильных сетевых структур в авионике. Дан обзор функциональных возможностей участников воздушного движения в условиях автоматического зависимого наблюдения в радиовещательном режиме (АЗН-В). Отмечена актуальность вопроса информационной безопасности в сетях с использованием технологии АЗН-В. Предложен метод аутентификации участников воздушного движения в мобильных сетевых структурах с применением криптографического алгоритма RSA. Разработано программное обеспечение микропроцессорного средства аутентификации на базе системы на кристалле 1892ВМ14Я «Мультиком-02» (МСот-02) отечественного производства.

Ключевые слова: *авионика, мобильные сетевые структуры, подвижные самоорганизующиеся сети, безопасность воздушного движения, АЗН-В, автоматическое зависимое наблюдение в радиовещательном режиме, электронная подпись, аутентификация, криптографические средства, информационная безопасность, импортозамещение, система на кристалле, микропроцессор.*

Постановка задачи

В самоорганизующейся сети обмен информацией между пользователями осуществляется по принципу взаимодействия смежных узлов, и доступ к различным сетевым услугам осуществляется посредством передачи и приема трафика через соседние узлы сети. Принцип децентрализованной динамичной структуры позволяет всем сетевым элементам быть равноправными и выполнять функции маршрутизаторов, осуществляя автоконфигурацию, самооптимизацию и самовосстановление подвижной сети. С учетом этих особенностей, топология самоорганизующейся сети изменяется во времени случайным образом, что накладывает особые требования к обеспечению доверия и безопасности информационного обмена между пользователями сети [1].

Принцип функционирования самоорганизующейся сети широко используется в мобильных сетевых структурах в авионике. Управление воздушным движением осуществляется по технологии автоматического зависимого наблюдения в радиовещательном режиме АЗН-В (автоматическое зависимое наблюдение – вещательное) путем передачи на наземные пункты наблюдения информации о географическом местоположении участников воздушного движения [2,7]. Однако следует отметить, что на современном этапе внедрения технологии АЗН-В недостаточно проработаны вопросы информационной безопасности участников воздушного движения, находящихся за пределами прямой видимости наземных пунктов наблюдения [3]. В связи с этим, для авионики актуальна задача обеспечения защиты передаваемой информации от несанкционированного доступа в условиях низкой ситуационной осведомленности в отдаленных и океанических регионах.

Для обеспечения информационной безопасности в условиях функционирования мобильных сетевых структур целесообразно решить следующие задачи:

1. Проанализировать функциональные возможности мобильных сетевых структур в авионике;
2. Оценить проблемы информационной безопасности участников воздушного движения в сетях с использованием технологии АЗН-В;
3. Разработать метод аутентификации участников воздушного движения за пределами прямой видимости наземных пунктов наблюдения АЗН-В;
4. Разработать программное обеспечение микропроцессорного средства аутентификации.

Функциональные возможности мобильных сетевых структур в авионике

В подвижной самоорганизующейся сети в условиях отсутствия базовых и опорных станций каждый узел сети (УС) может являться одновременно приемником, передатчиком и маршрутизатором передаваемой в сети нформации [1]. Для решения задач автоконфигурации, самооптимизации и самовосстановления сети все узлы сети должны выполнять следующие функции:

- соединение с ближайшими узлами сети с целью включения в состав существующей сети или для формирования новой сети;
- прием и передачу трафика внутри сети;
- маршрутизацию трафика.

Маршрут передачи информации определяется динамически, исходя из существующей топологии сети, которая почти всегда случайная. В варианте топологии самоорганизующейся сети, представленной на рисунке 1, видно, как отдельно показанное устройство не может быть частью данной сети из-за ограничения по мощности и значительной удаленности от ближайших элементов сети.

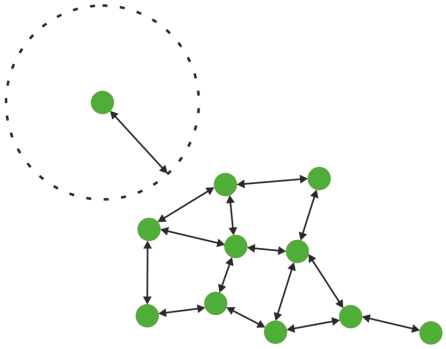


Рис. 1. Топология подвижной самоорганизующейся сети

В мобильных сетевых структурах в авионике сетевыми элементами являются воздушные средства транспорта. При этом данные о местоположении и намерениях воздушных судов передаются в широковещательном режиме наземным пунктам наблюдения в соответствии с технологией АЗН-В [2].

АЗН-В обеспечивает наблюдение за участниками воздушного движения в широковещательном режиме и позволяет осуществлять следующие функции:

1) Связь между участниками воздушного движения;
2) Навигацию. Участники воздушного движения самостоятельно определяют свое местоположение с помощью спутниковых навигационных систем и обмениваются информацией с наземными станциями и другими воздушными судами;
3) Наблюдение за параметрами местоположения, высоты, идентификации и векторов перемещения участников воздушного движения в пространстве.

Благодаря спутникам, участники воздушного движения синхронизируются по мировому стандарту времени UTC (от англ. Universal Coordinated Time) и получают информацию о своем местоположении в режиме реального времени от системы GPS (от англ. Global Positioning System) [4].

При взаимодействии узлов сети по технологии АЗН-В каждый участник воздушного движения перед взлетом проводит широковещательный опрос радиоканалов в течение некоторого времени, определяя свободные для вещания каналы и каналы, занятые другими участниками. Воздушное судно занимает свободный канал и использует его в качестве канала для вещания [3].

Топология мобильной сетевой структуры в авионике с использованием технологии АЗН-В представлена на рисунке 2, где сплошными стрелками обозначены каналы связи между узлами сети для обмена информацией о географическом местоположении и намерениях участников воздушного движения. Зоны прямой видимости наземных пунктов наблюдения обозначены пунктирными линиями.

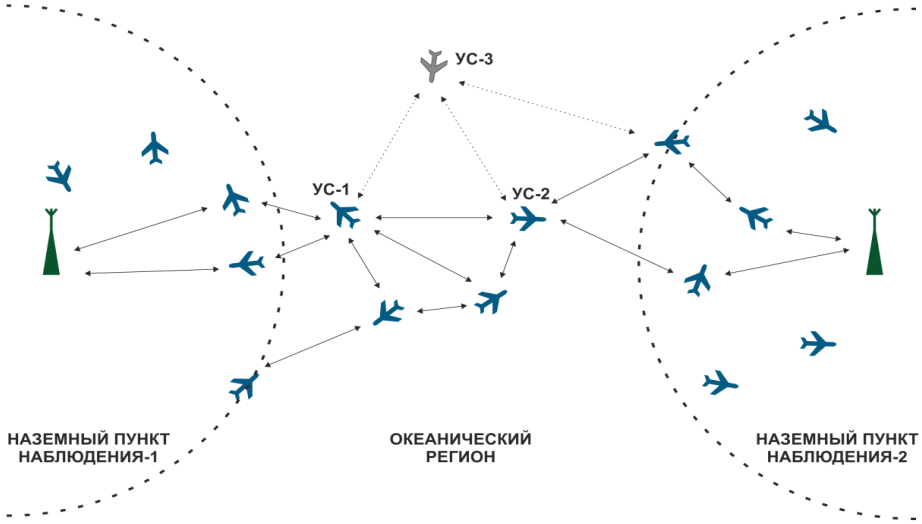


Рис. 2. Топология мобильной сетевой структуры в авионике

В удаленной зоне океанического региона воздушные суда передают информацию о местоположении и намерениях на основе самоорганизующейся сети, решая проблему ситуационной осведомленности об участниках воздушного движения, находящихся за пределами прямой видимости наземных пунктов наблюдения.

Отметим, что сообщения с информацией о местоположении и намерениях участников воздушного движения передаются по открытым каналам в незашифрованном виде, что создает риски информационной безопасности и возможности фальсификации сообщений, а также атаки на основе метода «человек посередине» [3]. Пунктирными стрелками на рисунке 2 показана связь с воздушным судном (УС-3), которое не вызывает доверия и может создать угрозу информационной безопасности. Информация об этом участнике воздушного движения так же передается на наземные пункты наблюдения.

Создание области доверия

Для решения проблемы информационной безопасности особое внимание следует уделить обеспечению доверия участников воздушного движения. Одним из методов защиты информации от несанкционированного доступа является электронная подпись и аутентификация – процедура подтверждения подлинности принимаемого сообщения на основе обеспечения однозначного соответствия идентификатора (открытого ключа) отправителю сообщения [5].

Область доверия, создаваемая на основе инфраструктуры открытых ключей, может стать основой формирования мобильной сетевой структуры, обеспечивающей функциональную надёжность, устойчивость и информационную безопасность системы управления воздушным движением на основе технологии АЗН-В [9]. Каждый открытый ключ уникален и соответствует конкретному узлу сети. Успешная аутентификация участника воздушного движения служит подтверждением того, что полученные информационные данные приняты от доверенного отправителя, владеющего индивидуальным закрытым ключом, а не от злоумышленника.

В мобильной сетевой структуре на базе технологии АЗН-В электронная подпись и аутентификация могут быть реализованы по следующему принципу: содержимое передаваемого пакета делится на две части, «открытую» и «закрытую». Открытая часть пакета представляет собой заголовок пакета сформированный на основе метода самоорганизующегося многостанционного доступа с временным разделением каналов STDMA (Self-Organizing Time Division Multiple Access). Закрытая же часть может содержать информацию о координатах участника воздушного движения, его векторе, высоте и идентификаторе, то есть то, что необходимо скрыть от несанкционированного доступа. При этом микропроцессорное криптографическое средство аутентификации должно проводить проверку подписи именно закрытой части пакета, игнорируя открытую.

Аппаратно-программная реализация криптосистемы, формирующей электронную подпись сообщения и проверяющую эту подпись при аутентификации, позволяет создать область доверия, повысить эффективность системы управления воздушным движением и уровень конфиденциальности участников воздушного движения в отдаленных и океанических регионах в условиях низкой ситуационной осведомленности

Метод аутентификации участников воздушного движения

В качестве метода аутентификации участников воздушного движения в мобильных сетевых структурах в авионике выбран алгоритм *RSA*, основанный на базовой криптографической операции возведения в степень. Для формирования электронной подписи применяется многократное возведение в степень с использованием нескольких закрытых ключей различных участников воздушного движения. При аутентификации алгоритм *RSA* позволяет не соблюдать порядок очередности открытых ключей, что и определяет выбор этого алгоритма в качестве возможного для применения в мобильных сетевых структурах. Процедура аутентификации позволяет участникам воздушного движения (узла сети) точно знать от кого получено сообщение, что исключает факт подмены и фальсификации информации. Следует отметить, что алгоритм *RSA* не обладает высоким уровнем криптостостойкости, которая определяется вычислительной мощностью и временем, затрачиваемых криптоаналитиком на попытки получить несанкционированный доступ к информации [5]. Однако комбинирование этого средства с шифрованием сообщений позволяет существенно повысить уровень конфиденциальности.

На рисунке 3 представлена схема электронной подписи и аутентификации по алгоритму *RSA* в мобильных сетевых структурах в авионике. Отправитель (УС-1) с помощью своего закрытого индивидуального ключа D преобразует зашифрованное сообщение X. Получившееся в результате число Y используется в качестве электронной подписи сообщения X по следующей формуле:

$$Y=X^{D} \bmod N, \quad (1)$$

где X – исходное сообщение (открытое или зашифрованное), для аутентификации которого генерируется электронная подпись; D – закрытый ключ УС-1; N – открытый ключ доверенной сети.

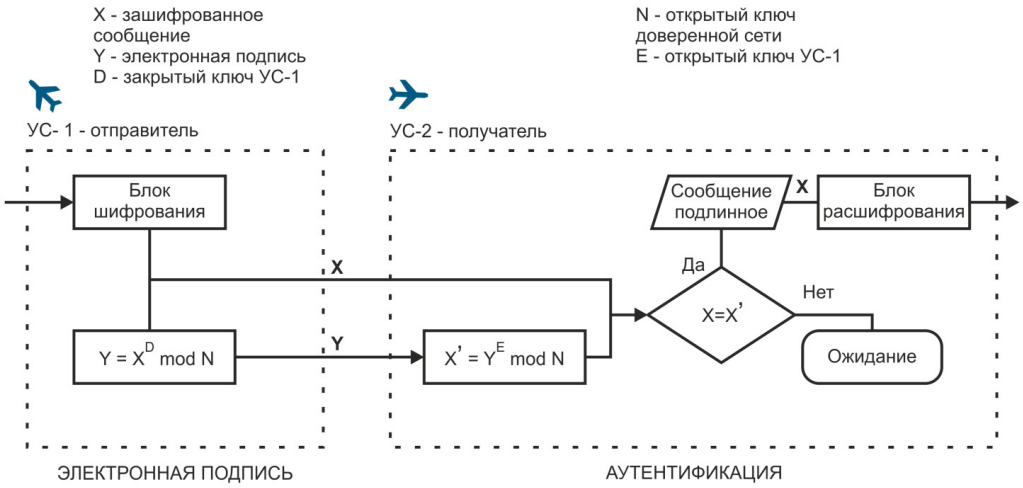


Рис. 3. Схема аутентификации по алгоритму *RSA*

Получатель (УС-2) выполняет аутентификацию электронной подписи по формуле:

$$X' = Y^{E} \bmod N, \tag{2}$$

где E – открытый ключ УС-1;

и проверяет равенство:

$$X = X' \tag{3}$$

Далее делается вывод о том, является ли сообщение подлинным или нет. В случае успешной аутентификации сообщение поступает в блок расшифрования. При отсутствии подтверждения электронной подписи получатель (УС-2) делает вывод о том, что отправитель (УС-1) не является участником доверенной сети и передает соответствующую информацию на наземные станции.

Предположим, что в мобильной сетевой структуре, представленной на рисунке 2, узел сети УС-1 намерен передать сообщение УС-2. В таком случае УС-1 подписывает его с помощью своего закрытого индивидуального ключа, после чего отправляет его УС-2. Узел сети УС-2, приняв сообщение, проводит его аутентификацию с помощью открытого ключа доверенной сети участников воздушного движения.

Преимущество алгоритма аутентификации *RSA* заключается в том, что если УС-1 и УС-2 не хватает мощности радиосигнала для обмена информацией, то они могут использовать в качестве транзитного другой УС, который так же подписывает принятое сообщение и передает дальше, выступая в роли маршрутизатора. УС-2, приняв сообщение, выполняет аутентификацию дважды и получает подтверждение подлинности принятого сообщения. Для реализации электронной подписи и аутентификации без конфиденциальности исходное сообщение X передается в незашифрованном виде.

С целью обеспечения импортозамещения в качестве аппаратного обеспечения криптографического средства аутентификации может быть использована система на кристалле отечественного производства, что экономически целесообразнее и гарантирует отсутствие недокументированных прерываний в процессоре, которые на аппаратном уровне могут приводить к несанкционированному доступу к информации.

В данной разработке использована отечественная система на кристалле (*SoC*) 1892ВМ14Я «Мультиком-02» (*MCom*-02) производства АО НПЦ «Электронные вычислительно-информационные системы» (АО НПЦ «ЭЛВИС») [6].

Для варианта реализации микропроцессорного криптографического средства аутентификации на базе системы на кристалле (SoC) MCom-02 (1892ВМ14Я) отечественного производства разработано программное обеспечение в среде разработке *MC Studio* 4, демонстрационная версия которой в свободном доступе представлена на официальном сайте АО НПЦ «ЭЛВИС» [7].

Блок-схема основной программы аутентификации main по алгоритму RSA представлена на рисунке 4. Она состоит из инициализации, обмена открытыми ключами и вызова двух процедур-функций func_st и func_ multi с целью выполнения аутентификации, после чего выполняется проверка равенства по формуле (3).

Блок-схема процедуры функции func_st представлена на рисунке 5. В ней выполняется сканировании битов показателя степени с целью определения положения старшего значещего разряда.

Блок-схема процедуры функции func_multi представлена на рисунке 6. В ней выполняется базовая криптографическая операция быстрого возведения в степень в простых полях Галуа.

С целью повышения уровня конфиденциальности в доверенной сети участников воздушного движения рекомендуется использовать математический аппарат расширенных полей Галуа, что исключит переполнение разрядной сетки процессора, а также реализовать алгоритм RSA на базе эллиптических кривых, способных обеспечить высокий уровень криптостойкости.

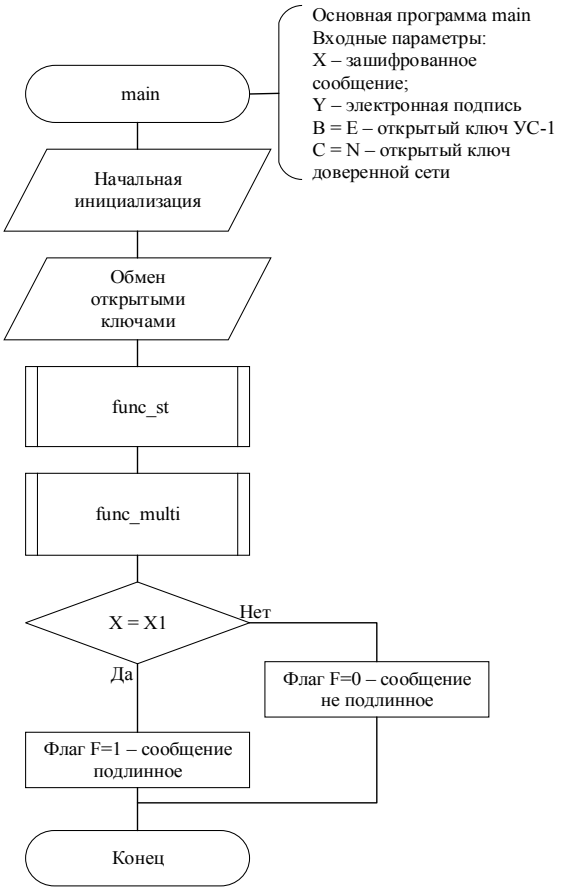


Рис. 4. Блок-схема основной программы аутентификации по алгоритму *RSA*

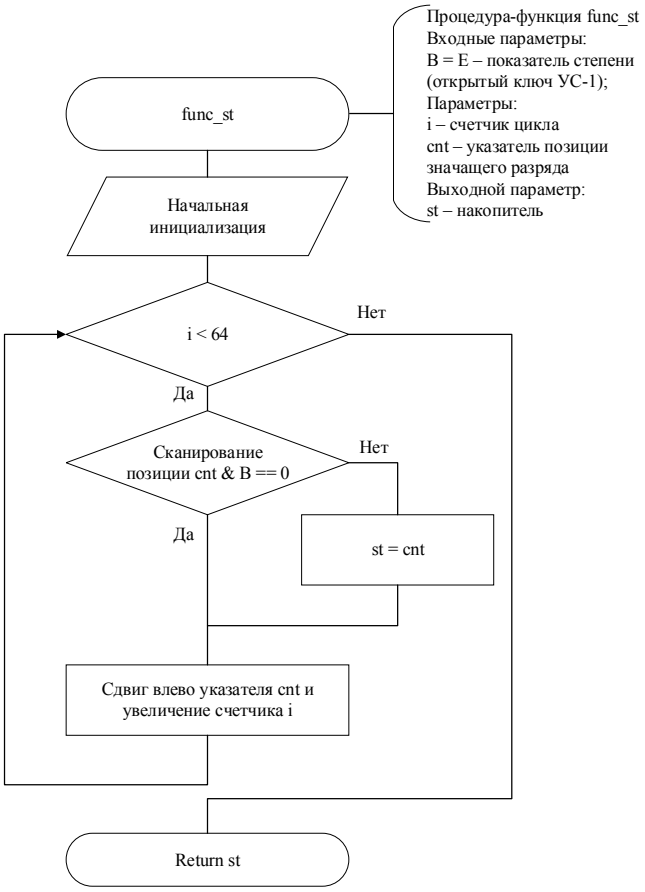


Рис. 5. Блок-схема процедуры-функции определения старшего значащего разряда показателя степени

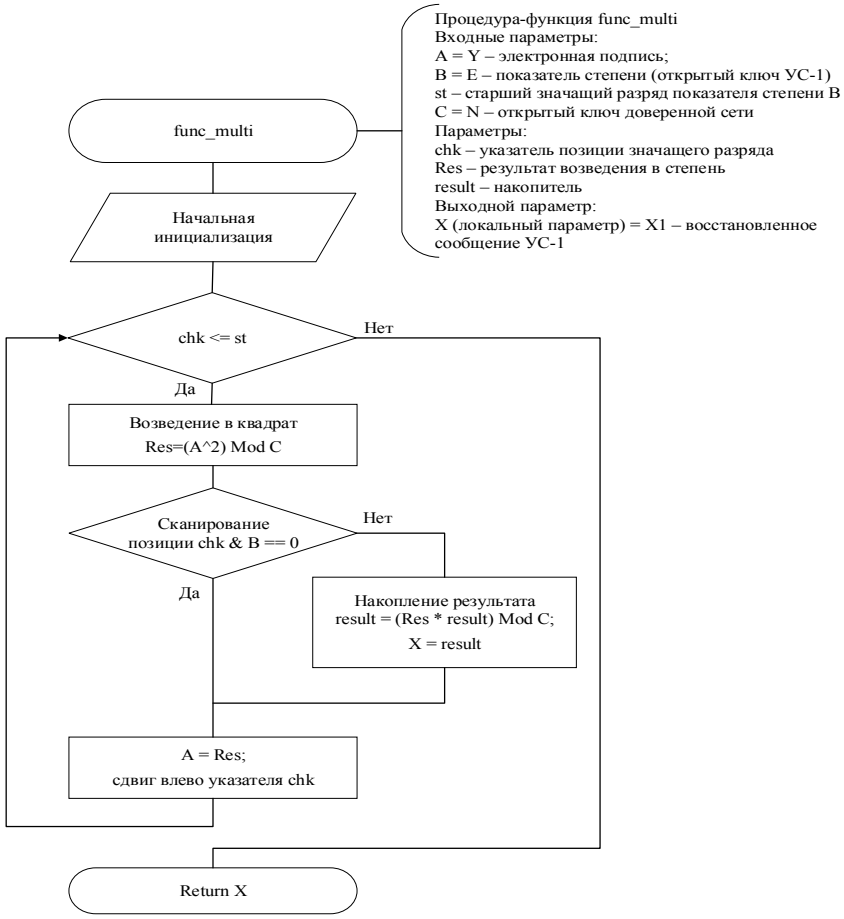


Рис. 6. Блок-схема процедуры-функции быстрого возведения в степень в простых полях Галуа

Заключение

Для решения проблемы информационной безопасности в мобильных сетевых структурах в авионике особое внимание следует уделять обеспечению доверия как неотъемлемой составной части функционирования системы управления воздушным движением по технологии АЗН-В.

Область доверия, создаваемая на основе инфраструктуры открытых ключей, обеспечивает функциональную надёжность, устойчивость и информационную безопасность системы управления воздушным движением за пределами прямой видимости наземных пунктов наблюдения. Каждый УС перед началом обмена трафиком должен выполнить аутентификацию. Успешная аутентификация служит подтверждением того, что полученные информационные данные приняты от доверенного отправителя, владеющего индивидуальным закрытым ключом.

Реализация программно-аппаратного обеспечения криптографического средства аутентификации является важным шагом для создания доверенной сети между участниками воздушного движения в условиях низкой ситуационной осведомленности, тем самым исключая, возможность подмены и фальсификации сообщений.

Предложенный метод аутентификации на базе алгоритма *RSA* позволяет нарушать порядок очередности открытых ключей, что и определило выбор этого алгоритма в качестве возможного для применения в мобильных сетевых структурах. Для обеспечения импортозамещения электронных компонентов в качестве аппаратного обеспечения криптографического средства аутентификации может быть использована система на кристалле 1892ВМ14Я отечественного производителя АО НПЦ «ЭЛВИС».

Литература

1. Что такое *MANET* или почему *WiFi* не решение всех телекоммуникационных проблем [Электронный ресурс]. Режим доступа: https://habr.com/ru/post/197860/ (дата обращения: 09.10.2021).
2. Программа «Внедрение средств вещательного автоматического зависимого наблюдения (2011 – 2020 годы)» : утв. Минтрансом РФ 19 мая 2011 г. // Совместное заседание секций НТС Минтранса. 2010. Протокол № ВО-57 от 10.11.2010.
3. *Кулаков М.С.* Разработка принципов организации мобильных сетевых структур в авионике [Электронный ресурс] : дис. … канд. техн. наук. : 05.12.13 : защищена 22.03.2018 / Кулаков Михаил Сергеевич – Режим доступа: dis-Kulakov.pdf (srd-mtuci.ru) (дата обращения: 09.10.2021).
4. *Рубцов Е.А., Калинцев А.С., Григорьева Е.И.* Анализ линии передачи данных автоматического зависимого наблюдения вещательного типа // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. №6.
5. *Шаврин С.С.* Защита информации в многоканальных телекоммуникационных системах. Часть 1 / Учебное пособие. «Защищенные системы связи». М.: МТУСИ, 2002. 62 с.
6. *Щёголев Р.А., Зуйкова Т.Н.* Анализ функциональных возможностей 1892ВМ14Я с целью применения в инфокоммуникационных приложениях // Телекоммуникации и информационные технологии. 2020. № 2. С. 80-85.
7. *Григорьев И.Д., Орлов В.Г.* Особенности метода доступа к среде в VDL MODE 4 // В сборнике: Технологии информационного общества. XI Международная отраслевая научно-техническая конференция: сборник трудов: Москва. 2017. С. 455.
8. Официальный сайт акционерного общества «Научно-производственный центр «Электронные вычислительно-информационные системы». – Режим доступа: https://multicore.ru/support (дата обращения: 09.10.2021).
9. *Григорьев И.Д., Орлов В.Г.* Исследование вопросов безопасности системы АЗН-В // Телекоммуникации и информационные технологии. 2016. Т. 3. № 2. С. 53-55.

METHOD OF AUTHENTICATION IN MOBILE NETWORK STRUCTURES FOR AVIONICS

Robert A. Shchegolev,
Student of MTUCI, Moscow, Russia,
Vannetis@yandex.ru

Tatiana N. Zujkova,
Senior lecturer of the department of MTS, MTUCI, Moscow, Russia,
t.n.zuikova@mtuci.ru

Abstract

An analysis of the features of the functioning of mobile network structures in avionics is presented. An overview of the functional capabilities of air traffic participants in conditions of automatic dependent surveillance in broadcasting mode (ADS-B) is given. The relevance of the issue of information security in networks using ADS-B technology is noted. A method for authenticating air traffic participants in mobile network structures using the RSA cryptographic algorithm is proposed. The software for a microprocessor-based authentication tool based on the "Multikom-02" (MCom-02) system-on-chip has been developed.

Keywords: *avionics, mobile network structures, mobile self-organizing networks, air traffic safety, ADS-B, automatic dependent surveillance in broadcast mode, electronic signature, authentication, cryptographic means, information security, import substitution, system on a chip, microprocessor.*

РИСКИ ПРИМЕНЕНИЯ RFID-ТЕХНОЛОГИИ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Тимощук Юлия Сергеевна,
студент МТУСИ, Москва, Россия,
iul.tim2012@yandex.ru

Маклачкова Виктория Валентиновна,
ст. преп. кафедры «Сетевые информационные технологии и сервисы»,
директор по науке НО АПОС, МТУСИ, Москва, Россия,
v.v.maklachkova@mtuci.ru

Аннотация

В статье рассматриваются потенциальные проблемы, возникающие при использовании технологии радиочастотной идентификации (RFID) в медицинских учреждениях. Приводятся примеры применения RFID-технологии для идентификации объектов, персонала и пациентов, описываются возникающие при использовании риски и возможные контрмеры для уменьшения их влияния.

Ключевые слова: *риск, уязвимость, радиочастотная идентификация, RFID, безопасность данных, здравоохранение.*

Введение

В последние годы развитие современной системы здравоохранения, ставящей перед собой задачу повышения комфорта и безопасности лечения пациентов, невозможно представить без информационно-коммуникационных технологий. Происходящая цифровая трансформация учреждений здравоохранения базируется на использовании технологии Интернета вещей (IoT). В секторе здравоохранения устройства IoT, также известные как Интернет медицинских вещей (IoMT), поддерживают основные функции организаций здравоохранения и услуги, связанные со здоровьем. IoMT является технологией, обеспечивающей взаимодействие концепции IoT с медицинскими системами и устройствами для поддержки удаленного мониторинга, лечения пациентов в режиме реального времени и отслеживания цепочек поставок.

Во избежание ошибок, связанных с человеческим фактором, которые могут повлечь за собой угрозу здоровью и жизни пациентов, и ввиду широкого спектра используемой документации, а также необходимости учета значительного количества информации, в медицинских организациях применяются технологии автоматической идентификации, в частности RFID, внедрению которой способствуют проблемы, обусловленные пандемией COVID-19.

RFID-технология широко используется в различных сферах бизнеса и экономики, таких как логистика, торговля, общественный транспорт и т.д. [11], вытесняя штриховое кодирование, которое обладает определёнными недостатками, не допускающими его применение для отслеживания объектов в реальном времени. Помимо этого, штриховые коды необходимо сканировать исключительно в пределах прямой видимости, и они в отличие от меток RFID неустойчивы к разрывам и к влаге. Активные RFID-метки могут использоваться для отслеживания оборудования и персонала в реальном времени, что также позволяет повысить эффективность работы медицинских работников и уровень безопасности пациентов.

Нарушение безопасности медицинских данных, в том числе и персональных данных пациентов, является одним из важнейших рисков в отрасли здравоохранения. По данным InfoWatch, количество утечек персональных данных в сфере здравоохранение с каждым годом растет: к примеру, в 2020 по сравнению с 2019 годом [21] наблюдалось увеличение на 42% количества утечек из чего следует, что с ростом использования в медицине информационно-коммуникационных технологий (ИКТ) количество утечек будет только возрастать [31].

Ожидается, что, несмотря на присутствующие риски, рынок радиочастотной идентификации будет продолжать динамичное развитие, и к 2023 году, в связи с пандемией, среднегодовой темп роста рынка RFID в здравоохранении составит 20% [32].

Технология RFID

RFID (Radio Frequency Identification) или радиочастотная идентификация — это способ автоматической идентификации, в котором с использованием электромагнитного излучения происходит считывание или запись информации на устройство, называемое тег (tag), метка (label) или транспондер (transponder). RFID-метки «прикрепляются» ко всем объектам, о которых необходимо сохранить информацию для последующего использования в системе. Метка состоит из чипа и радиоантенны, и защищена пленкой (рис. 1).

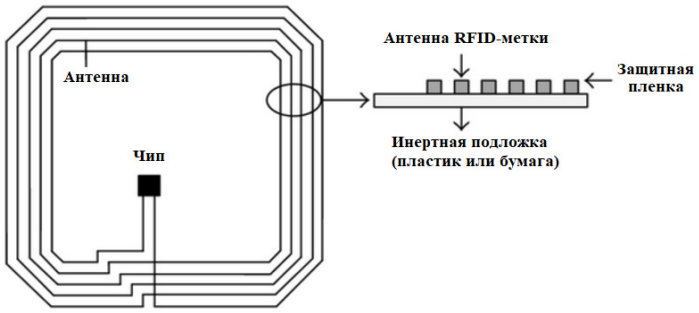


Рис. 1. Схематичное представление RFID-метки

Второй элемент системы RFID – считывающее устройство, так же называемое ридером (reader) или интеррогатором (interrogator). Считыватель может записывать данные в метку, устанавливая между собой и меткой двунаправленный обмен данными, а также выполнять аналого-цифровое и цифро-аналоговое преобразование [1].

По методу используемых источников питания RFID-системы делятся на пассивные и активные. Пассивные метки в качестве источника питания используют электромагнитное поле RFID-считывателя. Они обладают небольшой дальностью работы и имеют практически неограниченный срок службы. Активные - обладают собственным источником питания, что позволяет им иметь большую дальность считывания, а также энергозависимую память, для реализации, например, сложных протоколов шифрования [2].

RFID-системы могут работать на низких, высоких, сверхвысоких или микроволновых частотах. Активные RFID-метки обычно используют частоты 455 МГц, 2.45 ГГц или 5.8 ГГц, а пассивные – 124 КГц, 125 КГц, 135 КГц, 13.56 МГц, 860-960 МГц, 2.45 ГГц. С повышением частоты уменьшается дальность считывания, но повышается скорость передачи данных, что позволяет реализовать сложные протоколы данных [10].

Несмотря на то, что многие разработки в области RFID сосредоточены в области производственных процессов, в медицинских учреждениях также возможно применение любого из описанных типов RFID [4,5]. В настоящее время накоплен практический опыт внедрения этой технологии. Так, ещё в 2003 году во время вспышки SARS-2003, под контролем DOIT (Департамент промышленных технологий Тайваня) больницам были выделены средства на проведения исследований для внедрения технологии RFID, в ходе которых была изучена возможность повышения безопасности пациентов за счёт уменьшения медицинских ошибок с помощью специализированных технологических систем [13,14]. В России опыт внедрения RFID-систем был реализован компанией «Микрон» в 2017 году в виде RFID-браслетов для идентификации личностей пациентов. Тогда, в процессе исследования, были определены необходимые сведения для занесения на метку [22]. Во время эпидемии COVID-19 в 2019 году в фармацевтическом отделе больницы Пенсильвании (США) технологии RFID была использована для автоматизации процесса вакцинации от COVID-19 [23]. Помимо этого, успешное внедрение технология RFID в медицинские информационные системы было осуществлено в Дании, Ирландии, Италии, Германии, Швейцарии, Канаде, Чехии, Индии, Нидерландах, Финляндии, Великобритании и в других странах мира [15,16,19].

Применение RFID-технологии в медицинских учреждениях

Основная задача технологии RFID – автоматизированная аутентификация и идентификация объектов для повышения эффективности работы персонала и снижения влияния человеческого фактора на работу медицинского учреждения.

В таблице 1 представлены варианты реализации технологии RFID в сфере здравоохранения.

Таблица 1

Возможные применения автоматической идентификации

Общая задача	Пример реализации с использованием RFID
Идентификация пациентов	Использование браслетов для проверки личности до приема лекарств [19, 20]
Идентификация персонала	Автоматическая идентификация пользователя для работы в медицинской информационной системе
Идентификация документов	Маркировка документов с целью связывания с электронной копией на сервере
Слежение за оборудованием	Инструменты со встроенными метками для избегания ситуаций с оставлением инструментов внутри пациентов [6]
Идентификация лабораторных образцов	Идентификация биоматериала с автоматизированной регистрацией для последующего исследования
Отслеживание в банках крови	Этикировка пакетов с кровью для обеспечения переливания правильной группы крови
Идентификация и отслеживание лекарственных средств	Маркировка лекарств RFID-метками для снижения вероятности фальсификации лекарств [8]
Задача инвентаризации	Поддержка условий хранения биологических образцов и лекарственных средств
Отслеживание местонахождения персонала на территории больницы	Отслеживание контактов медицинских работников с положительными тестами COVID-19 [13]
Мониторинг состояния пациентов	Удаленный мониторинг пациентов и отслеживание их текущего самочувствия [17, 18, 20]

Уязвимости RFID-технологии

Целью RFID-систем, как части Интернета вещей, является обеспечение безопасности при обмене данными между частями медицинской информационной системой, что является особо критичным при работе с личностными данными (такими, как биометрические данные) [33]. Любая уязвимость в RFID-системах, и, соответственно в IoMT (Internet of Medical Things), позволяет злоумышленникам предпринять ряд действий, которые могут повредить здоровью и жизни пациентов [30]. В частности, бесконтактный метод связи, реализуемый с использованием малых объемов вычислительной мощности, делает RFID-системы уязвимыми к различным угрозам безопасности, среди которых можно выделить три группы, основанные на векторе атаки:

- **Угрозы на уровне оборудования** – связаны с атаками, при которых злоумышленник использует недостаточную устойчивость RFID-оборудования к физическим манипуляциям. К данному типу атак могут относиться: отключение, копирование или подмена RFID-меток, получение информации с меток методом обратной разработки; атаки с помощью намеренно вызванных сбоев оборудования, а также физическое вмешательство с целью получения данных [25].
- **Угрозы на транспортном уровне** – обусловлены атаками, основанными на уязвимостях используемых протоколов и способа передачи данных между объектами RFID-систем. К такому типу атак могут относиться такие атаки, как атака посредника, скимминг, атака повторного воспроизведения, а также электромагнитные помехи, предотвращающие связь меток со считывателями [26, 24].
- **Угрозы на программном уровне** – данный тип атак связан с несанкционированным доступом к информации, а также использованием уязвимости баз данных и приложений RFID-системы. Примером может служить внедрение вредоносного кода, компрометация криптографических ключей или применение DoS атаки [27, 25].

Для защиты RFID-систем на транспортном и программном уровнях предлагается использование таких защитных механизмов, как использование эффективных протоколов [29] и внедрение соответствующего программного обеспечения, нейтрализующего действия злоумышленников. Однако, некоторые риски остаются актуальными, либо по причине необходимости существенных затрат (атаки, связанные с аппаратным уровнем), либо из-за отсутствия эффективных технических решений (атаки, связанные с нарушением работоспособности RFID-аппаратуры) [25].

Проблемы использования RFID-систем в отрасли здравоохранения

Ввиду использования RFID-системы в учреждениях здравоохранения, задача построения такой системы осложняется наличием критически важных данных, требующих особой безопасности и надежности их хранения. Рассмотрим некоторые проблемы, возникающих при построении больничных RFID-систем [17-20]:

- Обеспечение конфиденциальности пациентов – большинство протоколов RFID требуют, чтобы метка имела уникальный идентификатор, что открывает возможность незаконной слежки или использование конфиденциальных данных мониторинга без разрешения пациента. Эта проблема осложняется тем, что многие RFID-метки не имеют высокоуровневых протоколов, позволяющих устанавливать параметры безопасности метки [1, 2]. В решении проблемы конфиденциальности может помочь шифрование [9, 28]. Так, в RFID-системах стандарта EPC Gen2 есть поддержка шифрования данных и создания конфиденциальных каналов связи, позволяющих обеспечить безопасность передачи данных [3].
- Проблема электромагнитной совместимости – исследования показывают, что низкочастотные RFID-системы могут повредить работе чувствительных к электромагнитному излучению, как имплантируемых, так и неимплантируемых устройств [4,5]. По этой причине перед развертыванием RFID-системы необходимо убедиться, что система не создаст электромагнитные помехи для медицинских устройств, а при размещении новых устройств, проверить их на устойчивость к радиочастотному излучению.
- Высокое энергопотребление активных RFID-меток – для активной RFID-технологии используются метки с встроенными источниками питания, ввиду чего возникает зависимость от ограниченного времени службы автономного источника питания и необходимости его периодической замены.
- Необходимость высокой точности данных – один из самых важных параметров в медицинских учреждениях – это точность передаваемых данных, от которых зависит жизнь пациента. Любое ошибочное, или ложное срабатывание снижает точность информационных данных, что ограничивает эффективность системы. С учётом этого больницы должны быть готовы к ложноположительным и ложноотрицательным срабатываниям [6, 7].
- Высокая цена развертывания RFID-систем – активные RFID-метки гораздо дороже, чем пассивные в обслуживании. Полноценно функционирующая RFID-система требует значительных затрат, связанных с покупкой меток и считывателей, промежуточного программного обеспечения, принтеров и других частей системы, а также с переоборудованием помещений. Возможным решением проблемы сокращения затрат может явиться использование недорогих систем, сочетающих пассивные и активные RFID-метки с штрих кодами, но это может затруднить реализацию требуемого уровня безопасности данных [8,12].

Медицинские данные требуют надёжной защиты. Медицинские организации все чаще начинают использовать облачную архитектуру IoMT, а это в свою очередь ведёт к увеличению риска нарушения конфиденциальности данных и усложняет процесс выявления новых рисков и использования средств по их минимизации [31, 34-36].

Заключение

Безопасность имеет первостепенное значение при развертывании систем RFID в медучреждениях. Обеспечивая точный мониторинг активов и продуктов в реальном режиме времени во всех цепочках поставок, технологии RFID повышают эффективность и безопасность этих цепочек. С учётом этого актуально управление потенциальными рисками и угрозами, которые связаны с применением данной технологии, с целью их идентификации и выработки мер для их предотвращения или минимизации отрицательного эффекта от их воздействия. Очевидно, что темпы внедрения RFID-технологии в сферу здравоохранения будут увеличиваться, поскольку данная технология имеет большие перспективы применения для автоматизации различных процессов, в том числе отслеживания цепочек поставок, и может потенциально обеспечить огромную пользу медучреждениям и пациентам за счёт экономии временных, финансовых и трудовых затрат.

Литература

1. *Вахрушева А. А.* Технологии позиционирования в режиме реального времени // Вестн. СГУГиТ. 2017. Т. 22/ № 1. С. 170-177.
2. *Hawrylak P.J., Hale J. (2015)* Data Privacy Issues with RFID in Healthcare. In: *Gkoulalas-Divanis A., Loukides G. (eds*) Medical Data Privacy Handbook. Springer, Cham. https://doi.org/10.1007/978-3-319-23633-9_21
3. *Engels D. W., Kang Y. S. and Wang J.* On security with the new Gen2 RFID security framework 2013 IEEE International Conference on RFID (RFID), 2013, pp. 144-151, doi: 10.1109/RFID.2013.6548148.
4. *Werner I. Electronic* Security Systems and Active Implantable Medical Devices 22 July 2003 Pacing and Clinical Electrophysiology/Volume 25, Issue 8 p./ 1235-1258, doi: 10.1046/j.1460-9592.2002.01235.x
5. *Seidman, S.J., Guag, J.W.* Adhoc electromagnetic compatibility testing of non-implantable medical devices and radio frequency identification. BioMed Eng OnLine 12, 71 (2013). https://doi.org/10.1186/1475-925X-12-71
6. *Tu, Y.-J., Zhou, W., & Piramuthu, S. (2009)*. Identifying RFID-embedded objects in pervasive healthcare applications. Decision Support Systems, 46(2), 586–593. doi:10.1016/j.dss.2008.10.001
7. *Kranzfelder, M., Schneider, A., Fiolka, A., Schwan, E., Gillen, S., Wilhelm, D., Schirren, R., Reiser, S., Jensen, B., Inf, D., Feussner, H. (2013)*. Real-time instrument detection in minimally invasive surgery using radiofrequency identification technology // Journal of Surgical Research, 185(2), pp. 704-710. doi:10.1016/j.jss.2013.06.022
8. *Афонин Д.Н., & Соколова Д.С.* (2019). Использование технологии радиочастотной идентификации (RFID-системы) в борьбе с фальсификацией и контрафакцией лекарственных средств // Bulletin of the International Scientific Surgical Association, 8 (1). С. 12-16.
9. *Бельский В.С., Грибоедова Е.С., Царегородцев К.Д., Чичаева А.А.* Безопасность RFID-систем // International Journal of Open Information Technologies. 2021. №9.
10. *Mier, J., Jaramillo-Alcázar, A., & Freire, J. J.* At a Glance: Indoor Positioning Systems Technologies and Their Applications Areas. Explorations in Technology Education Research. 2019, pp. 483-493. doi:10.1007/978-3-030-11890-7_47
11. *Григорьева А. Rfid в 2015 и в 2020 году //* Компоненты и технологии. 2021. Vol. 3., 6-8 URL: https://kit-e.ru/market/rfid-v-2015-i-v-2020.
12. *Mehta S, Grant K, Atlin C, Ackery A.* Mitigating staff risk in the workplace: the use of RFID technology during a COVID-19 pandemic and beyond. BMJ Health Care Inform. 2020;27(3):e100230. doi:10.1136/bmjhci-2020-100230
13. *S.-F. Tzeng, W.-H. Chen and F.-Y. Pai,* Evaluating the business value of RFID: Evidence from five case studies,International Journal of Production Economics 112(2). 2008, pp. 601-613.
14. *C.C. Lin, P.Y. Lin, P.K. Lu, G.Y. Hsieh, W.L. Lee and R.G. Lee,* A Healthcare Integration System for Disease Assessment and Safety Monitoring of Dementia Patients // IEEE Transactions on Information Technology in Biomedicine 12(5). 2008, pp. 579-586.
15. *Nahas, H. A., & Deogun, J. S. (2007)*. Radio Frequency Identification Applications in Smart Hospitals. Twentieth IEEE International Symposium on Computer-Based Medical Systems (CBMS'07). doi:10.1109/cbms.2007.90
16. *Ajami S, Rajabzadeh A.* Radio Frequency Identification (RFID) technology and patient safety. J Res Med Sci. 2013;18(9):809-813.
17. *Tao X, Shaik TB, Higgins N, Gururajan R, Zhou X. Remote Patient Monitoring Using Radio Frequency Identification (RFID)* Technology and Machine Learning for Early Detection of Suicidal Behaviour in Mental Health Facilities. Sensors (Basel). 2021 Jan 24;21(3):776. doi: 10.3390/s21030776. PMID: 33498893; PMCID: PMC7865785.
18. *H. Q. Omar, A. Khoshnaw and W. Monnet.* Smart patient management, monitoring and tracking system using radio-frequency identification (RFID) technology // 2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES), 2016, pp. 40-45. doi: 10.1109/IECBES.2016.7843411
19. *Ioan, T., Turcu, C., Turcu, C., & Cerlinc, M.* RFID-based Information System for Patients and Medical Staff Identification and Tracking. Sustainable Radio Frequency Identification Solutions. 2010. doi:10.5772/8015
20. *Haddara, M.; Staaby, A. RFID* Applications and Adoptions in Healthcare: A Review on Patient Safety. In Proceedings ofthe International Conference on Health and Social Care Information Systems and Technologies (HCIST), Lisbon, Portugal, 21-23 November 2018; Elsevier: Amsterdam, The Netherlands, 2018. Vol. 138, pp. 80-88.
21. Медицинские организации: утечки конфиденциальной информации // Infowatch Аналитика 24.08.2021. URL: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/meditsinskie-organizatsii-utechki-konfidentsialnoy-informatsii.

22. RFID-браслеты «Микрона» для идентификации пациентов протестировали в подмосковной клинике // mikron.ru 10.02.2017. URL: https://mikron.ru/company/press-center/news/2137.
23. B. Siwicki RFID tech helps Reading Hospital boost volume of COVID-19 vaccinations // HealthcareITNews 25.03.2021 URL: https://healthcareitnews.com/news/rfid-tech-helps-reading-hospital-boost-volume-covid-19-vaccinations.
24. *Khattab, A., Jeddi, Z., Amini, E., & Bayoumi, M.* RFID Security Threats and Basic Solutions. RFID Security. 2016, 27-41. doi:10.1007/978-3-319-47545-5_2
25. *Mitrokotsa, A., Beye, M., & Peris-López, P.* Classification of RFID Threats based on Security Principles. 2010.
26. *M. Jouini, L.B.A. Rabai,* Threats classification: state of the art, in: Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, 2016, pp. 368-392.
27. *Смирнов А. С., Мулейс Р. Б., Савчук А. В., Толстая А. М., Рубин Д. Т.* Анализ возможности внедрения вредоносного кода в системы автоматизированного управления на основе уязвимостей RFID-технологии // Спецтехника и связь. 2013. №1.
28. *A., Rahman S.S.M. (2017)* Security Solution of RFID Card Through Cryptography. In: *Wang G., Atiquzzaman M., Yan Z., Choo KK. (eds)* Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017 // Lecture Notes in Computer Science, vol.10658. Springer, Cham.
29. *Wang, S., & Zhang, B. (2019).* Research on Security Protocol of RFID System Based on Public Key Cryptography. Journal of Physics: Conference Series, 1237, 022134. doi:10.1088/1742-6596/1237/2/022134
30. *Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT* Communications: A Survey. Sensors. 2020, 20, 4828. doi:10.3390/s20174828
31. *Maklachkova V. V., Dokuchaev V. A., Statev V. Y. Risks* identification in the exploitation of a geographically distributed cloud infrastructure for storing personal data // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 – Proceedings, Vienna, 20-22 октября 2020 года. P. 9261541. DOI 10.1109/EMCTECH49634.2020.9261541.
32. *Dokuchaev V. A., Maklachkova V. V., Statev V. Yu*. Classification of personal data security threats in information systems // T-Comm. 2020. Vol. 14. No 1. P. 56-60. DOI 10.36724/2072-8735-2020-14-1-56-60
33. *Докучаев В. А., Маклачкова В. В., Статьев В. Ю.* Требования к информационным системам при работе с «цифровым образом» субъекта // III Научный форум телекоммуникации: теория и технологии ТТТ-2019 : Материалы XXI Международной научно-технической конференции, Казань, 18-22 ноября 2019 года. Казань: Казанский государственный технический университет им. *А.Н. Туполева,* 2019. С. 296-297.
34. *Гадасин Д. В., Шведов А. В., Клыгина О. Г., Гадасин Д. Д.* Реализация платформы туманных вычислений для предоставления сервисов IoT / // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 2. С. 65-75.
35. *Назаров М. Д., Шведов А. В.* Корреляция атрибутов соглашения об уровне обслуживания с основными параметрами QoS в корпоративных сетях // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 73-79.
36. *Гадасин Д. В., Шведов А. В.* Проблемы интеграции концепции "интернет вещей" и облачных вычислений // Технологии информационного общества: Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20-21 марта 2019 года. М.: ООО "Издательский дом Медиа паблишер", 2019. С. 22-23.

RISKS OF APPLICATION RADIOFREQUENCY IDENTIFICATION IN HEALTH FACILITIES

Julia S. Timoschuk,
Graduate MTUCI, Moscow, Russia,
iul.tim2012@yandex.ru

Victoria V. Maklachkova,
Senior Lecture, director for scientific NO "ACEM" MTUCI, Moscow, Russia,
v.v.maklachkova@mtuci.ru

Abstract

The article considers potential problems arising from the use of radio-frequency identification (RFID) technology in medical institutions. It gives examples of the application of RFID technology for the identification of objects, staff and patients, describes the risks arising from the use and possible countermeasures to reduce their impact.

Keywords: *risk, vulnerability, radiofrequency identification, RFID, data security, healthcare.*

АЛГОРИТМЫ ШИФРОВАНИЯ НА АБОНЕНТСКОМ ДОСТУПЕ В ИМИТАТОРЕ ОБЪЕДИНЕННОЙ СЕТИ ПД СПЕЦНАЛЬНОГО НАЗНАЧЕНИЯ

Басараб Михаил Алексеевич,
заведующий кафедрой ИБ МГТУ им. Н.Э.Баумана, д.ф.-м.н., Москва, Россия,
bmic@mail.ru

Бельфер Рувим Абрамович,
доцент кафедры ИБ МГТУ им. Н.Э.Баумана, к.т.н., Москва, Россия,
a.belfer @ yandex.ru

Глинская Елена Вячеславовна,
старший преподаватель кафедры ИБ МГТУ им. Н.Э.Баумана,
glinskaya-iu8@rambler.ru

Кравцов Александр Владимирович,
начальник отдела НИИЦ ЦНИИ ВВКО, Москва, Россия,
skyak78@gmail.com

Орлов Владимир Георгиевич,
главный специалист отдела ОНИРС, к.т.н., МТУСИ, Москва, Россия,
v.g.orlov@mtuci.ru

Аннотация

Приведены результаты разработки специализированных механизмов и алгоритмов шифрования данных на участке абонентского доступа для использования в имитаторе объединенной сети ПД специального назначении, в том числе следующие алгоритмы: алгоритм канального шифрования в разработанном алгоритме имитации объединенной сети ПД при установлении двух коммутируемых виртуальных каналов (КВК) в изолированных частных сетях ПД; алгоритм шифрования/дешифрации при формировании принудительной маршрутизации (от источника) для каждого устанавливаемого КВК и алгоритм шифрования/дешифрации при передаче результатов установления КВК в Центр Управления имитатором сети ПД. При этом источником установления каналов КВК служит оконечный пункт абонентского доступа.

Ключевые слова: *имитатор сети (network simulator), сеть передачи данных (data transmission network), имитатор сети (network simulator), маршрутизация (routing), принудительная маршрутизации (forced routing).*

Введение

Представленные в статье материалы основаны на результатах комплексных исследований, целью которых являлась разработка схемотехнических и алгоритмических решений, положенных в основу создания учебно-лабораторного имитатора для изучения особенностей функционирования и повышения эффективности объединенных сетей передачи данных (ПД) специального назначения

К категории сетей специального назначения в соответствие с ФЗ «О связи» (п.16) относятся сети «для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка» [1]. В ходе, проходившей в 2015 году IV-ой национальной конференции «Информационные технологии на службе оборонно-промышленного комплекса России-2015» были подробно рассмотрены и детально обсуждены вопросы построения и особенности функционирования сетей данного назначения. Особо подчёркнута актуальность этих вопросов в резолюции, принятой участниками конференции по результатам её работы [2]. В резолюции конференции была поставлена задача создания объединенной сети ПД, которая должна включать независимые изолированные частные сети государственных структур категории специального назначения. При этом каждая такая государственная структура может включать несколько частных сетей ПД.

Особенностью сетей связи специального назначения являются высокие требования к количественным показателям качества обслуживания. Одним из важнейших из них является информационная безопасность (ИБ). Методы и механизмы, обеспечивающие решение задач поддержки требуемого уровня информационной безопасности в сетях ПД, относящихся к категории сетей специального назначения, являются компетенцией государственных органов и специализированных научно-производственных организаций. В их практиках широко используются новые нестандартные подходы и механизмы, для достижения требуемых показателей ИБ. В рамках создания учебно-лабораторного имитатора сети ПД решалась иная задача, целью которой являлась разра-

ботка основных положений по построению системы архитектуры ИБ объединенной сети ПД категории специального назначения. При проведении научно-исследовательских работ по созданию имитатора использовались опубликованные работы и стандарты по ИБ зарубежных сетей связи общего пользования (ССОП), а также сетей связи в модернизированных технологических системах энергообеспечения Smart Grid и др.

1. Постановка задачи

В работе [3] кратко отмечается и необходимость канального шифрования адресной части пакета данных между узлами коммутации в сети ПД совместно со сквозным шифрованием между взаимодействующими оконечными пунктами соединения информационной части пакета данных. Такой подход к совместному использованию обоих видов шифрования повышает защищенность от угроз ИБ в сетях ПД. В данной статье рассматриваются вопросы и приводятся результаты разработки алгоритма канального шифрования на участке абонентского доступа источника соединения при установлении коммутируемого виртуального канала (КВК). Экспериментальная отработка алгоритма производилась с использованием учебно-лабораторного имитатора сети ПД специального назначения. Характерные отличия и особенности сетей ПД данной категории в сравнении с сетями общего пользования детально рассмотрены в [4-6].

Разработанный алгоритм канального шифрования представлен на примерах установления двух КВК между двумя частными сетями ПД (ЧС1 и ЧС3) с использованием имитатора объединенной сети.

На рисунке 1 представлена конфигурация учебно-исследовательского лабораторного имитатора объединённой сети ПД. Имитатор позволяет сформировать пучок маршрутов между оконечными пунктами, содержащий четыре различных пути маршрутизации, причём каждый из них включает три центра коммутации пакетов данных (ЦКП). При этом к двум граничным ЦКП в каждом из путей маршрутизации (ЦКП1.1, ЦКП1.2) подключены удаленные оконечные пункты (a,b,...,c).

Обмен данными между оконечными пунктами (ОП) КВК и граничными маршрутизаторами ЦКП1.1, ЦКП1.2 осуществляется по четырём путям маршрутизации, (по двум абонентским доступам с каждым граничным маршрутизатором). Для упрощения на рисунке 1 показано по одному абонентскому доступу к каждому граничному маршрутизатору.

Требуется разработать алгоритм канального шифрования при установлении соединения на всех четырех путях маршрутизации.

Примем физические адреса узлов коммутации: ЦКП1.1 – 11, ЦКП1.2 -12, ЦКП2.1 – 21, ЦКП2.2 – 22, ЦКП3.1 – 31, ЦКП3.2 – 32 и физический адрес центра эксплуатации сети ЦЭС – 0.

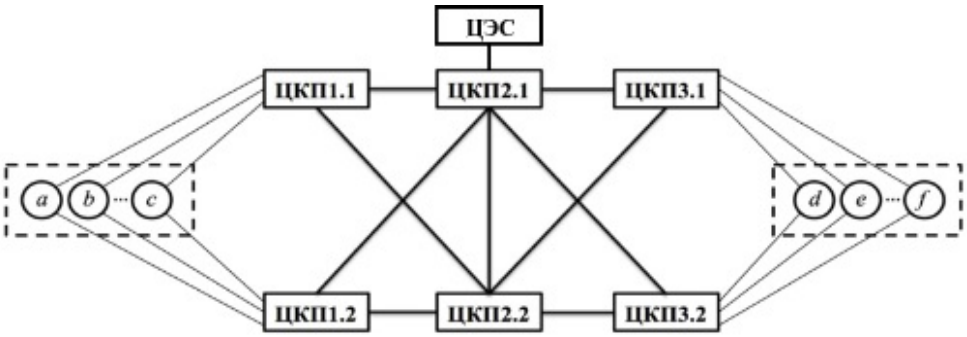


Рис. 1. Конфигурация учебно-лабораторного имитатора объединенной сети ПД

Оконечные пункты *a* (ОП*a*) и *f* (ОП*f*) на рисунке 1, который отображает конфигурацию имитатора объединенной сети ПД принадлежат частной сети 1 (ЧС1), а оконечные пункты *b* (ОП *b*) и *d* (ОП*d*) – частной сети 3 (ЧС3). Присвоим соответственно физические адреса для ОП*a,* ОП*f,* ОП*b и* для ОП*d* соответственно: 101; 601; 2101; и 2601.

Приведём описание укрупненных алгоритмов защищенного канального шифрования при установлении КВК на примере двух частных сетей ЧС1 и в ЧС3 объединенной сети ПД, сформированной с использованием имитатора, предположив, что ЧС1 и ЧС3 независимые изолированные частные сети разных государственных структур категории специального назначения.

Начнём с выполнения расчета канальных ключей, используемых для шифрования сообщений на всех четырех путях маршрутизации (всех абонентских доступов оконечных пунктов источника установления КВК), а так же применяемых при выполнении функции управления сетью по формированию принудительной маршрутизации (‘от источника”).

Обозначим КВКn – коммутируемый виртуальный канал частной сети n, тогда $КВК_1$ соответствует ЧС1, а $КВК_3$ – ЧС3.

Определим исходное состояние очередей свободных номеров в ЦКП1.1 и ЦКП1.2 абонентского доступа имитатора объединенной сети. Очереди свободных номеров с целью упрощения описания алгоритмов приняты одинаковыми в ЦКП 1.1 и в ЦКП 1.2:

– очередь ЧС1: О1свн1112: 809; 802; 805; 814; 815; 816; 817; 818; 819; 820; 821, 822, 823; 824; 825; 826; 827; 828; 804; 807… 801; 803;

– очередь ЧС3: О3свн1112:2809; 2802; 2805; 2814; 2815; 2816;2817; 2818; 2819; 2820; 2821, 2822, 2823; 2824; 2825; 2826; 2827; 2828; 2804; 2807… 2801; 2803.

2. Описание алгоритма абонентского доступа источника установления КВК в имитаторе объединенной сети ПД

Алгоритм абонентского доступа источника установления КВК в имитаторе объединенной сети ПД в настоящей работе рассматривается при исправном состоянии всех устройств имитатора на примере установления двух соединений – одного в ЧС1 ОП*a* – ОП*f,* другого в ЧС3 ОП*b*- ОП*d.*

2.1. Аутентификация оконечного пункта имитатора сети.

Алгоритм установления КВК в имитаторе объединенной сети ПД начинается с аутентификации оконечных пунктов источника - инициатора установления. В настоящем материале это относится к аутентификации оконечного пункта ОП*a* частной сети 1 и оконечного пункта ОП*b* частной сети 3.

2.2. Ассоциация безопасности.

Выполнение ассоциации безопасности SA (Security Association) производится по выбору механизма шифрования устанавливаемых КВК:

– КВК1 абонентских доступов первого и третьего путей пучка маршрутизации ОПа – ЦКП 1.1. и абонентских доступов второго и четвертого путей пучка маршрутизации ОПа – ЦКП1.2;

– КВК3 абонентских доступов первого и третьего путей пучка маршрутизации ОПb – ЦКП 1.1, абонентских доступов второго и четвертого путей пучка маршрутизации ОПb – ЦКП1.2; абонентского доступа ОПb - ЦКП1.2.

2.3. Формирование разовых канальных ключей на абонентском доступе.

Для защиты от угроз ИБ при установлении КВК на участке абонентского доступа оконечного пункта источника каждое сообщение должно подлежать канальному шифрованию/дешифрации. Для этого, кроме выбора механизма шифрования по алгоритму ассоциации безопасности, необходимо создать ключ канального шифрования (канальный ключ). Этот ключ необходим для защиты шифрованием/дешифрацией сообщений по каждому из четырёх путей маршрутизации между оконечным пунктом и граничными маршрутизаторами: ОП*a* –ЦКП 1.1, ОП*a* –ЦКП1.2 для $КВК_1$ и ОП*b* –ЦКП1.1, ОП*b* –ЦКП1.2 для $КВК_3$. При этом между ОП и ЦКП проходят первый и третий путь маршрутизации, а второй и четвертый – между ОП и ЦКП 1.2. [6].

С целью обеспечения высоких требований по ИБ в имитаторе сети ПД для каждого пути маршрутизации абонентского доступа создается головной (предварительный) ключ KPnm, где: P – номер пути маршрутизации устанавливаемого КВК; m – физические адреса граничного узла коммутации; n – физические адреса ОП, однозначно определяющие принадлежность устанавливаемого КВК к соответствующей ЧС. При взаимной аутентификации всех четырех абонентских доступов устанавливаемого КВК предусмотрено создание единого головного (подготовительного) ключа. Как будет показано ниже, на основе этого головного ключа формируется канальный ключ абонентского доступа.

В работе [7,8] изложен алгоритм взаимной аутентификации (на основе стандартов сети связи ISDN), включающий формирование; ключа первого и третьего пути маршрутизации, а именно; ключа K_{10111} для устанавливаемого $КВК_1$ на абонентском доступе (ОП*a* –ЦКП1.1) второго и четвертого путей маршрутизации; ключа K_{10112} на участке абонентского доступа (ОП*a* –ЦКП 1.2) первого и третьего путей маршрутизации; ключа K_{210111} для устанавливаемого $КВК_3$ на абонентском доступе (ОП*b* –ЦКП1.1) второго и четвертого путей маршрутизации, и ключа K_{210112} устанавливаемого $КВК_3$ на абонентском доступе (ОП*b* –ЦКП1.2.)

На основе подготовительного ключа формируются канальные ключи для каждого из четырех путей маршрутизации устанавливаемых $КВК_1$ и $КВК_3$. Канальные ключи являются **разовыми** в двух случаях:

1. Взаимная аутентификация на абонентском доступе производится при установлении каждого КВК;
2. Взаимная аутентификация на абонентском доступе производится при установлении не каждого КВК. В этом случае предварительным ключом является головной ключ последней взаимной аутентификации, увеличенный на очередной порядковый номер устанавливаемого соединения в ЧС, полученный из специально установленного счетчика КВК.

Разовые канальные ключи четырех путей маршрутизации установления КВК1 на абонентском доступе:

– ОПа –ЦКП1.1: K110111 = hash(K10111||1) и K210112 = hash(K10111||2),

– ОПа –ЦКП1.2: K310111 = hash(K10112||3), K410112 = hash(K10112||4).

Разовые канальные ключи четырех путей маршрутизации установления КВК3 на абонентском доступе:

– ОПb –ЦКП1.1: K1210111 = hash(K210111||1) и K2210112 = hash(K210111||2)

– ОПb –ЦКП1.2: K3210112 = hash(K210111||3), K410112 = hash(K210112||4).

2.4. Снятие в граничных маршрутизаторах ЦКП 1.1 и ЦКП 1.2 стоящий первым логический адрес LCN (Logical Channel Number)=809 в вышеприведенной очереди свободных номеров $О_{1свн1112}$ ЧС1.

Данная процедура включает последовательное выполнение следующих операций:

1. Передачу в ОПа стоящий первым логический адрес LCN по четырем защищённым путям маршрутизации с использованием соответствующих канальных ключей: К110111, К210112, К310111, К410112.
2. Дешифрацию на приеме, включающую снятие в граничных маршрутизаторах ЦКП1.1 и ЦКП1.2 стоящий первым логический адрес LCN=2809 в приведенной выше очереди свободных номеров $О_{3свн}$1112 ЧС3.
3. Передачу в ОПb этот LCN по четырем путям маршрутизации, защищённый соответствующими канальными ключами (К1210111, К2210112, К3210111, К4210112).
4. Дешифрацию переданных данных на приёме с использованием на приеме механизмов шифрования/дешифрации определённых в соответствие спри ассоциацией безопасности SA (п. 2.3).
5. Корректировку очереди и характеристик очередей $О_{1свн}$1112 и $О_{3свн}$1112. с целью использования для установлений других КВК для частных сетей, включая снятие с $О_{1свн}$1112 и $О_{3свн}$1112 соответственно LCN=2809 и LCN=2809.

2.5. Алгоритм формирования таблиц принудительной маршрутизации (“от источника”) при установлении $КВК_1$ и $КВК_3$ в имитаторе объединенной сети ПД.

Для объединенных сетей характерно мультиплексирование на участках сообщений разных частных сетей. На рассматриваемых установлениях $КВК_1$ и $КВК_3$ для формирования таблиц принудительной маршрутизации потребуется обмен сообщениями частных сетей ЧС1 и ЧС3 по одинаковым путям маршрутизации: ЦКП1.1 - ЦКП2.1 – ЦЭС и ЦКП1.2 - ЦКП2.1 – ЦЭС.

Для того, чтобы частные сети в объединенной сети ПД были изолированы между собой, сообщения обмена на их участках должны быть защищенными канальным шифрованием/дешифрацией от угроз безопасности. Ниже приведена формула вычисления канального ключа на участке сети между двумя узлами коммутации, используемыми нескольким частными сетями для формирования таблицы принудительной маршрутизации:

$$Krs(Z,P) = hash(Krs\,||Z||P), \quad (1)$$

где Krs – подготовительный канальный ключ между узлами коммутации r-s; Z – номер частной сети; P – номер пути маршрутизации.

Формула 1 позволяет вычислить отличающиеся друг от друга ключи канального шифрования не только для разных ЧС, но и с целью большей надёжности отличающимися для разных путей маршрутизации ЧС.

В следующем подразделе (2.5.1) приводится описание алгоритма выполнения этой функции, а именно определения механизма шифрования и формирования канальных ключей на общих участках имитатора сети ПД для частных сетей ЧС1 и ЧС3 с устанавливаемыми $КВК_1$ и $КВК_3$.

Для упрощения вычислений произведём их для общих для ЧС канальных ключей ЦКП 1.2- ЦКП 2.1 и ЦКП 2.1 – ЦЭС, в имитаторе сети установлений $КВК_1$ и $КВК_3$, т.е. по формуле Krs (Z) = hash(Krs ||Z). Как отмечено в раздел 1, эта процедура выполняется после предварительной взаимной аутентификации устройств имитатора объединенной сети ПД.

2.5.1.Выбор механизмов шифрования и создание канальных ключей на участках имитатора сети: ЦКП1.1- ЦКП2.1; ЦКП1.2 – ЦКП2.1; и ЦКП2.1 – ЦЭС.

На участках ЦКП1.1- ЦКП2.1 и ЦКП1.2- ЦКП2.1 производится выполнение следующих процедур:

- выбор механизма шифрования по алгоритму ассоциации безопасности обменом сообщениями между ЦКП 1.1 и ЦКП 2.1. В зависимости от требований ИБ для ЧС, эти механизмы могут различаться в ЧС1 и ЧС3 и в путях маршрутизации разных ЧС.
- создание канальных ключей. По результатам последней взаимной аутентификации устройств ЦКП 1.1 и ЦКП 2.1 создается подготовительный канальный ключ $К_{1121,}$ где 1121 - физические адреса соответственно ЦКП 1.1 и ЦКП 2.1. и ЦКП 1.1 - ЦКП 2.1. При вычислении по формуле Krs (Z) = hash(Krs ||Z) канальные ключи ЧС1 и соответственно ЧС3 равны: $К_{1121}$ (1) = hash($_{1121}$ ||1) и $К_{1121}$ (3) = hash($_{1121}$ ||3). На участке ЦКП 1.2- ЦКП 2.1 канальные ключи ЧС1 и ЧС3 соответственно равны $К_{1221}$ (1) = hash($_{1221}$ ||1), $К_{1221}$ (3) = hash($_{1221}$ ||3)
- выбор механизма шифрования по алгоритму ассоциации безопасности обменом сообщениями между ЦКП 1.2 и ЦКП 2.1. В зависимости от требований ИБ для частных сетей эти механизмы могут различаться для ЧС1 и ЧС3 в рассматриваемом примере имитатора объединенной сети ПД.
- создание канальных ключей. По результатам последней взаимной аутентификации устройств ЦКП 1.2 и ЦКП 2.1 создается подготовительный канальный ключ К1221, где 1221 -физические адреса соответственно ЦКП 1.2 и ЦКП 2.1. Обозначим Kz1221 - канальный ключ частной сети Z устройств на участке ЦКП1.2 - ЦКП2.1. В результате, канальные ключи ЧС1и ЧС3 соответственно К11221 = hash (К1221||1) и К31221 = hash (К1221||3).

Далее для участка ЦКП2.1 – ЦЭС выполняется:

– выбор механизма шифрования по алгоритму ассоциации безопасности обменом сообщениями между ЦКП 2.1 и ЦЭС. В зависимости от требований ИБ для частных сетей, эти механизмы могут различаться для ЧС1 и ЧС3 в рассматриваемом примере имитатора объединенной сети ПД.

– создание канальных ключей. По результатам последней взаимной аутентификации устройств ЦКП2.1 и ЦЭС создается подготовительный канальный ключ К210, где 210 -физические адреса соответственно ЦКП2.1 и ЦЭС. При вычислении по формуле Krs (Z) = hash(Krs ||Z). канальный ключи для ЧС1 и ЧС3 соответственно равны: К210 (1) = hash(210 ||1) и К210 (3) = hash(210 ||3).

2.5.2. Формирование сообщения-запроса цепочек маршрутизации.

Для каждого устанавливаемого соединения ($КВК_1$ и $КВК_3$) необходимо составить в граничных маршрутизаторах абонентских доступов (ЦКП1.1 и ЦКП1.2) сообщения-запрос соответствующих цепочек маршрутизации $ЗЦМ_1$ и $ЗЦМ_3$, включающие информацию о типе сообщения и следующие данные в $ЗЦМ_1$, в скобках для $ЗЦМ_3$:

- физический адрес ЦКП абонентского доступа оконечного пункта источника установления КВК - 101 (2101);
- физический адрес оконечного пункта абонентского доступа назначения установления КВК - 601 (2601);
- пути маршрутизации сообщений ЗЦМ от граничных маршрутизаторов в ЦЭС. Они одинаковые для $ЗЦМ_1$ и $ЗЦМ_3$: ЦКП 1.1- ЦКП 2.1- ЦЭС и ЦКП 1.2-ЦКП 2.1-ЦЭС;

2.5.3. Передача сообщений - запроса цепочек маршрутизации в ЦЭС.

Для реализации данной процедуры необходимо выполнение следующие действий:

- передачи в ЦКП2.1 из ЦКП1.1 зашифрованных в нем $ЗЦМ_1$ и $ЗЦМ_3$ с использованием канальных ключей ЧС1 ЦКП 1.1- ЦКП2.1 $К_{1121}$ (1) и ЧС3 $К_{1121}$ (3), а также дешифрование $ЗЦМ_1$ и $ЗЦМ_3$ в ЦКП2.1 на приеме. (Механизмы шифрования по алгоритму ассоциации безопасности между ЦКП1.1 и ЦКП2.1 определены в п. 2.5.1.).
- передачи из ЦКП1.2 в ЦКП2.1 зашифрованные в нем $ЗЦМ_1$ и $ЗЦМ_3$ с использованием канальных ключей ЧС1 ЦКП1.2- ЦКП2.1 $К_{1221}$ (1) и ЧС3 $К_{1221}$ (3) и затем дешифрация на приеме в ЦКП 2.1 данные $ЗЦМ_1$ и $ЗЦМ_3$
- передачи в ЦЭС из ЦКП2.1 зашифрованных в нем с помощью канальных ключей ЦКП2.1 и ЦЭС К1210 (К3210) данных ЗЦМ1 и ЗЦМ3, и дешифрация их при приёме в ЦЭС по алгоритму ассоциации безопасности между ЦКП2.1 и ЦЭС (п. 2.5.1).

2.5.4. Формирование сообщения цепочек маршрутизации.

На основании полученных в ЦЭС данных, содержащихся в $ЗЦМ_1$ и $ЗЦМ_3$ формируются два сообщения цепочек принудительной маршрутизации $ЦМ_1$ (для ЧС1) и $ЦМ_3$ (для ЧС3) соответственно для устанавливаемых $КВК_1$ и $КВК_3$. Каждое из этих сообщений включает, помимо типа сообщения, следующие значения для ЧС1 и ЧС3:

- принадлежность КВК определенной частной сети ЧС1 (ЧС3);
- текущий номер устанавливаемого КВК N1 для ЧС1 (N3 для ЧС3). Примем N1 = N3 =1;
- пути принудительной маршрутизации (“от источника”), устанавливаемые в граничные маршрутизаторы ЦКП1.1 и ЦКП1.2.

Для упрощения изложения положений, положенных в основу структуры разработанного алгоритма, примем одинаковыми пучки маршрутов, то есть цепочки устанавливаемых в имитаторе маршрутов КВК1-ЧС1 и КВК3-ЧС3.

В ЦКП 1.1 в пучках маршрутов КВК1 и КВК3 первого пути цепочки принудительной маршрутизации 11-21-31 и, соответственно, третьего пути маршрутизации 11-22-31, в ЦКП 1.2. Цепочки принудительной маршрутизации второго и четвёртого пути соответственно: 12-22-32 и 12-21-32. Все указанные четыре пути маршрутизации формируются в ЦЭС с учетом состояния устройств каналов сети ПД.

2.5.5. Передача сообщений цепочек маршрутизации в граничные маршрутизаторы.

Для выполнения данной процедуры необходимо:

- установить пути маршрутизации сообщений $ЦМ_1$ и $ЦМ_3$, обратные путям маршрутизации $ЗЦМ_1$ и $ЗЦМ_3$. ЦЭС- ЦКП 2.1- ЦКП 1.1 и
- ЦЭС- ЦКП2.1- ЦКП1.2.
- передать из ЦЭС в ЦКП2.1 зашифрованные в нём $ЦМ_1$ и $ЦМ_3$. При этом для шифрования и дешифрации в ЦЭС и ЦКП2.1 используются те же механизмы шифрования и канальные ключи, что и при передаче $ЗЦМ_1$ и $ЗЦМ_3$ между ЦЭС в ЦКП 2.1 (разд. 2.5.1.).
- преобразовать в ЦКП2.1 каждую $ЦМ_1$ и $ЦМ_3$ в две. Одну из них подготовить для передачи из ЦКП2.1 в ЦКП1.1, убрав цепочки принудительной маршрутизации второго и четвертого путей пучка маршрутизации (12-22-32 и 12-21-32), а вторую подготовить для передачи из ЦКП2.1 в ЦКП1.2, убрав цепочки принудительной маршрутизации первого и третьего путей пучка маршрутизации (11-21-31 и 11-22-31).

- передать из ЦКП2.1 в ЦКП1.1 зашифрованные $ЦМ_1$ и $ЦМ_3$ в ЦКП 2.1 и дешифровать их в ЦКП1.1. Для шифрования и дешифрации в ЦКП2.1 и ЦКП1.1 используются те же механизмы шифрования и канальные ключи, что и при передаче $ЗЦМ_1$ и $ЗЦМ_3$ ЦКП 2.1 в ЦКП1.1 (разд. 2.5.1.).
- передать из ЦКП2.1 в ЦКП1.2 зашифрованные $ЦМ_1$ и $ЦМ_3$ в ЦКП 2.1 и дешифровать их в ЦКП1.1.. Для шифрования и дешифрации в ЦКП2.1 и ЦКП1.1 также используются механизмы шифрования и канальные ключи, что и при передаче $ЗЦМ_1$ и $ЗЦМ_3$ из ЦКП2.1 в ЦКП1.1 (разд. 2.5.1.).

Заключение

На основе использования конфигурации разработанного учебно-лабораторного имитатора объединенной сети ПД и с учетом особенностей механизмов аутентификации и ассоциации процедур безопасности разработан алгоритм канального шифрования на удаленном абонентском доступе в объединенной сети ПД отнесённой к категории специального назначения при установлении КВК, источником которого является оконечный пункт этого доступа. Разработан алгоритм имитации установления соединения между двумя изолированными частными сетями по одному КВК на участке абонентского доступа объединенной сети ПД. Также разработаны алгоритм шифрования/дешифрации при формировании принудительной маршрутизации (“от источника”) для каждого устанавливаемого КВК и алгоритм шифрования/дешифрации при передаче результатов установления КВК в Центр Управления имитатором сети ПД.

Литература

1. Федеральный закон Российской Федерации «О связи» № 126-ФЗ от 07.07.2003 (редакция от 05.01.2018 г.).
2. Резолюция конференции «Информационные технологии на службе оборонно-промышленного комплекса России 2015» // Connect. 2015. № 9. С. 78-88
3. *Столингс В*. Основы защиты сетей. Приложения и стандарты. М.: Вильямс, 2002. 324 с.
4. *Матвеев В.А., Бельфер Р.А., Кравцов А.В.* Анализ технологий построения сети передачи данных с высокими требованиями по информационной безопасности, надежности и задержке // Электросвязь. 2017. № 5. С. 46-49.
5. *Матвеев В.А., Басараб М.А., Бельфер Р.А. и др*. Алгоритм функционирования УЛС защищенной сети ПД на базе виртуальных каналов с высокими требованиями к качеству обслуживания // Электросвязь. 2017. № 8. С. 57-62.
6. *Басараб М.А., Бельфер Р.А., Кравцов А.В. , Орлов В.Г.* Алгоритмы передачи данных в имитаторе объединенной сети специального назначения // Телекоммуникации и информационные технологии. 2019. № 2. С. 76-81.
7. *Бельфер Р.А., Глинская Е.В., Кравцов А.В.* Алгоритм программного обеспечения аутентификации абонентского доступа имитатора сети ПД учебного лабораторного стенда // Первая миля. 2018. №1. С. 64-68.
8. *Орлов В.Г., Фадеев А.Н.* Протоколы маршрутизации в мобильных ad-hoc-сетях // Фундаментальные проблемы радиоэлектронного приборостроения. 2012. Т. 12. № 6. С. 208-212.

ENCRYPTION ALGORITHMS FOR SUBSCRIBER ACCESS IN THE SIMULATOR OF THE UNITED DATA TRANSMISSION NETWORK FOR SPECIAL PURPOSES

***Michael A. Basarab*,**
Head of the Department of IS, Doctor of P&M Sciences,
*MSTU named after N.E. Bauman, Moscow, Russi*a,
bmic@mail.ru

Ruvim A. Belfer
Associate Professor of the Departmen of IS, PhD,
*MSTU named after N.E. Bauman, Moscow, Russi*a,
a.belfer @ yandex.ru

***Elena V. Glinskaya*,**
Senior Lecturer of the Department of IS,
*MSTU named after N.E. Bauman, Moscow, Russi*a

***Aleksandr V. Kravtsov*,**
Head of the Department of the R&TC of the CRI of ADF,
*Moscow, Russi*a,
skyak78@gmail.com

***Vladimir G.Orlov*,**
Chief specialist of the Department of OoRWoS, PhD.,
MTUCI, Moscow, Russia,
v.g.orlov@mtuci

Abstract

The results of the development of specialized mechanisms and algorithms for data encryption at the subscriber access section for use in a simulator of a unified DT network for special purposes, including the following algorithms: private networks of DT; an encryption / decryption algorithm when generating forced routing (from the source) for each installed SVC and an encryption / decryption algorithm when transmitting the results of establishing a SVC to the Control Center of the DT network simulator. The source of the establishment of the SVC channels is the subscriber access terminal point.

Keywords: *network simulator, data transmission network, network simulator, routing, forced routing.*

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

Зеленохат Роман Александрович,
студент МТУСИ, Москва, Россия,
zelenohat-r@mail.ru

Иванюк Александр Викторович,
старший преподаватель кафедры ТЭОД, МТУСИ, Москва, Россия,
iav@rans.ru

Аннотация

Рассматриваются меры системного реагирования на риски по обеспечению доверия и безопасности при использовании ИКТ, основанные на учете междисциплинарного характера цифрового пространства, которое охватывает сферы технологий, права, психологии, социологии, экономики, политологии, дипломатии. Показано, что системное реагирование на безопасность ИКТ зависит от сотрудничества всех заинтересованных сторон, участвующих в управлении и контроле рисков несанкционированного доступа к ресурсам Интернета.

Ключевые слова: *сеть Интернет, глобальная система доменных имён (DNS), глобальная система маршрутизации, уязвимости, угрозы, атаки, методы защиты.*

В наши дни Интернет стал неотъемлемой частью жизни большей части мирового населения, однако процесс создания и развития глобальной сети известен лишь узкому кругу профильных специалистов. При этом, только зная историю эволюции Интернета можно понять современные проблемы в обеспечении доверия и безопасности при работе в сети.

Выделяют три основополагающие даты в истории создания сети Интернет. Первой датой считается 29 октября 1969 года. В этот день между университетом Калифорнии и Стэнфордским исследовательским институтом состоялась первая в мире передача данных с использованием коммутации пакетов (ранее использовалась коммутация каналов). Второй «день рождения Интернета» датирован 1977 годом, когда была впервые проведена первая серьёзная демонстрация Интернета как универсальной сети, способной объединить сети, использующие различные технологии (состоялся информационный обмен меду сетями ARPANET, SATNET и сетью пакетного радио). Третья дата связана с новым взглядом на архитектуру Интернета и протоколов IP и TCP и датируется 1980 годом, когда был опубликован документ RFC760, содержащий спецификацию IPv4 и базовую архитектуру Интернета, которые остались неизменными и по сей день [1].

Глобальная система доменных имён (DNS)

Работа сети Интернет не представляется возможной без глобальной системы доменных имён DNS (Domain Name System) и системы маршрутизации, обеспечивающей оптимальный путь прохождения пакетного трафика. Рассмотрим архитектурные особенности построения и возможные уязвимости этих двух основополагающих систем.

Роль DNS состоит в трансляции легких для запоминания человеком буквенных имён ресурсов сети Интернет в понятные для компьютеров IP-адреса. DNS представляет собой иерархическую и распределённую систему, которая не имеет единой базы данных, хранящей информацию обо всех доменных именах и связанных с ними IP-адресах. Система насчитывает более миллиона баз данных, в каждой из которых находится информация о конкретном домене. Преимущество такой архитектуры состоит в обеспечении уникальности каждого доменного имени и в качественном распределении нагрузки и ответственности за работу системы между администраторами отдельных доменов [2] .

В системе DNS существует три основных типа серверов:

1. Авторитетные серверы, которые напрямую работают с зонами.
2. Резолверы, которые обслуживают множество пользователей, выполняя за них трансляцию имён и кешируют полученные ответы для повышения производительности системы;
3. Резолверы-заглушки, которые преобразуют запрос приложения в DNS запрос и передают его серверу.

Для наглядного представления работы системы доменных имён будет рассмотрен процесс преобразования имени в связанный с ним IP-адрес посредством набора данных пользователем в окне браузера, который представлен на рисунке 1.

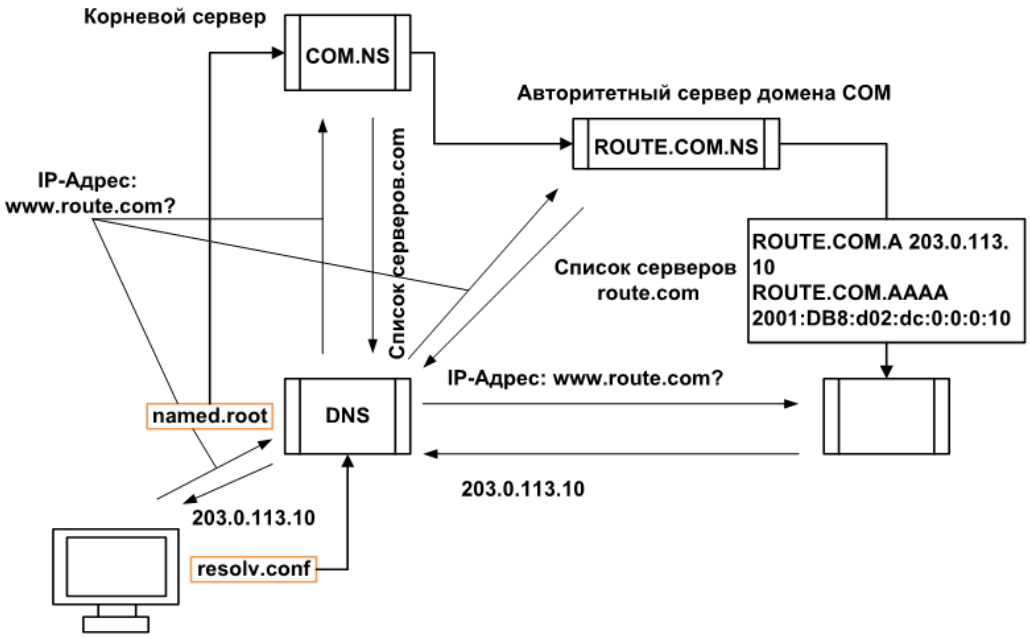


Рис. 1. Структурная схема процесса трансляции имён в DNS

Для создания TCP/HTTP соединения, в первую очередь, нужен IP-адрес сервера, который может получить браузер, обратившись к DNS-серверу с запросом: например, какой IP-адрес у сервера www.route.com?

Процесс разрешения имени состоит из нескольких этапов: для того чтобы пользователь получил конечный ответ нужно сузить круг поисков, а не опрашивать каждую зону. Для этого и предназначен итеративный резолвер, который в ответ на полученный запрос выдаёт конечный результат. Но существуют случаи, когда в кеше итеративного резолвера отсутствует информация по текущему запросу. Тогда резолвер определяет адреса серверов, обслуживающих корневую зону с помощью сравнения по специальному файлу, который называется hints. Этот файл содержит адреса 13 корневых серверов, на которые и будет перенаправлен запрос.

Поиск начинается с того, что резолвер посылает запрос одному из корневых серверов DNS. Эти серверы не располагают конечной, нужной пользователю информацией, но они могут указать с каким из серверов нужно связаться для её получения, в нашем примере это домен .com.

От одного из серверов домена .com резолверу поступает информация о нахождении адресов домена http://www.route.com, которые могут уже ответить на запрос о IP-адресе сервера www.route.com.

Любой процесс передачи данных имеет свои уязвимые места и соответствующие угрозы, и DNS не является исключением. Угрозы – это потенциальные атаки на DNS, которые возникают из-за наличия уязвимостей в системе. Угрозы могут нарушить функционирование, как самой системы, так и вывести её из строя на неопределённое время, что непосредственно влияет на работу Интернета. Угрозы, как и атаки на систему DNS можно разделить на две основные категории, а именно: на атаки отказа в обслуживании и атаки, связанные с подменой и модификацией данных в DNS [2,3].

Цель атак отказа в обслуживании (DoS-атак) – сделать недоступным разрешение имён для отдельных доменов, посредством генерации трафика в огромной количестве и направлении его на жертву, что приводит к нехватке ресурсов серверов доменов или всей инфраструктуры, которая обеспечивает работу. DoS-атаки могут привести к отказу в обслуживании всех дочерних доменов, а также к исчезновению самой зоны для обычных пользователей. DoS-атаки, которые имеют распределенные по сети источники генерации трафика, называются DDoS-атаками. DDoS атаки могут быть направлены против любого ресурса Интернета, но в данной атаке DNS может являться как жертвой, так и средством проведения атаки, а именно – атаки усиления.

Основной недостаток базового протокола DNS – это слабая система защита данных. В процессе передачи данных от сервера к клиенту, они могут подвергнуться изменению. Наглядное представление недостатка протокола и уязвимые места DNS приведены на рисунке 2.

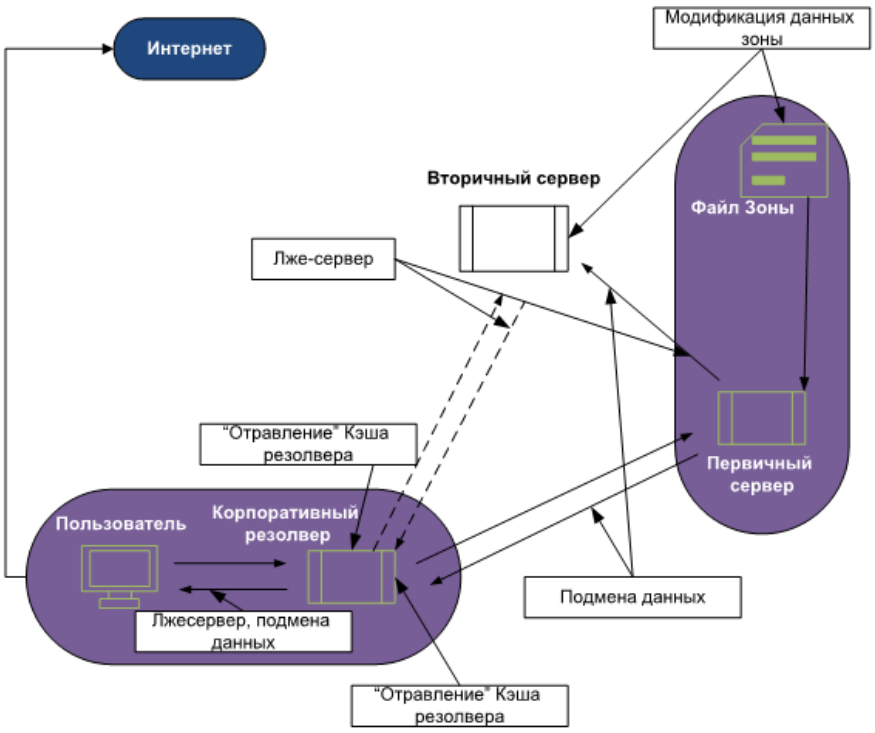


Рис. 2. Уязвимые места DNS

Из-за того, что злоумышленник потенциально может изменить данные в DNS, перед ним также открываются несколько вариантов дальнейшего развития атаки, в частности: создание ложного почтового сервиса, перехватывающего сообщения, которые, впоследствии, могут быть прочитаны злоумышленником; создание вебсайта, вводящего пользователя в заблуждение и вызывающего его доверие, вследствие чего злоумышленник потенциально может получить личную информацию пользователей, которые даже не будут подозревать, что сами отдали свои личные данные не в те руки.

Чтобы защитить систему DNS зная её уязвимые места и вариативность атак, специалисты по информационной безопасности разработали протокол, который стал расширением системы DNS – DNSSEC. Решая проблемы аутентичности и целостности данных, DNSSEC использует криптографию и является эффективным методом защиты от атак, которые связаны с подменой и модификацией данных DNS. DNSSEC позволяет пользователю убедиться, что полученные данные не были как-либо изменены в процессе передачи или публикации. Для защиты доступности информации также применяется технология ANYCAST.

Глобальная система маршрутизации

Аналогичным образом рассмотрим глобальную системы маршрутизации. Под маршрутизацией понимают определение маршрута пакетов от источника к получателю. В сети Интернет маршрут пакета состоит из большого количества участков. Определением участков, куда следует направить трафик, занимается маршрутизатор (роутер). Маршрутизатор связан со своими соседями (другими маршрутизаторами), обменивается с ними информацией и, таким образом, определяет оптимальный действующий в настоящее время путь следования пакета от источника к получателю. Преимущество данной архитектуры состоит в обеспечении автоматической проверки изменения топологии сети, а именно выхода из строя того или иного канала, узлов или целых сетей. Для наглядного представления архитектура процесса маршрутизации представлена на рисунке 3.

Неправильными маршрутами между связанными сетями являются маршруты, которые нарушают принцип valley-free (не пересекая долины). Маршрут может соответствовать принципу valley-free, когда он состоит из трёх последовательных участков, каждый из которых может быть нулевым (маршрут «в никуда», при котором пакеты идущие по этому маршруту игнорируются): движение в направлении клиент-провайдера, присутствует только один пиринговый линк и движение в направлении провайдер-клиента. В таком случае клиенты остаются клиентами, пиры – пирами, а провайдеры предоставляют оговоренный транзит [4].

Основным протоколом системы маршрутизации является BGP. Его суть состоит в том, что каждая сеть получает от своих соседей информацию о связанности, а именно через какую цепочку сетей доступен конкретный префикс (пул IP-адресов). Каждая сеть обрабатывает эту информацию и делается вывод о наилучшем для нее пути.

Рис. 3. Структурная схема процесса маршрутизации между автономными системами

Одной из особенностей протокола BGP является полное доверия соседям, которые в свою очередь доверяют своим соседям, что приводит к безоговорочному доверию внутри всей системы. Это существенно упрощает работу, но также вносит ряд уязвимостей в систему, таких как:

1. Отсутствие внутреннего механизма, обеспечивающего сильную защиту целостности, актуальности и аутентичности сообщений BGP, которыми обмениваются сети-пиры (сети-соседи) друг с другом;
2. Отсутствие механизма для проверки прав автономной системы или сети анонсировать префикс
3. Отсутствие механизма для проверки подлинности атрибутов пути, анонсированных сетью-пиром.

Векторы атаки на систему маршрутизации представлены на рисунке 4.

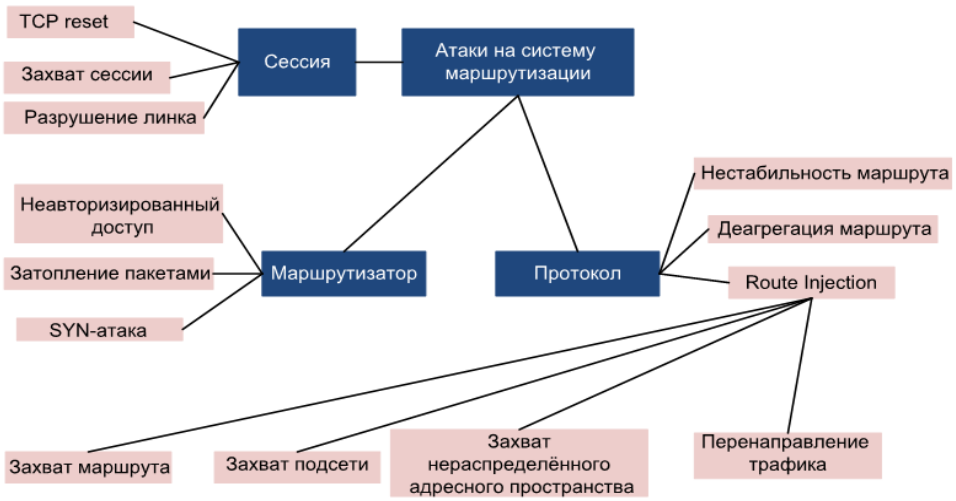


Рис. 4. Атаки на систему маршрутизации

Возможные атаки и их характеристики [1,3]:

1. **Создание чёрных дыр**, Цель атаки – отрезать сеть или несколько сетей от всего Интернета или его части. Весь трафик, который имеет отношение к этим сетям, перенаправляется и затем отбрасывается. Результатом становится то, что все сервисы, которое предлагаются данными сетями, становятся недоступными для пользователей.
2. **Перенаправление**. Цель атаки – доставка не предназначенного для данной сети трафика. Почти всегда эта сеть принадлежит атакующему и маскируется под атакуемую сеть, например для получения секретных данных. У перенаправления существует и другое предназначение, а именно проведение злоумышленниками крат-

косрочных акций, к примеру, рассылка спама. После проведения акции сеть или её копия исчезает. Злоумышленник в большинстве случаев пользуется не распределенным или не используемым адресным пространством.

3. **Перехват**. Атака направлена на кражу или изменение данных, поэтому её труднее обнаружить, чем обычную атаку, направленную на перенаправление трафика.

4. **Нестабильность**. Цель атаки данного вида - вынужденная фильтрация маршрутов сети провайдерами, в результате чего происходит нарушение связанности. Нестабильность в глобальной системе маршрутизации может быть вызвана частыми изменениями в анонсировании конкретной сети.

5. **Фабрикация источника трафика.** Обратный трафик направляется не к истинному получателю, а к получателю, чей адрес был сфабрикован. Целью атаки является не сама система маршрутизации, однако данный приём широко используется в рефлекторных атаках.

6. **Захват префикса.** Атака основана на использовании существующих уязвимостей в протоколе маршрутизации BGP для перенаправления или захвата трафика злоумышленником.

Чтобы защитить глобальную систему маршрутизации, зная её угрозы и уязвимые места, и вариативность атак, специалисты по информационной безопасности разработали технологию, которая стала расширением протокола BGP – BGPSEC. Аналогично DNSSEC, BGPSEC базируется на методах криптографической защиты и использует инфраструктуру открытых ключей ресурсов (RPKI).

Заключение

Само определение термина «Интернет» порождает споры, которые затем продолжаются в спорах об обеспечении доверия и безопасности работы в глобальной сети. Это не просто вопрос лингвистической аккуратности: различные оттенки смысла, вкладываемые в данный термин, порождают разные ожидания и подходы к выработке политического курса. Как правило, специалисты в области телекоммуникаций рассматривают проблему обеспечения доверия и безопасности при работе в сети Интернет сквозь призму технической инфраструктуры. Профессионалы в области компьютерных технологий в основном уделяют внимание разработке стандартов, языков и приложений. Специалисты по коммуникации делают акцент на упрощении обмена информацией. Активисты борьбы за права человека рассматривают вопросы безопасности с точки зрения свободы выражения убеждений, защиты тайны частной жизни и других основных прав человека. Юристы обращают внимание на вопросы юрисдикции и разрешения споров. Политиков и дипломатов в первую очередь беспокоит сам процесс регулирования и защита национальных интересов.

Вопросы обеспечения доверия и безопасности при работе в сети Интернет не ограничиваются только информационной безопасностью инфраструктуры сети. Они затрагивают права человека, социокультурные, экономические и нормативные правовые аспекты. Таким образом, только комплексный подход к обеспечению доверия и безопасности может служить залогом успеха функционирования ИКТ.

Литература

1. *Гуров В.В., Орлов В.Г.* Возможные уязвимости протокола MULTIPATH TCP // Телекоммуникации и информационные технологии. 2015. Т. 2. № 1. С. 45-48.
2. *А. Робачевский* Интернет изнутри, экосистема глобальной сети ООО “Альпина Паблишер”, 2015. 221 с.
3. Учебно-методическое пособие Основы технологий сети Интернет ООО “Фабрика Офсетной Печати”, 2019. 197 с.
4. *Йованн Курбалийя* Управление Интернетом, Опубликовано DiploFoundation, 2016. 390 с.

ISSUES OF ENSURING CONFIDENCE AND SECURITY WHEN OPERATING ON THE INTERNET

Roman A. Zelenokhat,
Student MTUCI, Moscow, Russia,
zelenohat-r@mail.ru

Alexander V. Ivanyuk,
Senior Lecturer, Department of TEOD, MTUCI, Moscow, Russia
iav@rans.ru

Abstract

Considered are measures of systemic response to risks to ensure trust and security in the use of ICT, based on the interdisciplinary nature of the digital space, which covers the spheres of technology, law, psychology, sociology, economics, political science, diplomacy. It is shown that a systemic response to ICT security depends on the cooperation of all stakeholders involved in the management and control of the risks of unauthorized access to Internet resources.

Keywords: *Internet, global domain name system (DNS), global routing system, vulnerabilities, threats, attacks, protection methods.*

МОДЕЛЬ КОНТЕЙНЕРА ДАННЫХ ДЛЯ МИНИМИЗАЦИИ ТРАФИКА ПРИ ПЕРЕДАЧЕ СУБЪЕКТИВНЫХ ХАРАКТЕРИСТИК ОБЪЕКТОВ НА ИЗОБРАЖЕНИИ ТРЕХМЕРНОЙ СЦЕНЫ

Кузин Иван Александрович,
магистрант МТУСИ, Москва, Россия,
IvanKuzin-forwork@yandex.ru

Гадасин Денис Вадимович,
доцент кафедры СИТиС, к.т.н, МТУСИ, Москва, Россия,
dengadiplom@mail.ru

Аннотация

Проблема понимания структуры объектов окружающего мира по их проекциям является одной из самых актуальных и прорабатываемых проблем, решаемых методами компьютерного зрении. Чаще всего такие системы реализуются посредством создания территориально распределенных комплексов, требующих передачу большого объема данных между их компонентами, что создает большую нагрузку на линии передачи. В статье рассматривается возможность минимизации объема данных, передаваемых по линиям связи путем хранения в виде единой структуры данных субъективных характеристик объектов объемной сцены, таких как цвет и глубина положения каждого пикселя, соответствующего объекту зафиксированной на нем сцены. Предложены модель контейнера данных и алгоритм его формирования.

Ключевые слова: *трехмерная реконструкция, компьютерное зрение, стереосопоставление, карта глубины, модель контейнера данных.*

С незапамятных времен человечество стало использовать изображения с целью долговременного хранения и последующей передачи информации. Применение данного метода представления данных не является случайностью и обусловлено особенностями работы зрительной системы человека, а также характером восприятия мозгом регистрируемой информации. Указанный вид организации информации наиболее легок для восприятия т.к. человек легко оперирует зрительными образами. Однако, применение двумерных проекций в качестве метода передачи информации по линиям связи имеет существенный недостаток: изображение не содержит в себе никакой явной информации о положении отображаемых объектов в пространстве. С развитием человеческого общества решение проблемы понимания структуры объектов реального мира, исходя из их двумерного представления, становится всё более актуальной.

Определение глубины расположения объектов объемной сцены

Современные методы восстановления субъективных характеристик объектов, зафиксированных на изображениях объемной сцены, позволяют с определенной точностью, обусловленной применяемыми подходами, алгоритмами и технической базой, восстанавливать структуру и параметры исходной сцены.

При решении задачи реконструкции объемной сцены основным этапом является получение информации о глубине расположения в пространстве всех видимых объектов. На данном этапе используются специальные программно-аппаратные комплексы, которые принято классифицировать на основе метода, применяемого для определения глубины расположения объектов. Согласно работам [2,3] они подразделяются на:

- системы, использующие устройства проецирования структурированного света;
- системы измерения времени полета света (ToF-сенсоры);
- системы, построенные на использовании стереоскопического эффекта.

Согласно многочисленным экспериментам, наиболее эффективной при использовании на открытых пространствах технологией является компьютерное стереозрение. Системы, основанные на данной технологии, имитируют работу зрительной системы человека, которая использует эффект горизонтального параллакса, проявляющегося в изменении видимого положения рассматриваемого объекта относительно удаленного фона при смене угла наблюдения [1]. Устройство фиксации изображения в таких системах представляет собой две камеры, зафиксированные таким образом, чтобы поля их обзора перекрывались на определенном расстоянии от точки наблюдения, а их положение относительно друга было выравнено. В результате работы систем, построенных на данном принципе, формируются изображения, на которых каждому пикселю соответствует небольшой участок пространства, а каждому объекту соответствует группа пикселей.

Процесс восстановления объемной сцены по последовательности её двумерных проекций обычно разбивают на следующий набор последовательных задач:

– стереосопоставление;

– получение пространственных структур по данным о глубине сцены.

На первом этапе производится оценка значения глубины для каждой точки сцены. В общем случае, для оценки глубины интересующего объекта трехмерной сцены необходимо выполнить следующие операции:

– определить ключевые атрибуты, такие как интенсивность цвета, координаты позиции на проекции и т.д. для каждой точки интересующего тела;

– провести попиксельное сопоставление изображений с целью нахождения их взаимного соответствия на каждой из проекций;

– сформировать карту глубины.

Задача установления ключевых атрибутов каждой точки объекта трудноразрешима по следующим причинами [4]:

– наличие на анализируемых изображениях световых бликов, размытия заслоненных областей на одном из изображений стереопары и других шумов;

– наличие на сцене объектов со сложной текстурой, которая дает «разрывы» глубины изобрпжеия при анализе.

Алгоритмы, позволяющие решить данные задачи с учетом отмеченных особенностей способов анализа изображения, подразделяются на два класса: локальные и глобальные. Первые, вычисляют смещение для каждого пикселя базового изображения, используя для корреляции прямоугольное окно фиксированного размера. При определении соответствия каждого пикселя производится сравнение локальных областей, находящихся в пределах окна. Алгоритмы, относящиеся к классу глобальных, в свою очередь, рассчитывают смещение сразу для всего изображения что позволяет добиться малого количества ошибок в вычислении глубины, но предполагает высокую сложность вычислений, и, как следствие, низкую скорость их выполнения, что не позволяет использовать алгоритмы данного класса при анализе видеопотока [3].

Задача поиска смещения пикселей изображений стереопары может быть формализована следующим образом: пусть для каждой точки поверхности, видимой на обоих изображениях, есть два луча в трехмерном пространстве, соединяющие её с центром проекции каждой камеры. Смещение представляет собой разность между положениями пикселей левого и правого изображения [3].

Геометрически процесс поиска смещения можно представить следующим образом (рис. 1). где: P – наблюдаемый объект; Z – расстояние до наблюдаемого объекта; O_l и O_r – центры камер; B – базовая линия; f – фокусное расстояние камеры; C_x^{left} и C_x^{right} -плоскости изображений с правой и левой камеры. X^L *и* X^R – проекции наблюдаемого объекта на соответствующую плоскость изображения; d_1 и d_2 – смещение точек X^L и X^R относительно центра фиксирующих их камер.

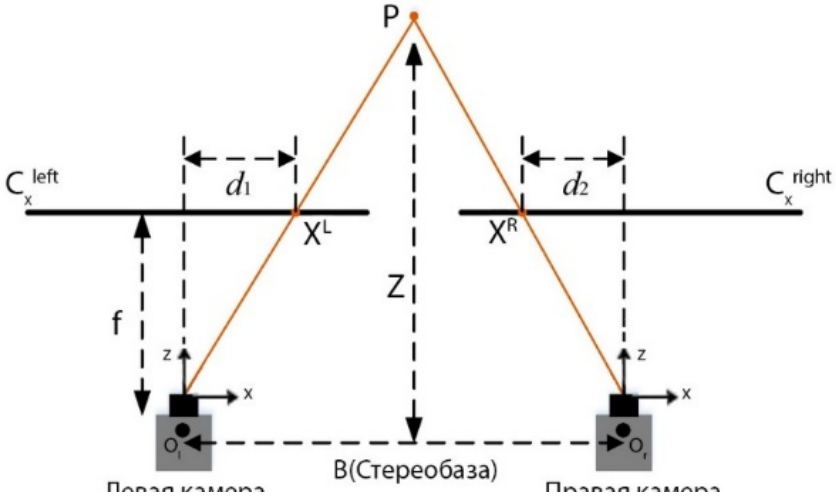


Рис. 1. Геометрическое представление наблюдаемой сцены

Тогда смещение точки P будет рассчитываться по формуле:

$$D_p = d_1 - d_2 \tag{1}$$

По итогу проведения операции сопоставления пикселей изображений, стереопары формируется особая текстура, называемая картой глубины. Она представляет собой изображение, интенсивность цвета каждого пикселя которого несёт информацию об удалённости соответствующего ему участка пространства от заданной точки наблюдения (рис. 2).

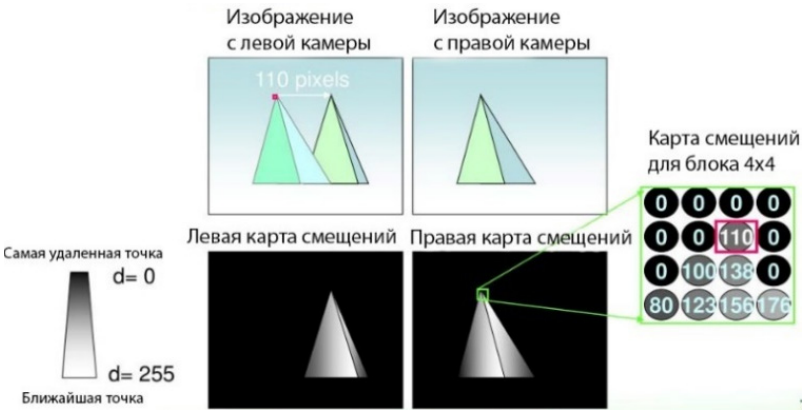


Рис. 2. Схема формирования карты глубины

При расчете глубины выполняется определение трехмерных координат точки сцены методом триангуляции. В общем случае, если известны величина базы между регистрирующими устройствами стереосистемы, а также расстояние их фокусировки, глубина изображения определяется по формуле:

— (2)

где: f – фокусное расстояние сенсоров; B – величина базы стереокамеры; D - величина смещения между точками проекций объекта трехмерной сцены в пикселях.

В соответствии с эффектом горизонтального параллакса, смещение точки обратно пропорционально её глубине [4]. Иллюстрация этой зависимость приведена на рис. 3.

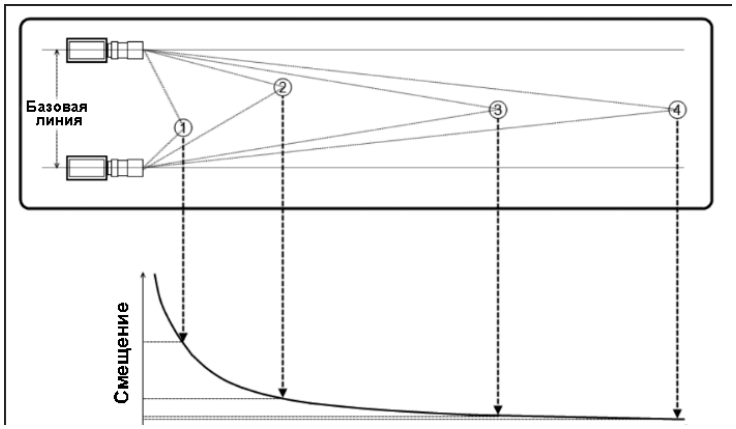


Рис. 3. Зависимость смещения наблюдаемого объекта от глубины изображения

Проблема согласования единиц измерения

Описанный метод восстановления субъективных характеристик объектов объемной сцены по её проекциям позволяет лишь приблизительно оценить характеристики реальных объектов [5]. Это обусловлено невозможностью достоверно определить реальные параметры объекта трехмерной сцены по изображению из-за отсутствия единой системы измерения. Во время своей работы рассматриваемая система одновременно находится в трех различных системах координат. Система координат, сформированная камерами и проективная система координат, описывают глубину изображения в пикселях, а мировая система координат описывает характеристики объекта в единицах метрической системы. Для сопоставления реальных параметров объекта его пиксельному представлению необходимо установить однозначную взаимосвязь его реальных параметров и его двухмерного представления, что требует дополнительных вычислений. При реализации систем бинокулярного компьютерного зрения в виде распределенных комплексов, по каналам связи приходится передавать большой поток разрозненных данных, включающий в себя базовое изображение сцены, карту глубины, матрицу смещений и другие данные, необходимые для получения трехмерной модели исходной сцены [3.4].

Целью данной работы является попытка решения задачи минимизации трафика путем формирования структуры данных, позволяющей хранить и передавать по каналам связи все субъективные характеристики объектов исходной сцены, а именно информацию о цвете каждого пикселя и об его удаленности от точки наблюдения в момент фиксации изображения.

Модель контейнера данных для хранения и передачи субъективных характеристик объектов трехмерной сцены

Системы бинокулярного компьютерного стереозрения работают с растровыми изображениями, которые представляют собой двумерный массив, описывающий характеристики каждой точки на изображении, а именно её цвет и положение на проекции [4]. Для описания цвета в компьютерной графике наиболее массовое применение получала аддитивная модель *RGB*. В указанной модели цвет каждого пикселя хранятся в виде трехмерного массива, и формируется путем смешивания базовых цветов модели. Указанная модель имеет широкое распространение благодаря своей простоте и универсальности, и получила большое количество модификаций, многие из которых имеют дополнительные каналы. В рамках данной работы, базируясь на модели *RGB,* предлагается сформировать специальный контейнер и использовать дополнительный канал для хранения информации о глубине каждого пикселя. В отличие от характерной для организации информации

4-байтового типа данных, выделяемого для описания цвета в каждом канале, в предлагаемом контейнере распределение данных реализовано таким образом, что одно 32-битное целое число без знака имеет выборку, определяющую глубину в 8-ми самых высоких битах, за которой следуют каналы, специфицирующие базовые цвета модели *RGB*. Для характеристики глубины значение 0 указывает на то, что пиксель максимально удален от точки наблюдения, а значение 255 определяет, что пиксель находится максимально близко к фиксирующему устройству.

Важной особенностью предлагаемой модели является возможность отражения глубины пикселя на изображении. Для этого необходимо использовать алгоритм смешивания с умножением (*premultiplied blending*) [5]. Смешивание цветов в рамках указанного алгоритма производится по формуле:

(3)

где: – цвет пикселя с учетом смешения; – исходный цвет пикселя; – значение глубины для текущего пикселя; – коэффициент прозрачности пикселя.

Таким образом, при формировании конечного изображения с учетом его глубины все пиксели, имеющие значение глубины равное 255 будут иметь исходный цвет. Пиксели, значение глубины которых стремиться к 0 будут иметь цвет, получившийся в результате смешивания исходного цвета и оттенка серого, интенсивность которого отражает удаленность данного пикселя от точки наблюдения.

Также следует отметить временную сложность и быстродействие алгоритмов, обеспечивающих работу с данной моделью. Для получения информации о глубине каждого пикселя на изображении достаточно знать его позицию и изъять значение первого байта. Такой подход позволяет обеспечить совместимость с алгоритмами компьютерного зрения, для которых требуется карта глубины в виде отдельной структуры данных. В худшем случае временная сложность алгоритма, извлекающего информацию о глубине пикселей всего изображения, составит O(n), так как он имеет линейное время работы.

Кроме этого, сама операция сборки информации о субъективных характеристиках объектов объемной сцены в единый контейнер, хотя и требует дополнительных операций, в конечном счете, уменьшает время обработки данных на сервере, так как не нужно производить повторного сопоставления карты глубины и базового изображения. Также передача данных по линиям связи в виде единого контейнера позволит снизить вероятность частичной потери информации о глубине.

Схема модели представления характеристик пикселя на изображении приведена на рисунке 4.

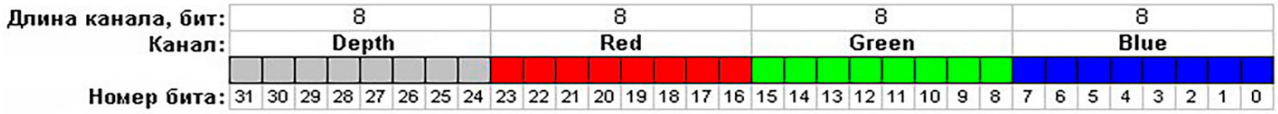


Рис. 4. Схема модели представления характеристик пикселя на изображении

Таким образом, в общем виде алгоритм формирования изображения, соответствующего предложенной модели включает:

1. Получение двух проекций трехмерной сцены с разных точек наблюдения, обусловленных положением сенсоров стереокамеры;
2. Проведение стереосопоставления и формирование карты глубины;
3. Создание структуры данных и занесение в нее информации о субъективных характеристиках каждого пикселя объектов исходного изображения;
4. Сохранение полученного изображения в виде файла для дальнейшей его обработки.

Достоинствами данного подхода, по мнению авторов, являются:

- Простота и наглядность модели: каждой точке пространства, зафиксированной на проекции, соответствует визуально воспринимаемый цвет и характеристика глубины, что позволяет дополнять проекцию для лучшего понимания структуры и характеристик сцены;

- Отсутствие необходимости хранить карту глубины в отдельной структуре, что ведет к некоторой экономии вычислительных ресурсов;
- Возможность распространения изображения и информации о характеристиках его глубины в виде единого объекта (файла), а не в виде набора изображений (проекция + карта глубины);
- Линейная временная сложность алгоритма извлечения глубины изображения.

Реализация предлагаемого контейнера позволит повысить удобство работы по формированию данных о конечном изображении и может найти применение в системах компьютерного зрения, в которых используется информация о глубине сцены.

Заключение

Анализ существующих алгоритмов восстановления характеристик объемных сцен показал, что, несмотря на все многообразие подходов к оценке глубины сцены, одним из наиболее эффективных методов анализа окружающего пространства на открытых территориях является метод, основанный на использовании системы стереозрения. Такие системы нашли применение в различных отраслях человеческой деятельности. Тем не менее, несмотря на высокую популярность, указанные системы не позволяют выгружать результаты своей работы в удобной форме для последующего их анализа или распространения.

Предложенная модель представления информации о субъективных характеристиках зафиксированных на изображении объектов трехмерной сцены в виде единого контейнера данных позволяет повысить удобство хранения, распространения и обработки этих данных, как непосредственно внутри самих систем компьютерного зрения, так и при реализации самостоятельных приложений

Литература

1. *Лукашевич М.М., Садыхов Р.Х.* Цифровая обработка сигналов и изображений: лабораторный практикум для студ. спец. I-400201 «Вычислительные машины, системы и сети» всех форм обуч.» Минск: БГУИР, 2010.

2. *Davies E.R.* Machine Vision: Theory, Algorithms, Practicalities. 3rd ed. Morgan Kaufmann, 2004. 968 p.

3. *Scharstein D., Szeliski R.* A Taxonomy and Evaluation of Dense Two-Frame Stereo Correspondence Algorithms // International Journal of Computer Vision. April 2002. Pp. 7-42.

4. *Jian Sun, Nan-Ning Zheng and Heung-Yeung Shum.* Stereo matching using belief propagation // IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 7, pp. 787-800, July 2003, doi: 10.1109/TPAMI.2003.1206509.

5. *Thomas Porter and Tom Duff.* Compositing digital images // Proceedings of the 11th annual conference on Computer graphics and interactive techniques (SIGGRAPH '84), 1984, Association for Computing Machinery, New York, NY, USA, pp. 253-259.

DATA CONTAINER MODEL FOR MINIMIZING TRAFFIC WHEN TRANSMITTING SUBJECTIVE CHARACTERISTICS OF OBJECTS IN THE IMAGE OF A THREE-DIMENSIONAL SCENE

Ivan A. Kuzin,
Graduate MTUCI, Moscow, Russia,
IvanKuzin-forwork@yandex.ru

Denis V. Gadasin,
Associate Professor of NITES department, Ph. D., MTUCI, Moscow, Russia,
dengadiplom@mail.ru

Abstract

The problem of understanding the structure of objects of the surrounding world by their projections is one of the most relevant and studied problems solved by computer vision methods. Most often, such systems are implemented by creating geographically distributed complexes that require the transfer of a large amount of data between their components, which creates a large load on the transmission lines. In this paper, we consider the possibility of minimizing the amount of data transmitted over communication lines by storing in a single data structure the subjective characteristics of objects in a three-dimensional scene, such as the color and depth of the position of each pixel corresponding to the object of the scene fixed on it. The article offers a model of the data container and offers an algorithm for the formation of the specified container.

Keywords: *Three-dimensional reconstruction, Computer vision, Stereo mapping, Depth map, Data container model.*

ПОДСИСТЕМА ПОДГОТОВКИ ДАННЫХ ДЛЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА РАСПОЗНАВАНИЯ ЖЕСТОВОГО ЯЗЫКА

Шакиров Ренат Ильдарович,
магистрант МТУСИ, Москва, Россия,
shakirovrenat@list.ru

Артемов Михаил Денисович,
аспирант кафедры ИСУиА, МТУСИ, Москва, Россия,
artemov_mikle@mail.ru

Воронова Лилия Ивановна,
заведующий кафедрой ИСУиА, д.ф.-м.н., профессор, МТУСИ, Москва, Россия,
voronova.lilia@ya.ru

Аннотация

В статье описывается разработка подсистемы обработки и подготовки данных программно-аппаратного комплекса (ПАК) по распознаванию жестового языка инвалидов с нарушениями слуха и речи. Произведён анализ продуктов-аналогов по автоматическому сурдопереводу, сформулированы технические и конструктивные требования к программно-аппаратному комплексу, описана архитектура ПАК на основе микросервисного подхода. Приведены результаты проектирования и частичная реализация подсистемы наполнения и обработки фото-видео материалов жестового языка, а также базы метаданных и хранилища данных. Описаны соответствующие сценарии и алгоритмы. Приведены примеры детектирования руки на изображении.

Ключевые слова: *распознавание образов, жестовый язык, нейросетевые технологии, программно-аппаратный комплекс, микросервисная архитектура.*

Введение

В последние годы активно решается проблема социальной адаптации людей с ограниченными возможностями с использованием разработок, использующих методы искусственного интеллекта**.** По данным «Всемирная организация здравоохранения» в мире более 460 миллионов человек имеют проблемы со слухом, включая полную потерю, при этом из них более 34 миллионов детей. При сохранении нынешней тенденции согласно оценкам экспертов, к 2050 году таких людей будет более 900 миллионов человек [1]. В России доля слабослышащих и глухих людей составляет около 10% от общего населения страны, то есть более 14 миллионов человек. Частичная или полная потеря слуха ведет к проблемам интеграции в общество и повышению уровня безработицы среди данной группы людей.

Решением задачи адаптации людей, имеющих проблемы со слуховым и речевым аппаратами, может служить использование жестового языка. Язык жестов построен только на жестикуляторно-мимической основе и, при прочих равных условиях, он не уступает звучащим языкам [2].

Множество компаний работают над разработкой продуктов, которые помогают осуществить автоматический перевод жестового языка:

- *MotionSavvy* – продукт от одноименной компании разработанный в 2015 году, обеспечивает двусторонний перевод от глухого к слышащему, и наоборот. Устройство состоит из планшетного компьютера, микрофона и *Leap Motion*. Устройство захватывает движение рук пользователя для распознавания жестов, после чего обозначение распознанных жестов выводится на экран планшетного компьютера в виде текста. Продукт позволяет распознать более 100 английских слов и около тысячи жестов. Русский жестовый язык не поддерживается, а стоимость устройства начинается от 600 долларов [3].
- *Arrm.io* – белорусский стартап 2018 г. по распознаванию жестового языка для автоматического сурдоперевода. Для распознавания жестов необходим персональный компьютер\ноутбук с *RGB*-камерой [4]. Распознавание происходит с помощью нейросетевой технологию *Deep Sign* [5]. Эта нейросетевая технология базируется на собственной архитектуре с методологией one-shot learning, что означает обучение нейронной сети по минимальному датасету. Из-за высокой сложности интерпретации жестового языка, а также большой зависимости от контекста ситуации, разработчиками было решено развивать продукт на основе увеличения семантических полей по узким тематикам. Например, прием в больнице, обращения в банк, в страховую компанию и др.

• *Google AI* – компания опубликовала в 2019 году один из новых подходов для отслеживания рук в режиме реального времени с помощью в системе *MediaPipe* [6], состоящий из взаимодействия нескольких моделей: модель детектора, модель разметки ладони, модель распознавания жестов. Средняя точность обнаружения рук/ладоней в реальном времени составляет 95,7%.

• Миелофон [7] – разработка от российского школьника Даниила Казанцева, предназначена для интерпретирования языка жестов чтобы заменить сурдопереводчика, проект получил премию *Lego Education Builder* в 2019 году от компании *Google*. Разработка базируется на технологии электромиографии, которая распознает электромеханическую активность мышц [8]. Для проверки функционирования разработки использовали пять жестов *American Sign Language (Hello, Yes, No, Please, I love you)*. В испытаниях участвовали три человека, включая создателя. Чтобы проверить эффективность системы каждый из участников проделал по 10 попыток для одного жеста. Проверка показала, что система распознает данные жесты с точностью 92,6%.

На кафедре «Интеллектуальные системы в управлении и автоматизации» МТУСИ ведутся научно-исследовательские работы по созданию программ с применением методов машинного обучения для поддержки людей с нарушениями слухового и речевого аппаратов. Результаты исследований приведены в [9-13, 16-18].

Технические и конструктивные требования к программно-аппаратному комплексу

Разрабатываемый программно-аппаратный комплекс (ПАК) при помощи видеокамеры устройства (смартфона, планшета, ноутбука) и программных средств интеллектуальной обработки данных должен выполнять распознавание жестового языка слабослышащих.

Инновационность разработки заключается в использовании технологий компьютерного зрения и машинного обучения, которые, основываясь на новейших разработках в области интеллектуального анализа данных, существенно повысят эффективность системы социальной коммуникации для инвалидов по слуху.

ПАК включает: *web*-приложение с графическим пользовательским интерфейсом и сервер приложений, где будет расположена нейронная сеть, выполняющая распознавание; сервер базы данных и файловое хранилище, служащее для хранения изображений жестов, которые в будущем понадобятся для дообучения нейронной сети. В устройстве пользователя должна быть видеокамера.

Сценарий работы системы: видеозапись с жестами слабослышащего, полученная с видеокамеры на стороне клиента преобразуется в набор кадров (изображений), которые по сети Интернет передаются на сервер приложений; сервер приложений, получив последовательность изображений, должен выполнить их предобработку и передать на вход нейронной сети, которая на выходе предскажет какой жест изображён пользователем; полученное предсказание преобразуется сервером в формат *JSON* и отправляется обратно на устройство пользователя, где отобразится в графическом интерфейсе пользователя.

Обучение нейронной сети, предназначенной для распознавания жестов, должно проводиться на специально разработанном наборе данных, в который войдут изображения и видеозаписи жестов. Обучение будет проводится с использованием графического процессора. В дальнейшем для улучшения точности предсказания нейронная сеть будет дообучаться на изображениях или видеозаписях жестов, полученных в ходе эксплуатации системы пользователями.

Архитектура ПАК распознавания жестового языка

На основе функциональных требований к программно-аппаратному комплексу автоматического распознавания жестового языка была спроектирована аппаратная архитектура. Комплекс представляет собой совокупность программных и аппаратных средств, предоставляющих возможность распознавания жестового языка с различных клиентских устройств. Размещение ПАК возможно, как локально, используя программно-аппаратные средства организации, так и удаленно в дата-центре. В случае удаленного размещения ПАК клиентское приложение размещается на устройстве пользователя. Аппаратная архитектура ПАК представлена на рисунке 1.

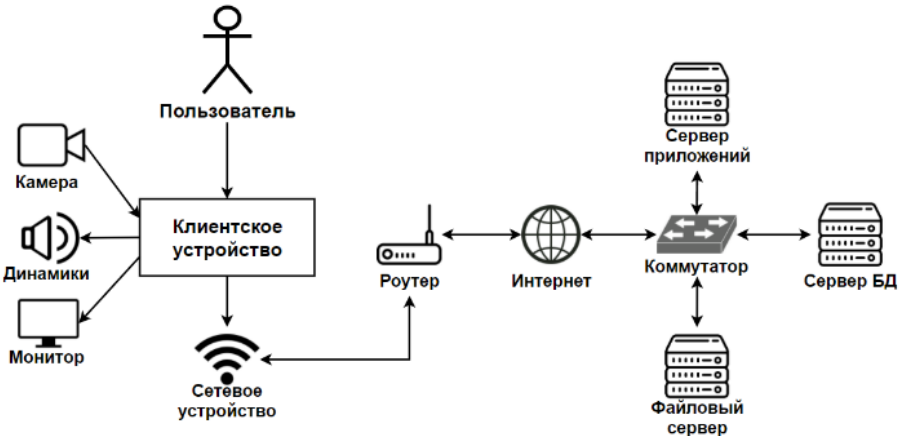


Рис. 1. Аппаратная архитектура ПАК по распознаванию жестового языка

Назначение элементов аппаратной архитектуры ПАК приведено в таблице 1.

Таблица 1

Элементы аппаратной архитектуры ПАК

Устройство	Назначение
Клиентское устройство	Управление устройствами ввода и вывода, использование клиентского приложения
Камера	Захват изображения движения рук
Динамики	Звуковое воспроизведение результатов распознавания
Монитор	Отображение графического интерфейса приложения
Сетевое устройство	Подключение клиентского устройства к сети Интернет
Роутер	Выход в сеть Интернет
Коммутатор	Объединение серверов в *LAN*
Сервер приложений	Программное обеспечение приложений и взаимодействия серверов
Сервер БД	Обеспечение хранения и обработки баз данных
Файловый сервер	Обеспечение хранения и обработки набора данных

В роли клиентского устройства может выступать персональный компьютер, ноутбук, смартфон или планшет.

Камера, динамики, монитор, сетевое устройство подключены к пользовательскому устройству для взаимодействия с клиентским приложением и обеспечения записи, обработки и передачи информации на серверное оборудование по сети Интернет.

ПАК имеет распределенную структуру серверов приложений, базы данных и файлового хранилища. В зависимости от требований они могут располагаться как на одном физическом сервере, так и на разных серверах.

На основе функциональных требований и разработанной аппаратной архитектуре ПАК была спроектирована программная архитектура. Программная архитектура включает в себя клиентское и серверное обеспечение, (рисунок 2).

В клиентское программное обеспечение входит *WEB*-клиент для браузера, который отвечает за графический интерфейс и функции ввода и вывода, система распознавания жестового языка и система пополнения хранилища данных (ХД) и базы метаданных (БД).

Серверное программное обеспечение состоит из системы распознавания жестового языка, системы пополнения хранилища данных и базы метаданных, системы обучения нейронных сетей (НС) для распознавания жестового языка, базы метаданных и хранилища данных.

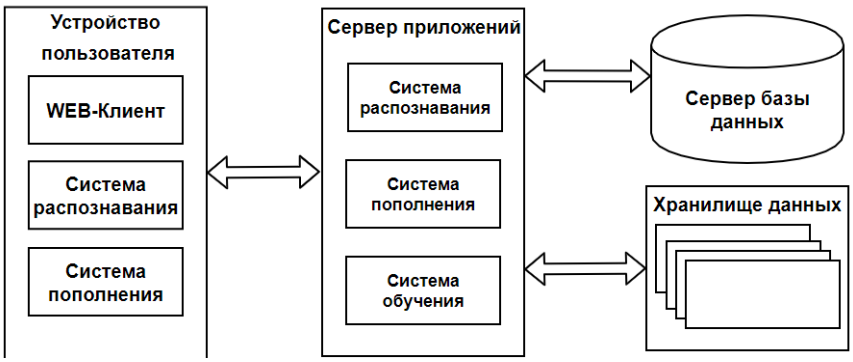


Рис. 2. Программная архитектура ПАК по распознаванию жестового языка

Для детального проектирования и разработки ПАК выбрана микросервисная архитектура, которая в отличие от общей модели клиент-серверной архитектуры, ориентирована на более слабую связность модулей. Это означает отказ от монолитной структуры приложения. Модули или подсистемы комплекса являются независимыми сервисами, которые взаимодействуют по сети. Сервисы могут быть реализованы на разных технологиях и языках программирования.

В микросервисном подходе выделенные ранее подсистемы являются сервисами как показано на рисунке 3:
• Сервис «*WEB*-клиент»;
• Сервис «Распознавание жестового языка»;
• Сервис «Пополнение ХД и БД»;
• Сервис «Обучение НС»;
• База данных;
• Хранилище данных.

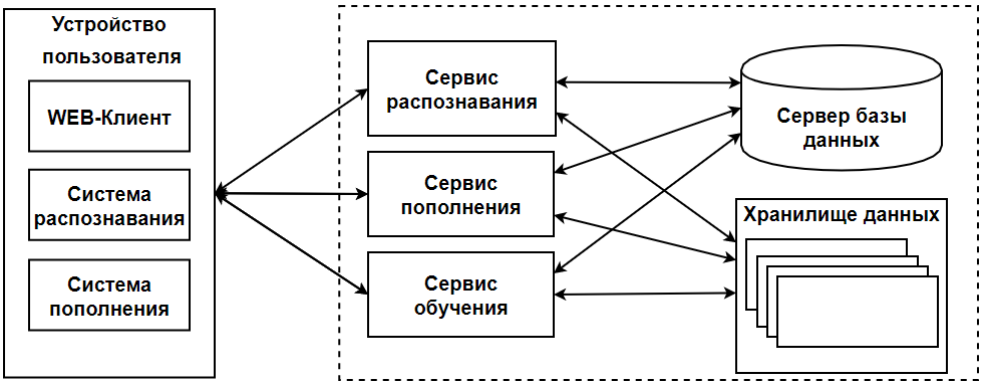


Рис. 3. Микросервисная архитектура ПАК по распознаванию жестового языка

Сервис «*WEB*-клиент» отвечает за клиентское веб-приложение, отображение пользовательского интерфейса и взаимодействие с другими сервисами ПАК такими как: «Распознавание жестового языка» и «Пополнение ХД и БД».

Сервис «Распознавания жестового языка» включает нейронные сети для распознавания жестового языка. Пользователь через сервис «*WEB*-клиент» записывает жесты и их данные передаются в сервис «Распознавание жестового языка», где происходит распознавание жеста. Результат распознавания передается обратно в сервис «*WEB*-клиент» и отображается у пользователя на экране в виде текстового обозначения жеста.

Сервис «Обучения НС» предоставляет функционал обучения нейронных сетей. Данный сервис связан с хранилищем данных и базой данных, где хранятся обучающие данные, а также с сервисом «Распознавание жестового языка».

Сервис «Пополнения ХД и БД» несет функционал пополнения хранилища данных и базы данных новыми обучающими данными для обучения нейронных сетей. Пользователь записывает жест в сервисе «*WEB*-клиент» и данные передаются в сервис «Пополнение ХД и БД». После проверки переданных данных они сохраняются в хранилище данных и базе данных.

Проектирование сервиса обучения НС

Сервис «Обучения НС» отвечает за обработку накопленных данных из сервиса «Пополнения ХД и БД» и подготовку обучающего набора данных, пригодного для последующего обучения нейронных сетей.

Для обучения нейронных сетей необходимо подготовить исходные изображения из сервиса «Пополнения ХД и БД» и преобразовать изображения в необходимый формат с разметкой по относительным классам данного изображения. Для этого необходимо определить, сколько входных нейронов будет у НС.

Исходные изображения жестов сохранены в цветном формате, а для распознавания жестов нет необходимости в цветном изображении. Для включения в набор данных максимума полезной информации и сокращения информационного блока, изображение может быть преобразовано в оттенки серого.

Исходные изображения жестов также могут содержать на снимке не только жестикуляцию, но и самого человека и посторонний фон. Данные элементы не несут полезной информации для обучения и распознавания, и поэтому для создания набора данных необходимо производить поиск области с жестикуляцией на изображении с выделением и сохранением данной области.

Для выбора размеров изображения с областью жеста (только руки и кисти без посторонних объектов) были проанализированы другие известные наборы данных, такие как: *MNIST* [14] – состоит из 10 классов, размеры изображений 32x32 *px*, изображения содержат оцифрованные рукописные цифры от 0 до 9; *CIFAR-10* и *CIFAR-100* [15] – состоят из 10 и 100 классов соответственно, имеют размеры обучающих изображений 32x32 *px*, изображения содержат снимки автомобилей, людей, животных, цветов, фруктов и тому подобное. На основании анализа полного набора данных был сделан вывод, что для классификации изображений достаточно использовать размер 32x32 *px*. Если в дальнейшем для увеличения количества распознаваемых жестов размера

32x32 *px* будет недостаточно или появится другая причина, то размеры области могут быть увеличены произвольно, а обучающий набор подготовлен снова в автоматическом режиме.

Следующим шагом после преобразования изображения в оттенках серого и на нём найдена и уменьшена до размеров 32x32 *px* область с жестом, будет преобразование изображения в массив (вектор). Вектор должен

представлять одномерный массив длиной равной 2 + 32*32 = 1026, где первое значение является *id* жеста (название жеста), а последующие 1024 – соответствуют пикселям выделенной области, значение которых могут изменяться от 0 до 255 (0 – черный цвет, 255 – белый цвет).

Подготовленный обучающий набор данных сохраняется в формате *CSV* с разделителем запятая, а каждая строка в файле соответствует одному обучающему примеру.

Алгоритм подготовки обучающего набора данных приведён рисунке 4. Он включает:

1. Загрузку изображений;
2. Преобразование изображений в градациях серого;
3. Обнаружение области с рукой и кистью;
4. Уменьшение размера обнаруженной области до размеров 32x32;
5. Преобразование полученного изображения ранее в массив данных с длиной массива 1026;
6. Сохранение полученных данных в файл с форматом *CSV*.

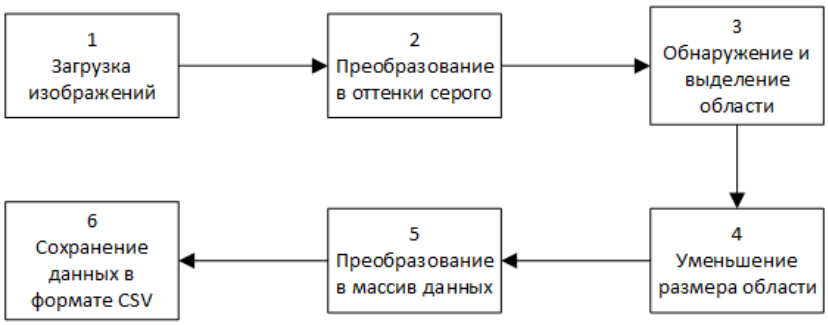


Рис. 4. Алгоритм подготовки обучающего набора данных

Разработка сервиса обучения НС

Задача реализации системы автоматического распознавания жестового языка связана с разработкой спроектированных сервисов, а именно: функционала разграничения пользовательского доступа, сервиса пополнения хранилища данных и базы метаданных, сервиса обучения нейронных сетей, сервиса распознавания жестового языка.

Исходя из составленных требований к программно-аппаратному комплексу, система должна иметь пользовательский интерфейс, позволять интегрировать различные модули распознавания, а также иметь функционал пополнения обучающего набора новыми данными.

Все вышеперечисленные сервисы и функциональные возможности могут быть реализованы совершенно на разных языках программирования и с применением различных технологий.

Таким образом, для объединения сервисов в одну систему и обеспечения взаимной работоспособности друг с другом её составляющих необходимо предусмотреть унифицированный подход в реализации API сервисов для взаимодействия и обмена данных.

Для реализации сервисов «*WEB*-клиент», «Пополнение ХД и БД» и «Распознавание жестового языка» выбран фреймворк *Spring Boot (Java)*, который позволяет быстро развернуть *web*-приложения, сокращая длину кода и упрощая разработку самого приложения, а для отображения пользовательского интерфейса используется *thymeleaf* – серверный механизм *Java*-шаблонов, который позволяет обрабатывать *HTML*, *CSS*, *JS*.

Для реализации базы метаданных выбрана *PostgreSQL* – объектно-реляционная система управления базами данных, главными преимуществами которой является бесплатность использования, не ограниченный максимальный размер базы данных и др.

Для реализации сервиса «Обучение НС» выбраны: язык программирования *Python*; библиотеки *OpenCV*, *NumPy* и фреймворк *MediaPipe* для работы и обработки изображений, детектирования области с рукой на снимке, а также фреймворк *Flask* для создания *web*-сервиса. Данный сервис не предусматривает пользовательского интерфейса, взаимодействие пользователя с сервисом происходит через сервис «*WEB*-клиент».

В сервисе «Обучение НС» реализовано два *HTTP* метода:

- *POST: /api/v1/outline* – метод служит для детектирования области руки с жестом, а также для преобразований выделенной области и выделения контуров руки. В теле запроса необходимо послать список *id* изображений жестов.
- *POST: /api/v1/csvfile* – метод служит для преобразования картинок жестов руки, которые были получены с помощью метода */api/v1/outline*, в *csv* файл для дальнейшего обучения нейронных сетей.

Реализованный сервис был протестирован в составе программно-аппаратного комплекса с сервисами «*WEB*-клиент», *«Пополнение ХД и БД»* (рис. 5).

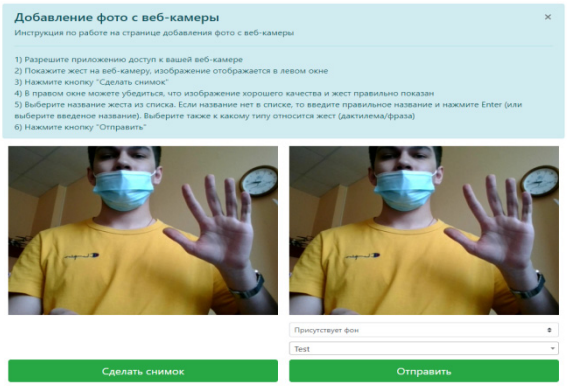


Рис. 5. Пополнение базы и хранилища данных снимками

Изображения, снятые и загруженные в хранилище данных *Amazon S3*, были успешно переданы в сервис «Обучения НС», где проведена детекция области с рукой и дальнейшие преобразования изображения (рис. 6).

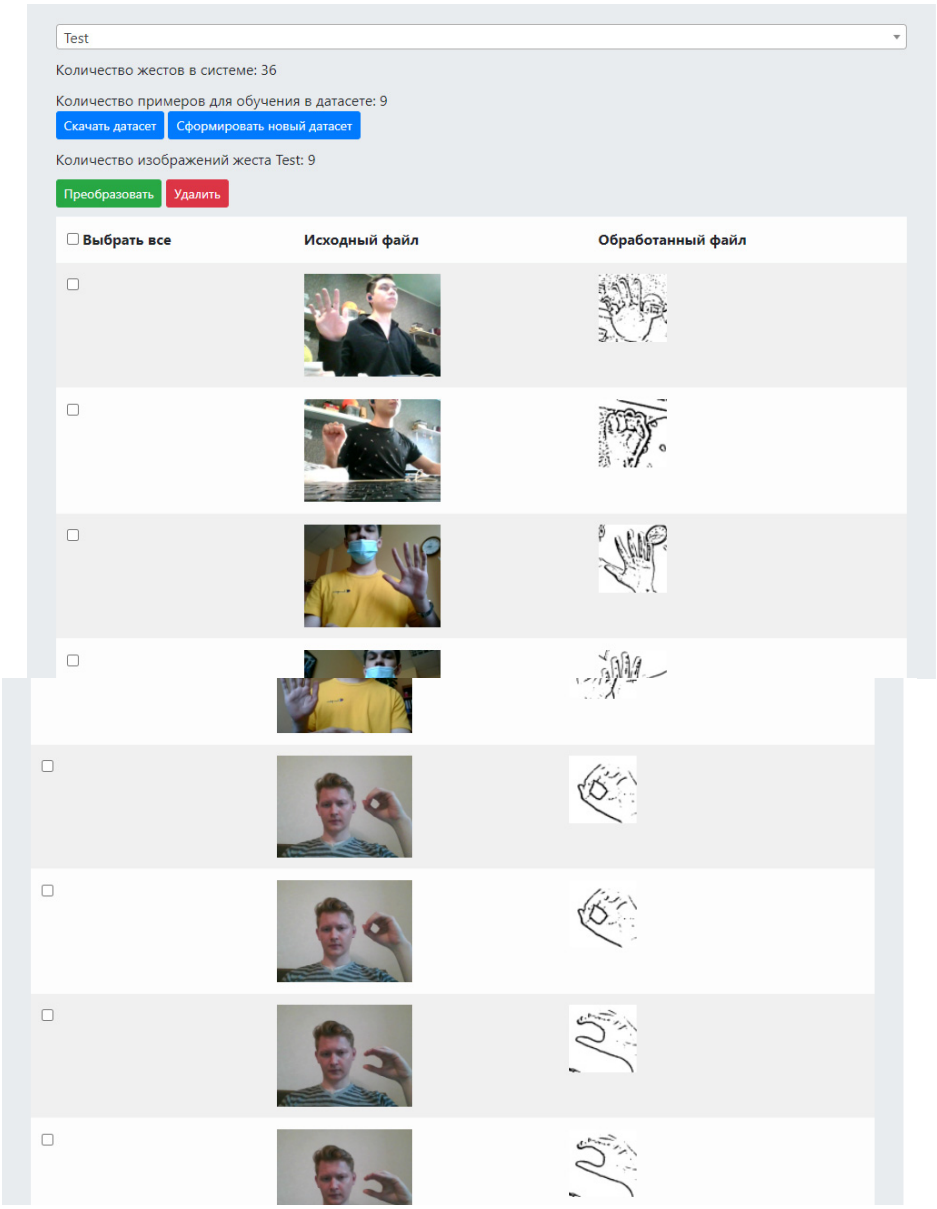


Рис. 6. Детекция руки и преобразование изображения

На выходе получаем область с контурами жеста, которые в дальнейшем можно преобразовать и записать в *csv* файл для обучения нейронных сетей (рис. 7).

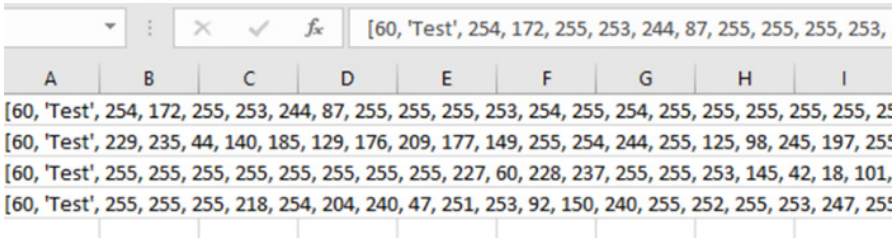


Рис. 7. *CSV* файл с изображениями жестов

Заключение

На основе анализа аналогов систем для автоматического распознавания жестового языка, выявлено, что в свободном доступе полноценные эффективные решения данного сервиса отсутствуют. Исходя из функциональных требований к системе её реализация, помимо наличия пользовательского интерфейса и программно-аппаратного комплекса, должна обеспечивать интеграцию различных модулей распознавания, а также иметь функционал пополнения обучающего набора новыми данными. Данные функциональные возможности и сервисы могут быть реализованы на разных языках программирования и с применением различных технологий.

Литература

1. Глухота и потеря слуха [Электронный ресурс] // Всемирная организация здравоохранения URL: https://www.who.int/ru/news-room/fact-sheets/detail/deafness-and-hearing-loss (дата обращения: 15.07.2020).

2. *Воскресенский А.Л.* Непризнанный язык (Язык жестов глухих и компьютерная лингвистика) // Труды Международного семинара «Диалог – 2002». Т. 2. Протвино, 2002. С. 100-106.

3. Giving Deaf People a Voice: MotionSavvy's Real-Time Sign Language Translation [Электронный ресурс] // URL: http://blog.leapmotion.com/ giving-deaf-people-a-voice-motionsavvys-real-time-sign-language-translation/ (дата обращения: 15.07.2020).

4. Deep sign – универсальная технология распознавания жестов [Электронный ресурс] // vc.ru — бизнес, технологии, идеи, модели роста, стартапы URL: https://vc.ru/tribuna/38876-deep-sign-universalnaya-tehnologiya-raspoznavaniya-zhestov (дата обращения: 14.07.2020).

5. *Jai Shah* Deepsign: A Deep-learning Architecture For Sign Language Recognition: Texas, 2018.

6. On-Device, Real-Time Hand Tracking with MediaPipe [Электронный ресурс] // Google AI Blog URL: https://ai.googleblog.com/2019/08/on-device-real-time-hand-tracking-with.html (дата обращения: 15.07.2020).

7. Школьник из России выиграл конкурс Google за разработку переводчика с языка жестов [Электронный ресурс] // Neurohive - Нейронные сети URL: https://hi-news.ru/technology/shkolnik-iz-rossii-vyigral-konkurs-google-za-razrabotku-perevodchika-s-yazyka-zhestov.html (дата обращения: 31.03.2020).

8. *Гриф М.Г., Козлов А.Н.* Сравнительный Анализ Программно-аппаратных Средств В Задачах Распознавания Жестовой Речи // Сборник Научных Трудов Новосибирского Государственного Технического Университета. 2014. №3.

9. *Artemov M. D., Voronova L. I., Vovik A. G.* Designing Soft-Hardware Complex for Gesture Language Recognition using Neural Network Methods // 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, 2020, pp. 1-6, doi: 10.1109/EMCTECH49634.2020.9261564

10. *Trunov A. S., Voronova L. I., Voronov V. I., Sukhachev D. I., Strelnikov V. G.* Legacy applications model integration to support scientific experiment // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 2018, pp. 1-7.

11. *Voronov V. I., Genchel K. V., Voronova L. I., Travina M. D.* Development of a Software Package Designed to Support Distance Education for Disabled People // 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), St. Petersburg, 2018, pp. 746-751, doi: 10.1109/ITMQIS.2018.8524958.

12. *Goncharenko A. A., Voronova L. I., Voronov V. I., Ezhov A. A., Goryachev D. V.* Automated support system designing for people with limited communication // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 2018, pp. 1-7.

13. *Artem A. Goncharenko, Lilia I. Voronova , Mikhail D. Artemov, Vjacheslav.I.Voronov, Danil N.Bezumnov* "Sign Language Recognition Information System Development Using Wireless Technologies for People with Hearing Impairments" 24th Conference of Open Innovations Association FRUCT, Moscow, Russia, 8-12 April 2019

14. База данных рукописных цифр MNIST URL: http://yann.lecun.com/exdb/mnist/ (дата обращения: 20.04.2021).

15. CIFAR-10 and CIFAR-100 datasets // Alex Krizhevsky URL: https://www.cs.toronto.edu/~kriz/cifar.html (дата обращения: 20.04.2021).

16. *Мартынов Д.А., Воронова Л.И.* Применение перцептрона для распознавания дактилем русского жестового языка // DSPA: Вопросы применения цифровой обработки сигналов. 2020. Т. 10. № 2. С. 37-46.

17. *Артемов М.Д., Воронова Л.И.* Разработка подсистемы распознавания простых динамических жестов с помощью 3DCNNLSTM // Телекоммуникации и информационные технологии. 2019. Т. 6. № 1. С. 150-154.

18. *Клешнин Н.Г., Воронова Л.И.* Применение нейронных сетей в подсистеме распознавания эмоций для проекта "сурдотелефон" // Телекоммуникации и информационные технологии. 2018. Т. 5. № 1. С. 126-130.

DATA PREPARATION SUBSYSTEM FOR HARDWARE COMPLEX FOR RECOGNIZING HARD LANGUAGE

Renat I. Shakirov,
Graduate MTUCI, Moscow, Russia,
shakirovrenat@list.ru

Mikhail D. Artemov,
Post-graduate student of the Department of ISA&A, MTUCI, Moscow, Russia,
artemov_mikle@mail.ru

Lilia I. Voronova,
Head Department of ISA&A, Doctor of Physical and Mathematical Sciences, Professor, MTUCI, Moscow, Russia,
voronova.lilia@ya.ru

Abstract

The article describes the development of a subsystem for processing and preparing data of a software and hardware complex (HSC) for recognizing the sign language of disabled people with hearing and speech impairments. An analysis of analogue products for automatic sign language translation was carried out, technical and design requirements for the software and hardware complex were formulated, the architecture of the PAK based on the microservice approach was described. The results of the design and partial implementation of the subsystem for filling and processing photo-video materials of the sign language, as well as the metadata base and data storage are presented. The corresponding scenarios and algorithms are described. Examples of hand detection in the image are given.

Keywords: *pattern recognition, sign language, neural network technologies, software and hardware complex, microservice architecture.*

АНАЛИЗ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ СИСТЕМЫ NB-IOT

Деревянных Даниил Антонович,
студент МТУСИ, Москва, Россия,
sport.dda@mail.ru

Долбич Юлия Михаиловна,
студентка МТУСИ, Москва, Россия,
ydolbich@inbox.ru

Херсонский Антон Владимирович,
ассистент кафедры МКиИТ, МТУСИ, Москва, Россия,
a.v.khersonskii@mtuci.ru

Аннотация

В работе проведен анализ технологии «Интернета вещей» на основе системы Narrowband Internet of Things (NB-IoT). Исследованы основные параметры нового стандарта беспроводного Интернета вещей NB-IoT. Рассмотрены диапазоны рабочих частот и определены наиболее перспективные участки спектра для внедрения телематической системы NB-IoT. Описан принцип действия беспроводной сети, работающей совместно с сетью сотовой связи четвертого поколения. Проведена оценка повышения спектральной эффективности диапазона частот при совместной работе с сетью LTE в одной полосе частот. Разработана структурная схема модема NB-IoT. Определены основные параметры системы для реализации модема данного стандарта на современной элементной базе.

Ключевые слова: *Интернет вещей, система M2M, сигнал OFDM, совместное использование частот, передача телеметрии, система LTE, система NB-IoT.*

Введение

Концепция «Интернета вещей» описывает взаимодействие между физической средой, явлениями и событиями, окружающими человека, системами передачи данных, центрами и устройствами обработки данных, объединенными в общую сеть и взаимодействующую с глобальной сетью «Интернет». Данная концепция является реализацией идеи полной автоматизации жизни человека, описанной в мировой литературе многими известными писателями-футурологами и фантастами задолго до появления современных систем связи и глобальной сети «Интернет». Понятие «Интернет вещей» описывает не только технические аспекты автоматизации жизни человека, но и взаимодействие людей в современном цифровом обществе, а также многие бизнес-процессы [1,2].

Технология «Интернета вещей» позволяет автоматизировать сбор и обработку информации в сети с удаленных датчиков, распределенных по территории предприятия, покрытого этой сетью, а значит, позволяет более эффективно управлять ресурсами на объекте. Характер собираемых данных может быть любым, но чаще всего это телеметрические данные.

Оборудованием «Интернета вещей» являются датчики, исполнительные устройства, телекоммуникационное оборудование, системы цифровой обработки данных и абонентские устройства. Датчики – это устройства, преобразующие внешние физические воздействия в цифровые сигналы, применяемые в качестве передаваемых сообщений по сети [11]. Исполнительные устройства - это электромеханические устройства, позволяющие выполнять механические действия над физическими объектами по сигналу, пришедшему с управляющего устройства, датчика или телекоммуникационного устройства. Телекоммуникационное оборудование включает приемо-передающее, коммутационное оборудование и линии системы связи, реализующие эффективную передачу и прием телеметрических данных от датчиков до абонентов систем «Интернета вещей». Системами цифровой обработки данных являются серверы и системы сбора и обработки телеметрических данных, на которые установлены программное обеспечение и приложения, позволяющие обрабатывать данные с датчиков и управлять исполнительными и телекоммуникационными устройствами. В качестве абонентского оборудования используются персональные и управляющие компьютеры, различные гаджеты и устройства отображения параметров и индикации работы оборудования системы «Интернета вещей», позволяющие абоненту управлять системой.

В представленной работе исследуется технология «Интернета вещей» NB-IoT, которая является современной технологией взаимодействия современных сетей связи и радиодоступа с физической средой при помощи различных датчиков. Технология NB-IoT является современной технологией передачи телеметрических данных, которая использует ресурсы опорной сети сотовой связи четвертого поколения.

В связи с тем, что технология NB-IoT является новой технологией «Интернета вещей» параметры ее сигнала до конца не определены. Исследования влияния данной технологии на характеристики канала и сигналы NB-IoT, а также электромагнитная совместимость системы NB-IoT с другими системами, работающими в данном диапазоне частот описаны недостаточно, что обусловливает актуальность материалов, представленных в данной статье.

Технология NB-IoT

На сегодняшний день известны несколько реализаций систем Интернета вещей. Наиболее распространенные из них: технология NB-IoT, ZigBee, технологии WiFi и WiMAX, система LoRaWAN, система «СТРИЖ», и др. Рассматриваемая технология беспроводной узкополосной передачи данных NB-IoT (Narrowband Internet of Things), разработана специально для приложений Интернета вещей. Предполагаемая дальность связи NB-IoT – до 15 километров в сельской местности. Однако, в городских условиях, из-за высокой плотности застройки, «умные устройства» могут передавать данные на расстоянии не более чем 2-3 километра.

Технология NB-IoT, как и любая другая технология, реализующая концепцию «Интернета вещей» относится к семейству технологий сетей LPWAN (англ. Low-power Wide-area Network – «энергоэффективная сеть дальнего радиуса действия»). Технология LPWAN обеспечивает большую дальность связи при низком энергопотреблении. Разработкой стандартов технологии NB-IoT занимается организация 3GPP. В июне 2016 года Технология NB-IoT была стандартизована в

13-ом релизе 3GPP и предполагает организацию отдельной сети передачи данных. В числе компаний, принимающих участие в разработке, внедрении NB-IoT и её использовании: Huawei, Ericsson, Qualcomm, Vodafone, Orange, Cisco, Nokia, Мегафон, МТС. Сеть NB-IoT может быть развернута как с помощью оборудования сотовых сетей LTE, так и отдельно, на уникальном оборудовании системы NB-IoT известных производителей. Одно из основных требований, предъявляемых к подобным устройствам– низкое энергопотребление.

Преимуществом технологии NB-IoT перед известными системами «Интернета вещей» является возможность использования ресурсов сети четвертого поколения LTE, что упрощает развертывание сети рассматриваемой технологии. Технология NB-IoT имеет много общего с LTE, начиная с физической структуры радиосигнала и заканчивая архитектурой сети LTE. В LTE применяется принцип разделения каналов OFDM, что означает мультиплексирование с ортогональным частотным разделением каналов [2-4]. Технология NB-IoT создавалась с целью использования в условиях низкого уровня сигнала, высокого уровня шумов, и с учетом экономии емкости батареи.

Режимы работы NB-IoT. Основными режимами работы и размещения в частотном канале сети LTE спектра сигнала системы NB-IoT являются режимы, представленные на рисунке 1.

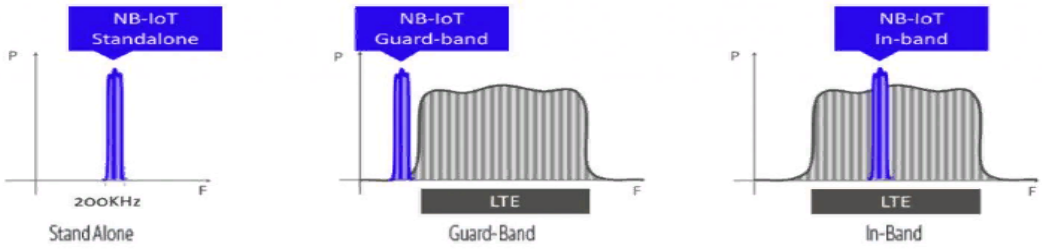


Рис. 1. Режимы развертывания системы NB-IoT [7]

Автономный режим (Stand-alone operation) призван заменить несущие систем GSM несущими NB-IoT и отображает режим работы системы NB-IoT, в котором система «Интернета вещей» не взаимодействует с другими системами радиосвязи, тогда как внутриполосный режим (In Band operation) использует блок ресурсов внутри обычной поднесущей LTE.

Самый распространенный режим работы – Guard Band (работа в защитной полосе сети LTE). С края границы своего спектра в области защитных и нулевых частот операторы сетей четвертого поколения выделяют необходимую для NB-IoT модулей полосу частот, которая соответствует одной поднесущей сигнала LTE.

Режим с защитной полосой (Guard Band operation) использует защитную полосу несущей LTE. Для поставщиков услуг LTE внутриполосный режим работы обеспечивает максимально эффективное развёртывание NB-IoT. Например, при завершении передачи трафика NB-IoT блок физических ресурсов (PRB), доступный для несущей NB-IoT, можно использовать для других целей, поскольку NB-IoT полностью интегрирован в существующую инфраструктуру LTE. Это позволяет планировщику базовой станции мультиплексировать трафик LTE и NB-IoT в один и тот же спектр.

Таким образом, в режимах In Band и Guard Band организуется совместное использование радиочастотного спектра системами LTE и NB-IoT. В режиме In Band система передачи NB-IoT занимает один ресурсный блок сигнала опорной сотовой системы связи как показано на рисунке 2.

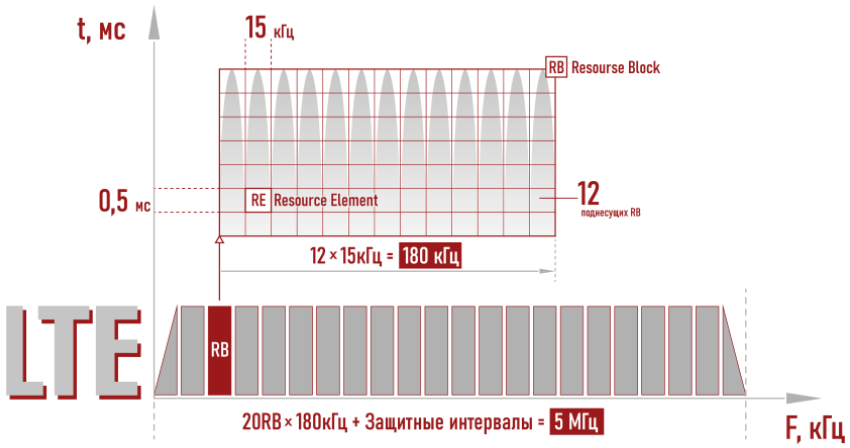


Рис. 2. Составляющие спектра сигнала системы NB-IoT в спектре сигнала системы LTE [2]

Частотный канал системы NB-IoT равен 180 кГц, что соответствует одному ресурсному блоку сотовой системы радиосвязи четвертого поколения, который в свою очередь соответствует одному частотному каналу сети 2G или одной поднесущей в частотном канале системы 4G. Эти параметры также соответствуют 12 ресурсным элементам сигнала опорной сети LTE [5-7].

Структурная схема модема системы NB-IoT

Система LTE построена на основе технологии OFDM. Соответственно, являясь опорной системой для NB-IoT технологии, структурная схема преемника и передатчика системы NB-IoT повторяет структурные схемы устройств формирования и обработки обычного сигнала OFDM. С учётом этого, структурные схемы приемника и передатчика системы NB-IoT представлены на рисунке 3. Различия заключаются в параметрах сигнала для системы NB-IoT с различными видами модуляции. С учётом этого на рисунке 3 изображена обобщенная структурная схема модема системы связи NB-IoT.

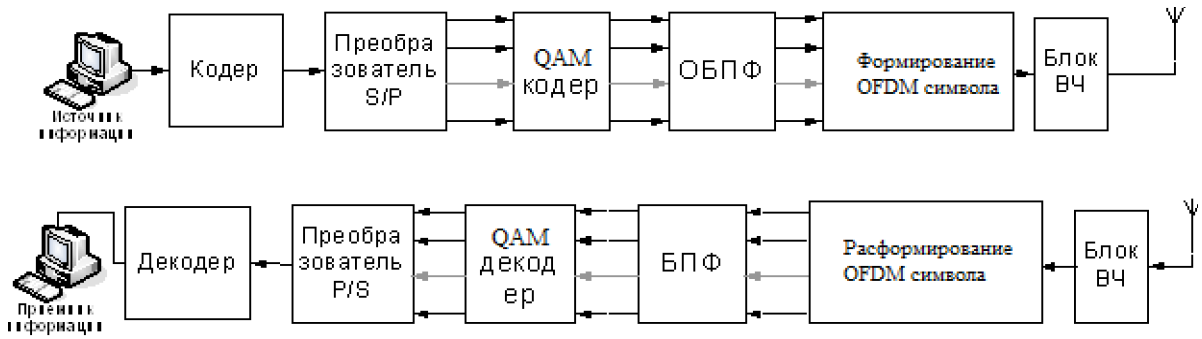


Рис. 3. Обобщенная структурная схема приемника и передатчика беспроводной системы связи на основе сигналов с ортогональным частотным разделением

Принцип работы модема системы NB-IoT повторяет принцип работы обычного OFDM модема. Последовательность бит, генерируемая источником информации, поступает на вход передатчика системы NB-IoT и на вход кодера, где во входную последовательность бит добавляется избыточные биты кодовой последовательности. Кодирование сообщения позволяет увеличить помехоустойчивость системы передачи данных и снизить влияние характеристик канала, а также выявить и исправить не более двух ошибок в передаваемом сообщении.

После прохождения параллельно-последовательного преобразователя (блок «Преобразователь S/P») сигнал поступает на блок QAM-кодера, который с использованием кода Грея присваивает блокам битовых последовательностей значения амплитуд и фаз квадратурных составляющих сигнала, тем самым производя QAM-модуляцию сигнала [13]. Затем модулированный сигнал поступает на блок ОБПФ, в котором производиться обратное быстрое преобразование Фурье (ОБПФ). Далее происходит: формирование OFDM символа с добавление сигналов синхронизации, параллельно-последовательное преобразование и добавление защитного префикса.

Задача блока ВЧ на передающей стороне состоит в преобразовании сигнала в квадратурные составляющие, выходной фильтрации и переносе спектра сигнала в высокочастотную область.

В приемнике выполняются обратные функции, и все выполненные преобразования сигнала производятся в обратном порядке, а именно: расформирование OFDM символа, быстрое преобразование Фурье, QAM-декодирование (демодуляция), параллельно-последовательное преобразование (блок «Преобразователь P/S»),

декодирование. Таким образом, переданный сигнал на приемной стороне восстанавливается, и принятое сообщение приводится в соответствие с переданным сообщением.

Определение параметров сигнала

Так как система NB-IoT достаточно новая и большинство параметров сигнала для реализации системы неизвестны, были определены (рассчитаны) основные параметры сигнала (таблица 1) по известной методике, представленной в [10,12].

Таблица 1

Параметры сигнала системы NB-IoT

№	Параметр	Значение	
	Метод модуляции	QAM-64	QAM-256
2	Длительность интегрируемой части OFDM-символа, T_{OFDM}, с	$12{,}8*10^{-6}$	$12{,}8*10^{-6}$
3	Расстояние между поднесущими, Δf, Гц	$0{,}078125*10^{6}$	$0{,}078125*10^{6}$
4	Количество используемых поднесущих в заданной полосе частот, N используемых *MediaPipe*	64	64
5	Количество поднесущих, используемых для передачи данных (кодовых бит), N *MediaPipe* кодовых бит	31	31
6	Число поднесущих Nподн. в одном OFDM-символе	32	32
7	Число не используемых (нулевых) поднесущих, N н. исп подн	1	1
8	Интервал дискретизации по времени комплексной огибающей OFDM-символа, Δt, с	$0{,}2 * 10^{-6}$	$0{,}2 * 10^{-6}$
9	Длительность защитного интервала, Тзащ, с	$3{,}2 * 10^{-6}$	$3{,}2 * 10^{-6}$
10	Длительность OFDM-символа, Тс	$9{,}6 * 10^{-6}$	$9{,}6 * 10^{-6}$
11	Общее число отсчетов огибающей OFDM-символа, Nотсч	80	80
12	Число отсчетов огибающей OFDM-символа на защитном интервале, Nзащ.	16	16
13	Число кодовых бит на одной поднесущей или в одном КАМ-символе, Nбит КАМ	6	8
14	Число кодовых бит в одном OFDM-символе (блоке), Nкод бит бл.	282	376
15	Число информационных бит в одном OFDM-символе (блоке) на входе кодера, Nинф бит бл.	141	188
16	Выходная мощность передатчика, дБм	20	20
17	Расчетная дальность системы, м	2150	2150
18	Расчетная скорость передачи данных, кбит/с	5,20	7,09

Полученные в результате расчета параметры исследуемой системы позволяют реализовать систему NB-IoT на современной элементной базе. В ходе расчета параметров сигнала системы NB-IoT был определен радиус действия модема равный **2150 м** и скорость передачи данных при модуляции QAM-64 равная **5,20 кбит/с**, а при модуляции QAM-256 – **7,09 кбит/с**.

Анализ современной элементной базы

В рамках данной работы был проведен анализ современной элементной базы для системы NB-IoT.

Одним из наиболее перспективных производителей NB-IoT-модулей на сегодняшний день является компания Quectel. Основными сериями современных радиомодулей NB-IoT данной компании являются радиомодули Quectel: BG95, BG96, BG77, BG600L-M3, BC660K-GL – на базе чипсета Qualcomm.

Таблица 2

Технические характеристики BG77 [8]

Наименование	Чипсет	Поддерживаемые технологии	Поддерживаемые диапазоны, МГц	Напряжение питания, В	Энергопотребление	Корпус, размер (ДхШхВ), мм	Особенности модуля
BG77	Qualcomm MDM9205	LTE Cat M1, Cat NB2	LTE-FDD: B1, B2, B3, B4, B5, B8, B12, B13, B18, B19, B20, B25, B26, B27,	2,6…4,8	3,2 мкА при задействованном PSM (USB и UART отключены	94-pin LGA, 14,9×12,9×1,7	SoftSIM; QuecLocator; QuecOpen; обновление прошивки: по USB, DFOTA; Jamming Detection

Также выпускаются модули EXS62/EXS82, выполненные на базе современного чипсета Qualcomm, поддерживающие работу в сетях 4G и 2G. Технические характеристики радиомодулей EXS62/EXS82 представленные в таблице 3.

Таблица 3

Технические характеристики NB-IoT-модулей EXS62/EXS82 [9]

Частотный диапазон, МГц	LTE Cat. M1: 600 (Bd71), 700 (Bd12, Bd13, Bd14, Bd28, Bd85), 800 (Bd18, Bd19, Bd20, Bd26, Bd27), 850 (Bd5), 900 (Bd8), 1700 (Bd66), AWS (Bd4), 1800 (Bd3), 1900 (Bd2, Bd25), 2100 (Bd1) LTE Cat. NB1/NB2: 600 (Bd71), 700 (Bd12, Bd13, Bd17, Bd28, Bd85), 800 (Bd18, Bd19, Bd20, Bd26), 850 (Bd5), 900 (Bd8), 1700 (Bd66), AWS (Bd4), 1800 (Bd3), 1900 (Bd2, Bd25), 2100 (Bd1)
Скорость передачи данных	LTE Cat.M1 DL: до 300 кбит/с, UL: до 350 кбит/с LTE Cat.NB1 DL: до 27 кбит/с, UL: до 63 кбит/с
ГНСС	GPS/BeiDou/Galileo/ГЛОНАСС
Интерфейсы	SMT-LGA 114 площадок, последовательный интерфейс, 2 SIM-карты, LTE-антенна, ГНСС-антенна
Обновление	по интерфейсу/OTA/incremental FOTA
Питание, В	LTE и GSM: 3,0…4,5 LTE (GSM выкл.): 2,5…4,8
Диапазон рабочих температур	-40°C…+85°C
Размеры, мм	27,6 x 18,8 x 2,17
Вес, г	3,5

Данные модули являются наиболее перспективными для реализации модемов системы NB-IoT, так как поддерживают работу в большом количестве частотных диапазонов и обладают расширенной функциональностью.

Выводы

1. Так как система NB-IoT базируется на сети сотовой связи четвертого поколения и занимает один ресурсный блок, соответственно, она оказывает минимальное влияние на базовую сеть.
2. Применение OFDM модуляции для системы NB-IoT в одном ресурсном блоке базовой технологии позволяет повысить спектральную эффективность использования частотного диапазона и, при этом, реализовать относительно высокоскоростную передачу телеметрии на большие расстояния.
3. При реализации модема системы NB-IoT на выбранном цифровом сигнальном процессоре можно обеспечить передачу телеметрических данных при модуляции QAM-64 со скоростью 5,20 кбит/с на расстояние 2151 м.

Литература

1. Технология NB-IoT в России: Устройства, инфраструктура и внедрение. // Материал сайта компании ЕвроМобайл-Групп. [Электронный ресурс]: https://www.euromobile.ru/m2m-resheniya/tekhnologiya-nb-iot-v-rossii-ustroystva-infrastruktura-i-vnedrenie/ (дата обращения 22.03.2021).
2. Технология NB-IoT: интернет вещей в умном городе / Акционерное общество «Телеофис» [Электронный ресурс]: https://teleofis.ru/blog/tekhnologii/tekhnologiya-nb-iot-internet-veshchey-v-umnom-gorode/ (дата обращения 22.03.2021).
3. *Алексеев В.* Технологии мобильной связи для IoT стандарта 3GPP Rel. 13 // Беспроводные технологии. 2016. №4. С. 44-51.
4. *Вишневский В., Красилов А., Шахнович И.* Технология сотовой связи LTE – почти 4G // Электроника: Наука, Технология, Бизнес. 2009. №1. С. 62-72.
5. *Рыжков А.Е.* Развитие технологии NB-IoT // Труды учебных заведений связи. 2017. Т.3. №4. С. 94-101.
6. NB-IoT: как он работает? [Электронный ресурс]: https://habr.com/ru/company/ru_mts/blog/430496/ (дата обращения 22.03.2021).
7. Технология NB-IoT: особенности развертывания в сотовых сетях. [Электронный ресурс]: https://networkguru.ru/tekhnologiia-nb-iot-osobennosti-razvertyvaniia/ (дата обращения 22.03.2021).
8. Quectel BG600L-M3 LTE Cat M1/Cat NB2/EGPRS Module. [Электронный ресурс]: https://ru.mouser.com/datasheet/2/1052/Quectel_BG600L-M3_LPWA_Specification_V1.0-1830028.pdf (дата обращения 22.03.2021).
9. Cinterion EXS82/62 и TX82/62 – новые модули для сетей LPWA от Thales-Gemalto. [Электронный ресурс]: https://www.symmetron.ru/news/cinterion-exs82-62-i-tx82-62-novye-moduli-dlya-setey-lpwa-ot-thales-gemalto/ (дата обращения 22.03.2021).
10. *Бакулин М. Г., Крейнделин В. Б., Шлома А. М., Шумов А. П. и др*. Технология OFDM: учебное пособие для вузов. М.: Горячая линия – Телеком, 2017. 360 с.
11. *Орлов В.Г., Тюмин С.Г.* Стандарты беспроводной связи для системы умный дом // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 20-28.
12. *Волков Л. Н., Немировский М. С., Шинаков Ю. С.* Системы цифровой радиосвязи: базовые методы и характеристики: учебное Пособие. М.: Эко-Трендз, 2005. 392 с.
13. *Журавлев В. И., Трусевич Н. П.* Методы модуляции-демодуляции радиосигналов в системах передачи цифровых сообщений. М.: Инсвязьиздат, 2009. 312 с.

ANALYSIS OF INTERNET OF THINGS TECHNOLOGY BASED ON A SYSTEM NB-IOT

Daniil A. Derevyannykh,
Student MTUCI, Moscow, Russia,
sport.dda@mail.ru

Yulia M. Dolbich,
Student MTUCI, Moscow, Russia,
ydolbich@inbox.ru

Anton V. Kherson,
Assistant of the Department of MC&IT, MTUCI, Moscow, Russia,
a.v.khersonskii@mtuci.ru

Abstract

The paper analyzes the "Internet of Things" technology based on the Narrowband Internet of Things (NB-IoT) system. The main parameters of the new standard for the wireless Internet of things NB-IoT are investigated. The ranges of operating frequencies are considered and the most promising areas of the spectrum for the implementation of the NB-IoT telematics system are identified. The principle of operation of a wireless network operating in conjunction with a fourth generation cellular network is described. An assessment of the increase in the spectral efficiency of the frequency range when working together with the LTE network in the same frequency band is carried out. The block diagram of the NB-IoT modem has been developed. The main parameters of the system for the implementation of a modem of this standard on a modern element base have been determined.

Keywords: *Internet of Things, M2M system, OFDM signal, frequency sharing, telemetry transmission, LTE system, NB-IoT system.*

РАЗРАБОТКА ВИЗУАЛИЗАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ АВТОМАТИКОЙ ДЛЯ «УМНОГО ОФИСА» НА БАЗЕ КОНТРОЛЛЕРОВ LOGICMACHINE

Савельев Никита Денисович,
студент МТУСИ, Москва, Россия,
nikita.savelev@lm.net.ru

Сасс Василий Дмитриевич,
студент МТУСИ, Москва, Россия,
vasily@sass.pro

Безумнов Данил Николаевич,
старший преподаватель МТУСИ, Москва, Россия,
d.n.bezumnov@mtuci.ru

Аннотация

Целью статьи является разработка визуализации системы управления автоматикой в офисных помещениях на базе контроллеров LogicMachine с web-интерфейсом. Рассмотрены перспективы развития рынка промышленного управления и автоматизации. Проведён анализ предметной области в сфере автоматизации офисных помещений. Приведена разработка системы на базе промышленного контроллера LogicMachine. обеспечивающей удаленное управление системами автоматики "умного рабочего места", упрощение процесса обслуживания оборудования и обладающей интуитивно-понятный web-интерфейс.

Ключевые слова: *автоматизация, визуализация, LogicMachine, CSS, lua, KNX, удаленный контроль, web-SCADA, мониторинг.*

Введение

Системы управления бытовыми и промышленными приборами активно интегрируются в жилые, офисные и производственные помещения. С развитием рынка смартфонов и мобильных приложений многие системы получили функции дистанционного управления. По данным компании *Research and Markets* ожидается, что объем рынка промышленного управления и автоматизации производства будет расти с 2021 по 2026 год он со среднегодовым темпом роста 8,2% [1]. Ключевыми факторами, способствующими росту рынка, являются: массовое внедрение новых технологий, таких как искусственный интеллект и Интернет вещей; появление связанных предприятий в промышленных средах; потребность в наращивании массового выпуска новой продукции; государственные инициативы по продвижению промышленной автоматизации и оптимальному использованию ресурсов, а также фискальная политика региональных финансовых учреждений, направленная на поддержку предприятий в условиях пандемии COVID-19 [2].

Одной из сфер применения решений по автоматизации инженерных систем и бизнес процессов является «Умный офис». «Умный офис» – это автоматизированная система управления, которая предназначена для контроля и управления освещением, отоплением, вентиляцией, водоснабжением, безопасностью, аудио/видео аппаратурой и другими инженерными системами офисных помещений. Важной частью работы с такими системами является интерфейс управления и визуализация.

Производства, идущие в ногу со временем и активно использующие новые технологии, все глубже интегрируют в свои производственные процессы использование различных свободно программируемые контроллеров для повышения производительности труда, диагностики ошибок в технических процессах, создания комфортных условий труда, привлечения высококвалифицированных сотрудников и повышения эффективности их работы.

Решения в области визуализации элементов управления на российском рынке предлагают компании *iRidium Modile* [3] и *Embedded Systems Rus* [4]. Интерфейс их продуктов представлен на рисунке 1.

Рис. 1. Интерфейс систем визуализации iRidium modile и Embedded Systems Rus

Эти компании предлагают свои подходы к разработке визуализаций как с точки зрения подбора оборудования, так и дизайнерских решений. Компания *iRidium Modile* делается акцент на оконечных панелях и дизайнерской части визуализации. Компания *Embedded Systems Rus* предлагает более универсальное и функциональное оборудование для создания интеллектуальных и инженерных систем, но не располагает оконечными панелями и серьезными дизайнерскими наработками. В статье приводится описание созданного шаблона визуализации на базе оборудования компании Embedded Systems Rus, с помощью которого можно достичь синергии функциональности инсталляции и эргономичности процессов управления.

Постановка задачи

Целью данной работы является разработка шаблона визуализации элементов управления автоматикой и инженерными системами, обладающей следующими функциональными возможностями:

1. Мониторинг основных параметров помещений: температура, влажность и качество воздуха, показания счетчиков и датчиков или других поступающих показаний;
2. Удаленное управление «умными» устройствами;
3. Контроль и диагностика обслуживающими организациями аварий и событий на объекте;
4. Оповещение пользователей о событиях корпоративного характера;
5. Автоматизированное управление сценариями работы подсистем «умного офиса»: установка комфортных для пользователя настроек освещенности, температуры и влажности воздуха, работ систем по сценарию «Начало рабочего дня», «Конец рабочего дня» и т. д.

Для решения вышеперечисленных проблем был разработан шаблон визуализации. Задачей визуализации является создание комфортных условий труда в рамках офисных помещений, в частности пользователю должна быть доступны: регулировка параметрами освещения, климата, положением штор и жалюзей; управление системами мониторинга условий труда и жизнедеятельности; получение уведомлений о событиях в системе; предоставление обслуживающим организациям возможности проводить упрощенную удаленную диагностику и мониторинг состояний модулей системы.

При разработке визуализации отдельно можно выделить проблемы эргономичности и безопасности. Так, интерфейс для восприятия конечного пользователя должен быть понятен, однозначен, иметь адекватность насыщения и не требовать большого количества действий от пользователя.

В то же время необходимо обеспечить контроль доступа к управлению инженерными системами, чтобы не допустить переход управления к третьим лицам.

Необходимо заранее продумать механику деления пользователей на имеющих неограниченные функциональные возможности (сервисные службы, руководство компании) и рядовых пользователей, которым дозволено работать только со своими персональными зонами ответственности. Таким образом, с помощью средств визуализации можно решить проблему предоставления пользователям возможности управления и получения информации без дополнительного риска аварий и умышленного причинения вреда.

Архитектура системы

В большинстве интеллектуальных систем ключевым связующим и логическим звеном выступают программируемые контроллеры. На них возлагаются следующие задачи: по получение команд от человека посредством web-страниц визуализации и информации с датчиков; управление оконечными устройствами и интеллектуальными системами; хранение, обработка, представление, транслирование и передача информации; объединение в одну инсталляцию устройств разных стандартов и технологий в качестве мультипротокольного шлюза, который выступает сервером для web-SCADA и визуализации.

SCADA (от англ. ***S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition*) представляет собой программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. Web-SCADA – это SCADA, работающая на web-платформе, получение доступа к которой осуществляется посредством браузера.

Архитектура проекта и место визуализации в нем представлена на рисунке 2.

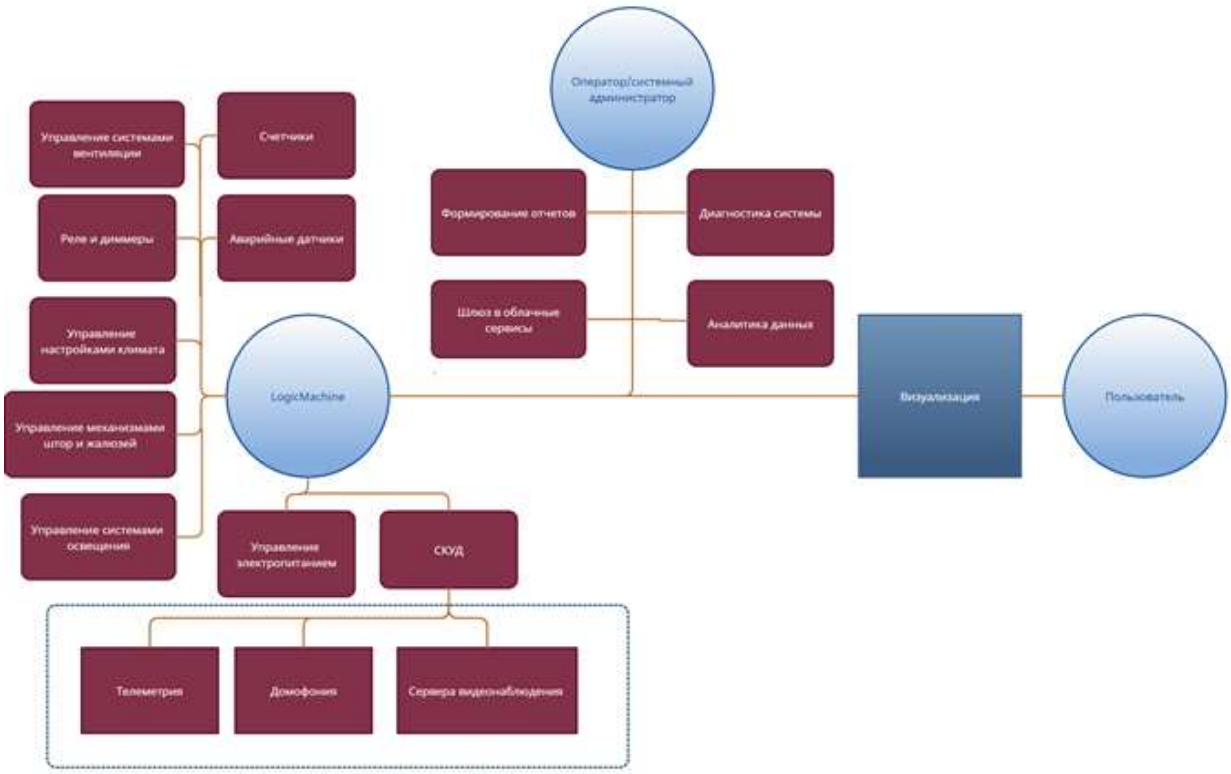


Рис. 2. Архитектура проекта

При разработке визуализации для систем управления, необходимо: продумать иерархию страниц и создать систему логичной навигации между ними, исключив путаницу и избыточное количество действий пользователя; реализовать концепцию планов, виджетов и страниц так, чтобы процессы управления и получения информации были интуитивно понятны, давали четкое понимание связи реальных объектов и систем с их представлениями на страницах; разработать дизайнерское решение, удовлетворяющее эстетическим требованиям к визуализации; написать скрипты реализующие логику управления реальными элементами со страниц визуализации.

Таким образом, разработка визуализации – комплексная задача, требующая навыков программирования и дизайна; понимания принципов создания эргономичных интерфейсов и потребностей конечных пользователей; знаний в сфере работы ПЛК в целом, протоколов управления оконечными устройствами и особенностей работы с конкретной моделью ПЛК.

Проектирование аппаратной части

В качестве центрального устройства управления в работе использован контроллер LogicMachine 5 (Lm5Cp2-DW1) [6].

Устройства семейства LogicMachine представляют собой свободно программируемые контроллеры промышленного уровня, широко применяемые на рынке автоматизации и «умного дома». Отличительной чертой данных контроллеров является богатый набор интерфейсов, что позволяет в рамках одного проекта интегрировать в одну устойчивую инсталляцию устройства различных производителей, наряду с поддержкой большинства актуальных IT протоколов.

Модель Lm5Cp2-DW1 обладает набором портов и интерфейсов, состоящих из 2-х DALI (*Digital Addressable Lighting Interface* – протокол управления освещения) интерфейсов, интерфейсом CAN FT (полевая шина), одного порта RS485 (интерфейс физического уровня с большим количеством надстроенных протоколов), порта RS485/RS232, и разъемами USB 2.0 и Ethernet.

Контроллеры LogicMachine включают блок логики, межпротокольный шлюз и сервер для работы web-SCADA и визуализации систем управления. Внутренняя адресация и работа с объектами построена на объектах KNX [7], т.е. элементы управления и представления информации привязываются к KNX объектам и могут транслироваться в шину KNX по KNX IP/TP. Каждый контроллер выступает сервером для собственной web-SCADA, изображённой на рисунке 4.

Web-SCADA контроллеров LogicMachine поставляется в виде предустановленного программного обеспечения и создана для визуальной работы инженера с объектами, скриптами, устройствами и данными.

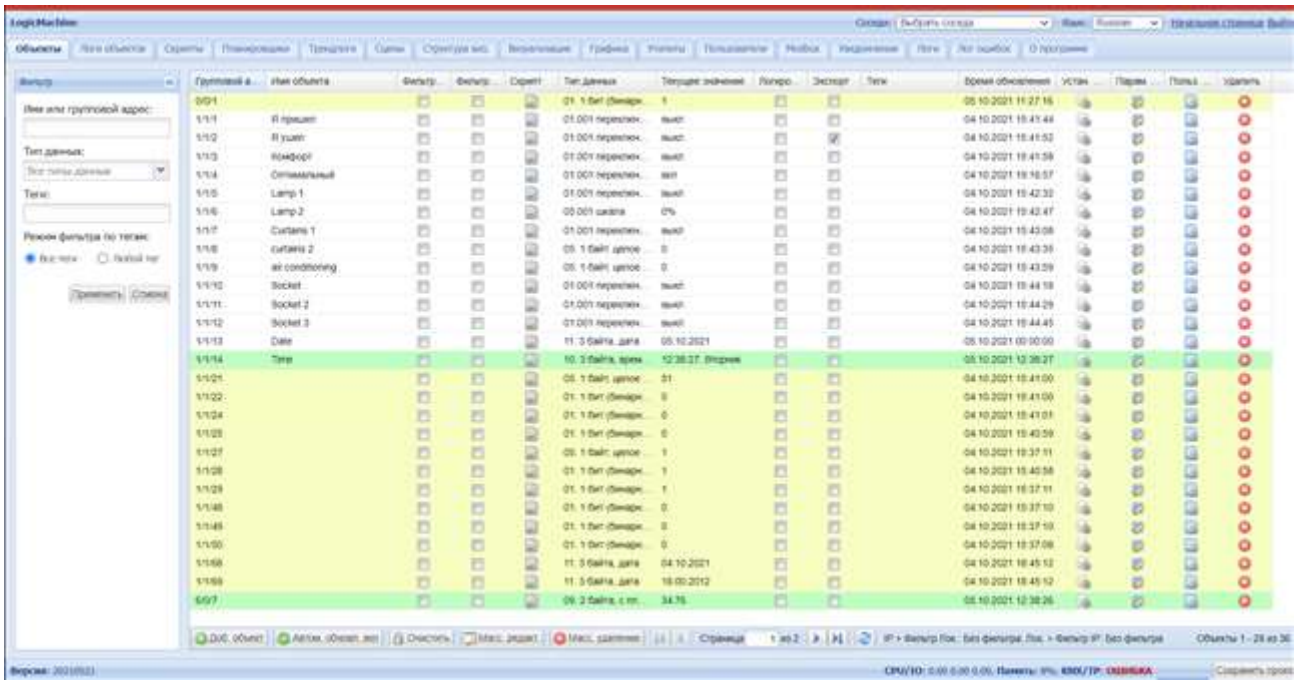


Рис. 4. Главный экран Web-SCADA

Программирование контроллера проводится на языке Lua [8] и реализовано тремя видами скриптов: резидентными (включаются по временному интервалу), событийными (отрабатывают при изменении значения группового адреса) и скриптами по расписанию (позволяют планировать включение скрипта в строгом соответствии с реальным временем). При создании визуализаций есть возможность подгружать пользовательский код JavaScript [9] и CSS[10]. В работе использовались практически все виды перечисленных скриптов: резидентные – для ежесекундного обновления счетчика времени и даты, событийные – для отработки сценариев при нажатии на кнопки визуализации и отправки сообщений в журнал, CSS – для визуального редактирования элементов визуализации.

Алгоритм создания визуализации

Рассмотрим последовательность этапов создания визуализации, универсальную для всех контроллеров LogicMachine и всех типов визуализаций:

1. Создание общей иерархии и страниц с помощью встроенного менеджера страниц. Создается родительский каталог, в нем создаются уровни, в уровнях - отдельны планы страниц. После создания все страницы представляют собой белые пустые листы. Создание иерархии страниц актуально для больших проектов (например, для нескольких зданий).
2. Создание подложек и виджетов. Подобно созданию страниц, генерируются пустые белые пространства, которые можно дополнительно вызывать на страницах «поверх» основной страницы.
3. Загрузка графики на контроллер: установка шрифтов, загрузка изображений, иконок, GIF-анимаций и прочих элементов. Процесс загрузки может быть осуществлен как по протоколу FTP напрямую, так и с помощью кнопки «Загрузить» в разделе хранилища графики.
4. Построение плана страниц: установка фоновых изображений, привязка иконок к объектам KNX, создание переходов между страницами, расположение объектов, фреймов, текста и изображений по плану. Для рассматриваемого в статье шаблона все иконки нарисованы авторами самостоятельно. Для создания переходов между страницами использовалась область «прозрачной кнопки», которая представляет собой прозрачный элемент, при нажатии на который происходит перенаправление на другую страницу.
5. Написание CSS-кода для модификации встроенных средств и элементов под проект. Существует возможность загрузки пользовательского JavaScript кода для создания более совершенных визуализаций. Посредством CSS в работе персонализированы все элементы на плане страницы.
6. Написание управляющих скриптов на языке Lua.
7. Написание кода для создания системы уведомлений. Для этого на контроллере создан файл-обработчик, который принимает и выводит на экран аргументы функции eventlog.
8. Проведение финальной настройки для придания визуально эстетичного вида. Корректировка настроек самой визуализации по типу «ориентирования страницы» или «время сна».

Принцип работы визуализации

Конечные пользователи настоящей визуализации условно поделены на две группы:

1. Простой пользователь: сотрудник организации или посетитель; имеет возможность управления только определенной частью системы, в остальные разделы он не допускается;

2. Суперпользователь: представитель руководства организации, сетевой администратор или сотрудник обслуживающей организации; имеет полные права доступа к информации и элементам управления.

Рассмотрим рядовой сценарий использования визуализации:

1. Пользователь входит на страницу web-SCADA.

2. Происходит перенаправление на главную страницу непосредственно его личного кабинета или рабочего места. Адрес страницы, на которую происходит перенаправление, определяется заранее для каждого пользователя и происходит в соответствии с введенным логином и паролем при входе на web-SCADA контроллера (рис. 5).

3. Совершает необходимые действия. Например, сотрудник офиса пришел на свое рабочее место и включает сценарий «Я пришел», в рамках которого одновременно начинают работать системы вентиляции, климата, освещения, увлажнения воздуха и прочие.

На главной странице располагается весь наиболее часто используемый функционал (рис. 5).

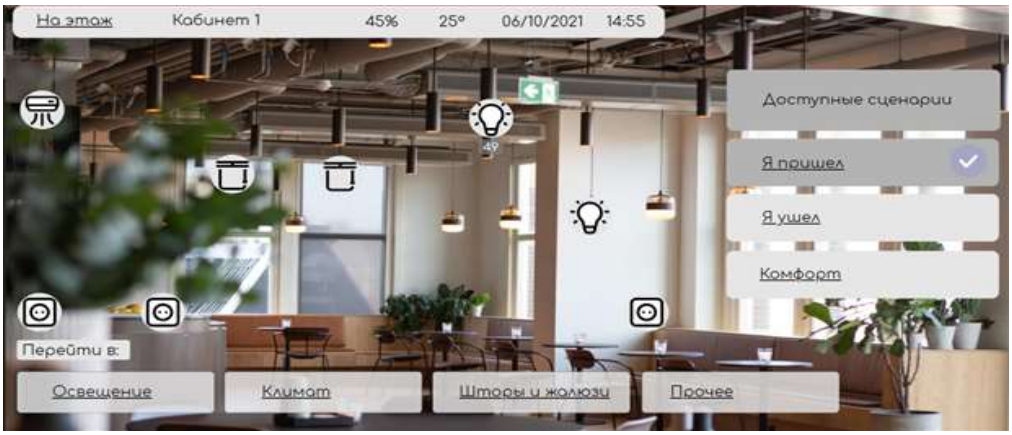


Рис. 5. Главная страница пользователя

В верхней части страницы располагается информационная полоса. Она демонстрирует показатели состояния воздуха, дату и время, назначение страницы, позволяет перейти на этаж и в навигационное меню.

В правой части размещено меню выбора активного сценария. Сценарий позволяет в одно нажатие выставить настройки всех систем в соответствие с потребностями, заранее запрограммированными. Например, стандартный сценарий «Я пришел» включает все системы для создания оптимальных условий, а сценарий «Я ушел» выключает.

Снизу расположена полоса специализированных разделов. Перейдя в один из них, пользователь может провести отдельную настройку подсистемы в соответствие с требованиями, отличающимися от выбранного сценария (рис. 6). Вложенность специализированных страниц позволяет обеспечить необходимую функциональность и не создает избыточность поиска нужного элемента управления.

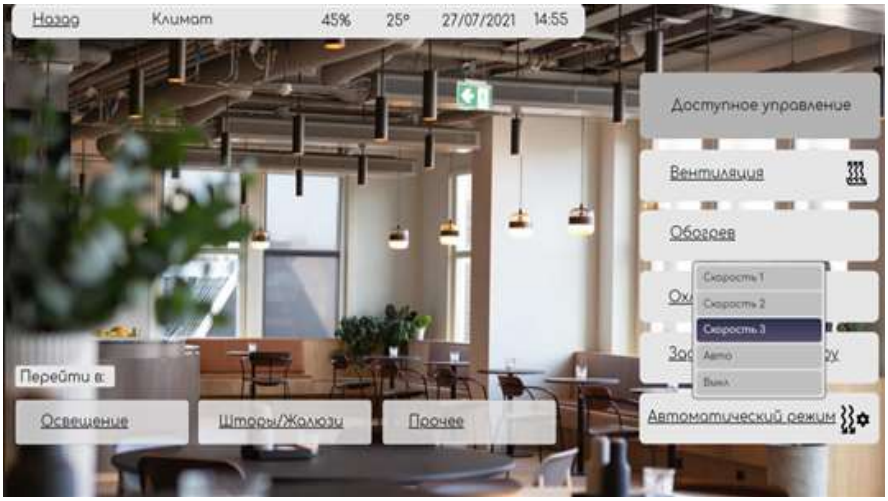


Рис. 6. Пример специализированной страницы

Если пользователю необходимо совершить простое действие: закрытие штор, выключение светильника и др. – сделать это можно с помощью активных иконок, расположенных по центру плана.

Простому пользователю возможность перейти на страницу этажа и далее, однако он не имеет прав для изменения каких-либо значений и управления чем-либо.

Другой вариант разграничения функционала – оставить только возможность работать с персональным, отделенным от остальной визуализации, набором страниц.

Принимая во внимание, что большая часть офисов представляют собой открытые пространства с большим количеством одновременно работающих сотрудников (так называемый

« open space»), также был подготовлен шаблон для такого типа офисных помещений (рис. 7).

Рис. 7. Страница-шаблон для открытых офисных помещений («openspace»)

В данном случае представлена возможность изменения ограниченного списка параметров. Например, каждый из пользователей может регулировать только свою лампу и розетку, но регулировать общие параметры помещения, (выбирать режим работы кондиционера и др.) могут все пользователи, находящиеся в этом помещении. Суперпользователь, как отмечалось выше, имеет полный набор прав.

Стартовая страница суперпользователя представлена на рисунке 8.

Рис. 8. Стартовая страница суперпользователя

Как видно на рисунке 8, стартовая страница поделена на четыре функциональные области:

1. Вертикальная полоса состояний. Служит для отображения информации, температуры, влажности, даты и времени.

2. Навигационная система. Слева расположена древовидная система навигации по зданиям, этажам, помещениям (рис. 9).

3. Функциональная зона. Два столбца кнопок для управления.

4. Журнал уведомлений. Данный журнал представляет собой внутреннюю систему уведомлений. Сообщения в него отправляются посредством скрипта. Также, реализован мигающий индикатор, демонстрирующий появление нового уведомления (рис. 10).

Рис. 9. Система навигации

Пиктограмма молнии рядом с названием помещения свидетельствует о нерациональном или излишнем потреблении электроэнергии. Например, если оборудование осталось включенным после конца рабочего дня или произошли ошибки в работе систем помещения.

Рис. 10. Работа журнала уведомлений

Также для суперпользователя создана специализированная страница для оценки состояний узлов, проверки ошибок и аварий (рис. 11).

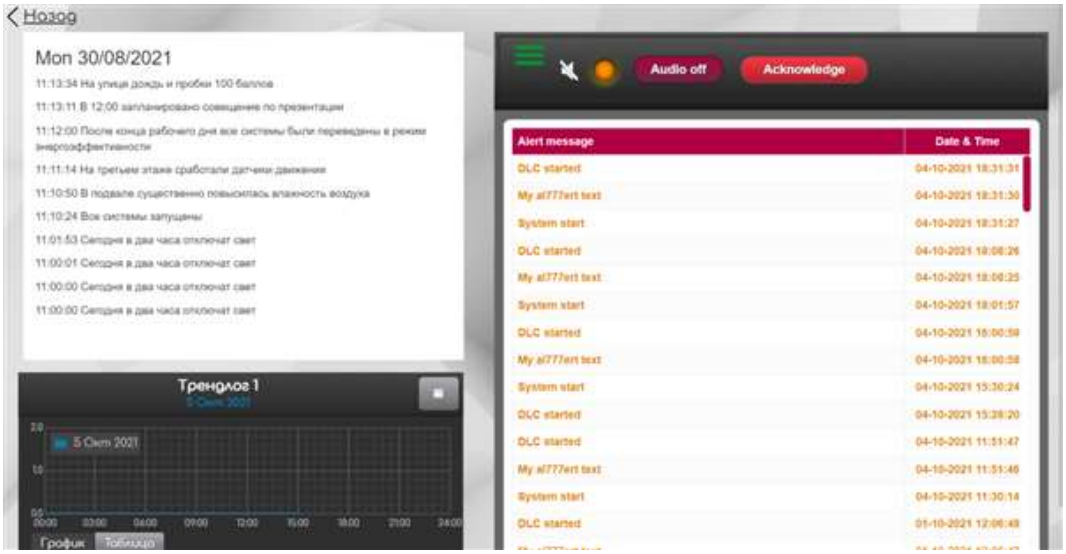


Рис. 11. Информационная страница

Справа на рисунке 11 расположен журнал аварий, в который автоматически отправляются все сведения об ошибках приложений или систем. Слева находится тот же журнал уведомлений, что и на главной странице, но в отличие от него, в нём сохраняются 1000 последних сообщений, а не 10. Снизу на информационной странице представлен график активности группового адреса, что позволяет отслеживать изменения значения адреса в течение времени.

Разработанная система визуализации обладает рядом достоинств:

1. Универсальность. Систему можно развернуть, используя любой контроллер LogicMachine за несколько минут и перейти к детальной настройке системы.

2. Простота в работе и обслуживании. Настройка визуализации под конкретную задачу не требует услуг высококвалифицированных программистов или инженеров, достаточно пройти базовое обучение работе с контроллерами LogicMachine.

3. Низкая стоимость. Для создания системы визуализации помимо контроллера не требуется дополнительное оборудование, лицензии на расширение проекта и услуги узконаправленных специалистов.

4. Масштабируемость под вновь разрабатываемые проекты. Система не имеет ограничений на количество планов, страниц или функциональность. Разработчик ограничен только техническими возможностями контроллера и объёмом памяти Flash-карты.

Заключение

Рынок IoT и автоматизации в последние года неуклонно растет. Автоматизируются не только технологические процессы, но и управление условиями труда, системами жизнедеятельности, и даже частными домами [11].

Умный офис – это современный формат помещения, оснащенного интегрированными инженерными системами, интеллектуальным мультимедийным комплексом и информационными системами для комфортной и эффективной работы компании. Такой формат помещений актуален для компаний различный отраслей, которые стремятся к рациональному использованию материальных ресурсов и современному комфорту в ежедневной работе персонала.

Разработка визуализации системы управления автоматикой в офисных помещениях проводилась с использованием возможностей web-SCADA и средств визуализации контроллеров семейства LogicMachine, Поставленные задачи разработки решались за счет визуального представления данных и элементов управления конкретно в сфере офисных помещений. В виду универсальности контроллеров и его средств их визуализации, разработанный шаблон визуализации можно использовать и в других проектных условиях.

Универсальные возможности контроллеров позволяют управлять устройствами, соответствующих основным стандартам и технологиям рынка автоматизации, такие как: KNX, Modbus, CANx, Zigbee, DMX512, 1-Wire, DALI, Ekey, GSM, BAcnet/IP и другие. Таким образом, и визуализация, построенная на этих контроллерах, позволяет взаимодействовать с большим количеством устройств различных технологий и производителей.

Используя предложенные решения инженеры-инсталляторы получают возможность предлагать заказчику удобный интерфейс управления системой; сервисные службы – использовать упрощенный способ контроля работоспособности и диагностики систем, а конечные пользователи – использовать интуитивно понятный способ управления автоматикой и дополнительный корпоративный информационный канал.

Литература

1. Research and Markets [Электронный ресурс]. Режим доступа: https://www.researchandmarkets.com/about-us (Дата обращения 09.10.2021).
2. Исследование и прогноз рынка автоматизации на 2026 год. [Электронный ресурс]. Режим доступа: https://www.researchandmarkets.com//5393391/global-industrial-control-and-factory-automation?utm_source=CI&utm_medium=PressRelease&utm_code=bcbqds&utm_campaign=1578934++Global+Industrial+Control+%26+Factory+Automation+Market+Report+2021%3a+Market+is+Expected+to+Reach+%24197.8+Billion+by+2026++Opportunities+in+the+Adoption+of+Industry+4.0+Principles&utm_exec=chdo54prd (Дата обращения 09.10.2021).
3. iRidium Mobile [Электронный ресурс]. Режим доступа: https://iridi.com/ru/projects/smart-buildings/ (Дата обращения 09.10.2021).
4. Embedded Systems Rus [Электронный ресурс]. Режим доступа: https://logicmachine.net.ru/resheniya/visualization/ (Дата обращения 09.10.2021).
5. Что такое SCADA [Электронный ресурс]. Режим доступа: http://datasolution.ru/chto-takoe-scada.
6. LogicMachine5 Power (LM5p-DW1). Документация продукта [Электронный ресурс]. Режим доступа: https://logicmachine.net.ru/wp-content/uploads/document/LM5/lm5_DW1_manual_Final.pdf (Дата обращения 09.10.2021).
7. Ассоциация KNX [Электронный ресурс]. Режим доступа: https://www.knx.org/knx-en/for-professionals/What-is-KNX/A-brief-introduction/index.php (Дата обращения 09.10.2021).
8. The Programming Language Lua [Электронный ресурс]. Режим доступа: https://www.lua.org/ (Дата обращения 09.10.2021).
9. JavaScript [Электронный ресурс]. Режим доступа: https://www.javascript.com/ (Дата обращения 09.10.2021).
10. Cascading Style Sheets [Электронный ресурс]. Режим доступа: https://www.w3.org/Style/CSS/Overview.en.html (Дата обращения 09.10.2021).
11. *Орлов В.Г., Тюмин С.Г.* Стандарты беспроводной связи для системы умный дом // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 20-28.

DEVELOPMENT OF THE VISUALIZATION OF THE AUTOMATION CONTROL SYSTEM FOR "SMART OFFICE" BASED ON LOGICMACHINE CONTROLLERS

Nikita D. Saveliev,
Student MTUCI, Moscow, Russia,
nikita.savelev@lm.net.ru

Vasily D Sass,
Student MTUCI, Moscow, Russia,
vasily@sass.pro

Danil N. Bezumnov,
Senior lecturer, MTUCI, Moscow, Russia,
d.n.bezumnov@mtuci.ru

Abstract

The purpose of the development is to develop a control system for automation in office premises based on LogicMachine controllers with a web interface. The prospects for the development of the automated control market are considered. The analysis of the subject area in the field of office space automation has been carried out. The developed system solves the issue of remote control of the automation systems of the "smart workstation", simplifies the process of equipment maintenance and has an intuitive web interface. The system is based on the industrial controller LogicMachine.

Keywords: *automation, visualization, LogicMachine, CSS, lua, remote control, KNX, web-SCADA, monitoring.*

РАСЧЕТ ПРОИЗВОДСТВЕННОЙ ПРОГРАММЫ ПО ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ ПОДВИЖНОГО СОСТАВА АТП НА ОСНОВЕ РЕЗУЛЬТАТОВ РАСЧЕТА В ПО «ТЕХНОЛОГИЧЕСКИЙ РАСЧЕТ АВТОБУСНОГО АТП»

Поживилов Никита Васильевич,
к.т.н., старший преподаватель, МАДИ, Россия,
nikita.pozhivilov@madi.ru

Максимов Виктор Александрович,
д.т.н., профессор, МАДИ, Россия,
vamaximov57@mail.ru

Крылов Григорий Александрович,
старший преподаватель, МАДИ, Россия,
grigory_a_krylov@mail.ru

Аннотация

В статье рассматриваются особенности проведения технологического расчета автобусного АТП с использованием специально разработанной компьютерной программы, позволяющей в автоматизированном режиме, после ввода исходных данных, получать результаты, в частности, производственную программу обслуживания и ремонта подвижного состава предприятия, распределение работ по производственным подразделениям и др. Рассмотрен интерфейс и основные возможность компьютерной программы «Технологический расчет автобусного АТП». Приводятся скриншоты рабочих окон программы. В программе проведен расчет количества ТО-1 и ТО-2 автобусов одного «условного» Московского АТП, проведено сравнение расчетных значений с фактическими. По результатам анализа приводятся рекомендации руководству АТП по совершенствованию организации и управления технологическими процессами за счет корректировки графика постановки автобусов в ТО-1 и ТО-2.

Ключевые слова: *автобус, АТП, технологический расчет, техническое обслуживание, прогнозирование, подвижной состав, производственная программа обслуживания и ремонта подвижного состава, управление, структура управления*

Введение

Автомобильный парк сегодня существенно отличается от парка 10, 20 летней давности. Автомобили стали более комфортабельными, надежными, безопасными (в том числе и экологически) [1,2, 11-18], но развитие электроники и усложнение конструкции привели к снижению ремонтопригодности и для технического обслуживания (ТО) и текущего ремонта (ТР), зачастую требуется специальное технологическое и диагностическое оборудование.

Изменения в конструкции автомобилей, технологии их ТО и ТР, повышение требований к эксплуатации и безопасности транспортных средств приводят к изменениям структуры управления производственно-технической базой (ПТБ) автотранспортных предприятий (АТП), обновленного распределения работ по рабочим постам и производственным подразделениям, а также потребности в квалифицированном персонале [3,4].

Требования к качеству перевозки пассажиров и грузов автомобильным транспортом постоянно возрастают [5], что вынуждает руководство АТП уделять больше внимание показателям надежности подвижного состава. Показатели безотказности подвижного состава предприятия напрямую зависят от выстроенной системы ТО и ремонта. Управлением этими процессами занимается техническая служба АТП, в обязанности которой входит поддержание в технически исправном состоянии парка автомобилей с заданными показателями надежности.

Для проверки качества и полноты выполнения работ по ТО и ремонту парка автомобилей необходимо проводить комплексную политику управления техническими системами АТП, в том числе давать количественную оценку показателям работы персонала, производственных подразделений (отделов, цехов, участков и т.д.), а также эффективности реализации целей и задач технической службы путем сравнения плановых значений с фактическими.

Технологический расчет АТП позволяет получить целый ряд численных значений параметров, которые позволят провести анализ расхождения плановых (расчетных) значений и фактических показателей работы технической службы АТП.

Одним из этапов технологического расчета является расчет производственной программы технического обслуживания и ремонта подвижного состава. Подобный расчет рекомендуется проводить регулярно, как минимум один раз в год. Проведение расчета в ручном режиме является достаточно трудоемким процессом и сопряжено с возможными ошибками. Научным коллективом кафедры ЭАТиС и кафедры прикладной математики МАДИ была разработана специальная компьютерная программа для автоматизированного технологического расчета автобусного АТП. Программа позволяет при наличии исходных данных по подвижному составу и требуемым характеристикам работы АТП получить выходные данные результатов технологического расчета.

В рамках данной статьи рассмотрены основные этапы и некоторые особенности технологического расчета АТП, компьютерная программа «Технологический расчет автобусного АТП», проведен расчет производственной программы автобусов АТП, расположенного в городе Москве.

Основные этапы технологического расчета АТП

Задачей технологического расчета является определение численности производственных рабочих, количества постов, площадей производственно-технической базы автотранспортного предприятия для организации или совершенствования организации технологического процесса ТО и ТР подвижного состава.

Основные этапы технологического расчета АТП:

1. Сбор исходных данных.

Структура парка АТП, среднесуточный пробег единицы подвижного состав, условия эксплуатации, режимы работы ТО и ремонта подвижного состава и пр.

2. Расчет производственной программы, объемов работ и численности ремонтных рабочих.

Производится расчет на основе исходных данных. В результате расчета определяются:

– периодичность видов ТО, пробег до КР или ресурсный пробег до списания автомобиля, трудоемкость ТО и ТР;

– годовые объемы работ по ТО, ТР и вспомогательных работ АТП и их распределение по производственным подразделениям предприятия;

– численность производственных рабочих;

– численность вспомогательных рабочих.

3. Технологический расчет производственных зон, цехов, участков и складов.

Режим работы АТП и подвижного состава являются основой для технологического расчета различных зон, цехов, участков и складов. В состав расчета входят:

– выбор и обоснование режима работы зон, цехов и участков, методов организации ТО и диагностирования подвижного состава;

– расчет числа постов и линий для ТО и числа постов для текущего ремонта;

– определение состава и расчет площадей производственных, складских помещений, площадей зон хранения и площадей административно-бытовых помещений.

4. Оценка результатов технологического расчета и проектирования.

Производится на основе сопоставления проектных показателей (постов, производственных рабочих, площадей) с фактическими показателями АТП.

При выполнении технологического расчета следует руководствоваться следующими нормативными документами: «Общесоюзные нормы технологического проектирования предприятий автомобильного транспорта» [6], руководства по эксплуатации, технологии обслуживания и ремонта, технологические карты технического обслуживания моделей (модификаций) автомобилей, участвующих в расчетах, другие документы и источники, которые используются на предприятии.

Коэффициенты корректирования К1, К2, К3, К4, К5 соответственно зависят от условий эксплуатации, модификации подвижного состава и организации его работы, природно-климатических условий, пробега с начала эксплуатации и количества обслуживаемых и ремонтируемых автомобилей на АТП и количества технологически совместимых групп подвижного состава.

При проведении технологического расчета надо учитывать тот факт, что некоторые нормативные значения, в том числе периодичность выполнения ТО-1 и ТО-2 для большинства современных моделей и модификаций автобусов указываются производителями в документации и руководствах по эксплуатации уже с учетом климатических условий и категории условий эксплуатации транспорта.

Методические подходы по определению производственной программы технического обслуживания подвижного состава автобусного АТП

Своевременное, полное и качественное выполнение технического обслуживания является необходимым условием безотказной работы автобуса и сохранения гарантийных обязательств.

Техническое обслуживание современных городских автобусов подразделяется на два этапа [7,8]:

– ТО в начальный период эксплуатации;

– ТО в основной период эксплуатации.

В начальный период эксплуатации автобуса выполняются следующие виды обслуживаний:

– ежедневное обслуживание ЕО;

– техническое обслуживание ТО-1000.

В основной период эксплуатации автобуса выполняются следующие виды обслуживаний:

– ежедневное обслуживание ЕО;

– первое техническое обслуживание ТО-1;

– второе техническое обслуживание ТО-2;

– сезонное техническое обслуживание СТО;

– дополнительные операции технического обслуживания.

Работы по техническому обслуживанию являются профилактическими и должны выполняться в обязательном порядке и в указанные сроки.

При проведении технологического расчета АТП рассчитывается производственная программа только видов обслуживания в основной период эксплуатации, так как виды обслуживания в начальный период имеют разовых характер.

Для расчета производственной программы необходимо вычислить годовой пробег группы автобусов по модификациям [9].

Годовой пробег группы ПС по модификациям подсчитывается по формуле:

$$L_{\text{ГП}} = \text{А}_{\text{И}} \cdot L_{\text{Г}}, \text{ км} \quad (1)$$

где $\text{А}_{\text{И}}$ – количество автомобилей конкретной модификации, единиц;

$L_{\text{Г}}$ – среднее значение годового пробега единице ПС конкретной модификации, км.

Также, при необходимости произвести корректировку периодичность ТО-1 и ТО-2.

Скорректированная нормативная периодичность ТО-1 (L_1) или ТО-2 (L_2) рассчитывается по формуле:

$$L_i = L_i^{(\text{Н})} \cdot \text{К}_1 \cdot \text{К}_3, \text{ тыс. км} \quad (2)$$

где $L_i^{(\text{Н})}$ – нормативная периодичность ТО-1 или ТО-2, тыс. км; К_1, К_3 – корректирующие коэффициенты, учитывающие соответственно условия эксплуатации и природно-климатические условия

Необходимо учитывать, что некоторые производители автобусов приводят уже скорректированные нормативы периодичности ТО-1 и ТО-2 для региона эксплуатации.

Годовое число обслуживаний подсчитывается по формулам:

$$\sum N_{\text{ЕОсг}} = \text{А}_{\text{И}} \cdot \text{Д}_{\text{раб.г}} \cdot \alpha_{\text{в}} \quad (3)$$

$$\sum N_{\text{ЕОтг}} = \sum (N_{1\text{г}} + N_{2\text{г}}) \cdot 1{,}6 \quad (4)$$

$$\sum N_{1\text{г}} = L_{\text{ГП}} \cdot \left(\frac{1}{L_1} - \frac{1}{L_2}\right) \quad (5)$$

$$\sum N_{2\text{г}} = L_{\text{ГП}} \cdot \frac{1}{L_1} \quad (6)$$

где $\sum N_{\text{ЕОсг}}$ – годовое число ежедневных обслуживаний, выполняемых при возврате и выпуске ПС на линию;

$\sum N_{\text{ЕОтг}}$ – годовое число ежедневных обслуживаний, выполняемых перед ТО и ТР;

$\sum N_{1\text{г}}$ – годовое число ТО-1;

$\sum N_{2\text{г}}$ – годовое число ТО-2;

1,6 – коэффициент, учитывающий выполнение $N_{\text{ЕОтг}}$ при ТР.

СТО выполняется два раза в год (соответственно весной и осенью) и его проведение совмещается с ближайшим ТО-1 или ТО-2.

Также, стоит отметить, что обычно производители автомобилей, в том числе автобусов, предоставляют информацию о периодичности и трудоемкости ТО-1, ТО-2 и СТО, однако информацию об удельной трудоемкости текущего ремонта не указывают. Это связано с тем, что данное значение фактически не рассчитывается производителями автомобилей, а значение должно быть рассчитано индивидуально с учетом условий эксплуатации подвижного состава конкретного АТП после сбора и обработки исходных данных по отказам, неисправностям и времени их устранения [10].

Описание компьютерной программы «Технологический расчет автобусного АТП»

Компьютерная программа «Технологический расчет автобусного АТП» разработана научным коллективом преподавателей кафедры «Эксплуатация автомобильного транспорта и автосервис» и кафедры «Прикладная математика» Московского автомобильно-дорожного государственного технического университета (МАДИ) и с конца 2020 года работает в тестовом режиме.

После завершения этапа разработки и тестирования, программа будет предназначена в первую очередь для использования студентами, магистрантами и аспирантами МАДИ в учебных целях, однако функционал программы позволит проводить и научно-исследовательскую работу обучающимся и преподавателям университета.

На данный момент в программе реализованы следующие функции:

– выбор уровня доступа (оператор или редактор);

– форма заполнения исходных данных оператора;

– блок исходных данных, включая параметры подвижного состава, распределение годовых объемов работ по видам и режим работы и характеристики постовых работ);

– основные результаты ручного расчета;

– результаты расчета (реализована функция расчета производственной программы);

– справочная информация.

В справочной информации сформирована база данных модификаций автобусов и характеристик, необходимых для проведения технологического расчета АТП, таких как периодичность ТО-1, ТО-2, трудоемкость выполнения работ ЕО, ТО-1, ТО-2, СО, ТР и другая информация (рис. 1.)

МОДИФИКАЦИИ (МАРКИ) АВТОБУСОВ — Last UpDate 19.02.2021

Выбор | Новый | Изменить | Удалить | Печать | Выход

Наименование модификации	Тип	Вид топлива	$L^{(Н)}_{КР}$, км	$L^{(Н)}_{ТО-1}$, км	$L^{(Н)}_{ТО-2}$, км	$Д^{(Н)}_{ТО-ТР}$ д/т.км	Трудоемкости ТО (чел-ч), ТР (чел-ч/1000 км)							Км	Габариты, м	
							ЕОс	ЕОт	ТО-1	ТО-2	ТР	СО осень	СО зима		длина	ширина
Fiat Ducato	МВ	Дизель	250000	5000	20000	0.25	0.89	0.89	3.60	7.10	4.18	8.42	8.42	0.60	0.000	0.000
Mercedes Benz Conecto	БВ	Дизель	800000	10000	20000	0.35	1.20	1.20	6.40	29.30	6.23	18.20	18.20	0.60	0.000	0.000
Волжанин-5270	БВ	Дизель	480000	10000	20000	0.35	1.20	1.20	6.40	24.10	6.00	15.98	15.98	0.60	0.000	0.000
Волжанин-6270	ОБВ	Дизель	480000	10000	20000	0.45	0.77	0.77	7.17	26.48	5.87	11.36	11.36	0.60	0.000	0.000
Голаз-525110	БВ	Дизель	800000	22500	45000	0.50	1.41	1.41	6.65	12.87	6.33	7.98	8.00	0.60	0.000	0.000
Голаз-6228	ОБВ	Дизель	400000	5000	20000	0.45	1.70	1.70	9.92	21.10	11.27	13.29	13.29	0.60	0.000	0.000
ЛиАЗ-429260	СВ	Дизель	800000	15000	30000	0.40	1.02	1.02	5.07	21.03	4.20	9.40	9.04	0.60	9.500	2.500
ЛиАЗ-5256	БВ	Дизель	400000	5000	20000	0.50	0.67	0.67	9.48	29.10	5.35	15.75	6.00	0.60	11.400	0.250
ЛиАЗ-529220	БВ	Дизель	600000	10000	20000	0.50	1.28	1.28	6.68	24.47	6.00	18.51	18.64	0.60	0.000	0.000
ЛиАЗ-529221	БВ	Дизель	600000	10000	20000	0.50	1.28	1.28	6.68	24.47	6.00	18.51	18.64	0.60	0.000	0.000
ЛиАЗ-529222	БВ	Дизель	800000	10000	20000	0.50	1.28	1.28	6.68	24.47	6.00	18.51	18.64	0.60	11.900	2.500
ЛиАЗ-529265	БВ	Дизель	800000	15000	30000	0.50	0.98	0.98	5.51	23.70	6.00	9.80	9.80	0.60	0.000	0.000
ЛиАЗ-529271	БВ	Газ (Метан)	800000	10000	20000	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60	0.000	0.000
ЛиАЗ-529271-79	БВ	Газ (Метан)	800000	10000	20000	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60	0.000	0.000
ЛиАЗ-52937	БВ	Дизель	400000	5000	20000	0.35	1.70	1.70	9.54	29.20	9.04	17.53	17.53	0.60	0.000	0.000
ЛиАЗ-621320	ОБВ	Дизель	600000	10000	20000	0.55	1.58	1.58	7.68	30.07	9.60	19.25	19.38	0.60	0.000	0.000
ЛиАЗ-621321	ОБВ	Дизель	600000	10000	20000	0.55	1.58	1.58	7.68	30.07	9.60	19.25	19.38	0.60	0.000	0.000
ЛиАЗ-621322	ОБВ	Дизель	800000	10000	20000	0.55	1.50	1.58	7.68	30.07	9.60	19.25	19.38	0.60	18.040	2.500
ЛиАЗ-621365	ОБВ	Дизель	800000	15000	30000	0.55	1.57	1.57	5.79	22.78	9.60	13.88	13.76	0.60	0.000	0.000
ЛиАЗ-621371	ОБВ	Газ (Метан)	800000	10000	20000	0.55	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60	0.000	0.000
МАЗ-103	БВ	Дизель	600000	7000	30000	0.35	1.20	1.20	12.43	28.22	6.57	13.29	13.29	0.60	0.000	0.000
МАЗ-107	ОБВ	Дизель	600000	10000	30000	0.45	1.32	1.32	10.00	36.72	8.68	15.15	15.15	0.60	0.000	0.000
Наименование Марки	?	Дизель	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.000	0.000

Рис. 1. Справочная информация характеристик автобусов по модификациям компьютерной программы «Технологический расчет автобусного АТП»

По состоянию на январь 2021 года произведена проверка корректности работы программы по части получения данных годовой производственной программы по ТО и ТР автобусов. В 2021 году планируется продолжить работу по модернизации и совершенствования программы по другим этапам технологического расчета.

Расчет производственной программы технического обслуживания подвижного состава автобусного АТП в городе Москве

Для проверки соблюдения в 2020 году графика выполнения работ по техническому обслуживанию (ТО-1 и ТО-2) подвижного состава автобусного АТП, расположенного на территории Москвы необходимо было сравнить фактические данные выполнения ТО-1 и ТО-2, а также расчетные данные производственной программы технического обслуживания. В целях экономии времени, а также исключения ошибок ручного расчета для проведения расчета производственной программы использовалась программа автоматизированного расчета «Технологический расчет автобусного АТП».

На первом этапе из базы данных АТП выгружались данные по подвижному составу по модификациям, затем данные обобщались, группируя по модификациям автобусов и представлялись в виде сводной таблицы (табл. 1).

Таблица 1

Исходные данные о подвижном составе АТП в 2020 году для проведения технологического расчета

Модификация автобуса	Списочное количество, $A_И$, единиц	Среднее значение накопленного пробега на начало периода, $L_{Н.Э.}$, км	Среднее значение накопленного пробега на конец периода, $L_{Н.Э.}$, км	Среднее значение пробега автобуса за период, $L_Г$, км
ГОЛАЗ 525110	18	533 904	621 270	72 848
ЛиАЗ 429260	48	208 754	268 841	60 087
ЛиАЗ 525613	11	589 270	642 394	53 124
ЛиАЗ 529221	107	539 792	587 161	47 369
ЛиАЗ 529222	111	480 675	547 383	66 708
ЛиАЗ 529265	33	238 638	325 704	87 066
ЛиАЗ 621320	8	532 988	548 140	15 152
ЛиАЗ 621321	55	528 931	572 334	43 402
ЛиАЗ 621322	28	436 686	501 623	64 937
Лиаз 621365	43	111 525	179 377	67 851

На втором этапе исходные данные по подвижному составу и пробегам вносились в программу «Технологический расчет автобусного АТП» (рис. 2). Сформированные исходные данный о подвижном составе АТП представлены на рис. 3.

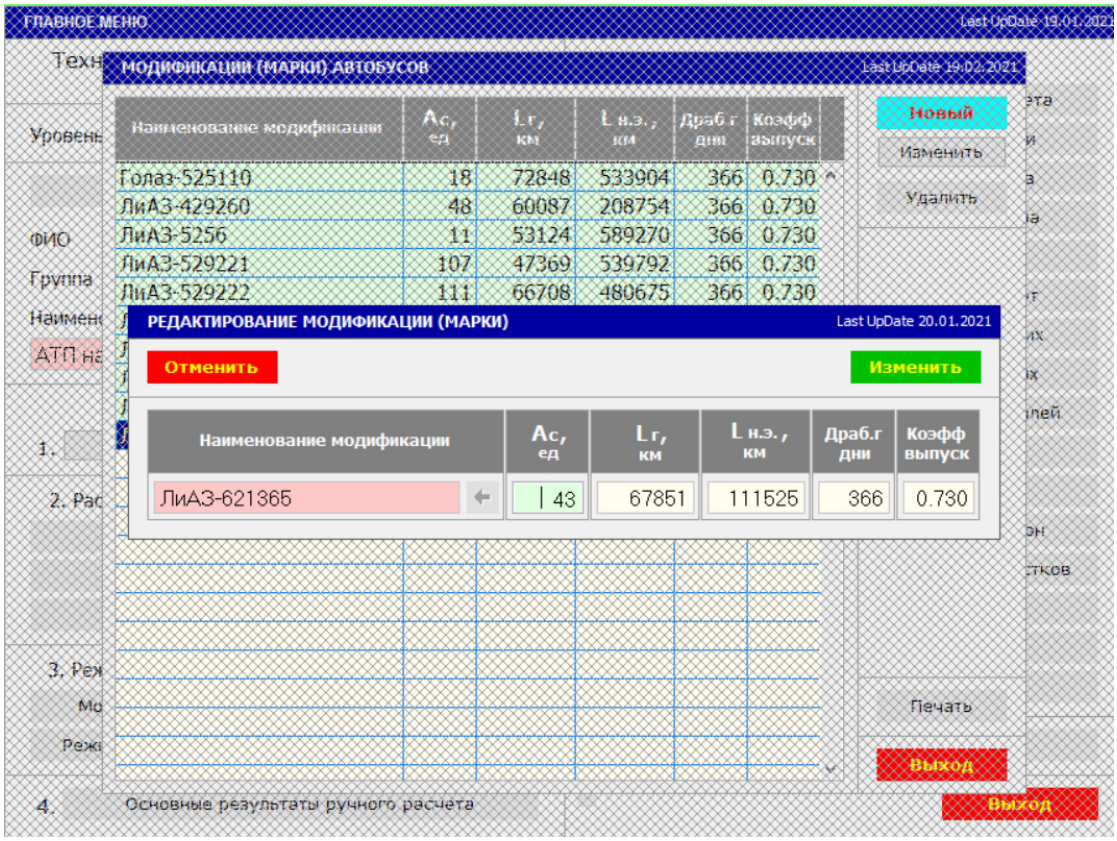


Рис. 2. Окно внесения исходных данных о подвижном составе АТП в программе «Технологический расчет автобусного АТП»

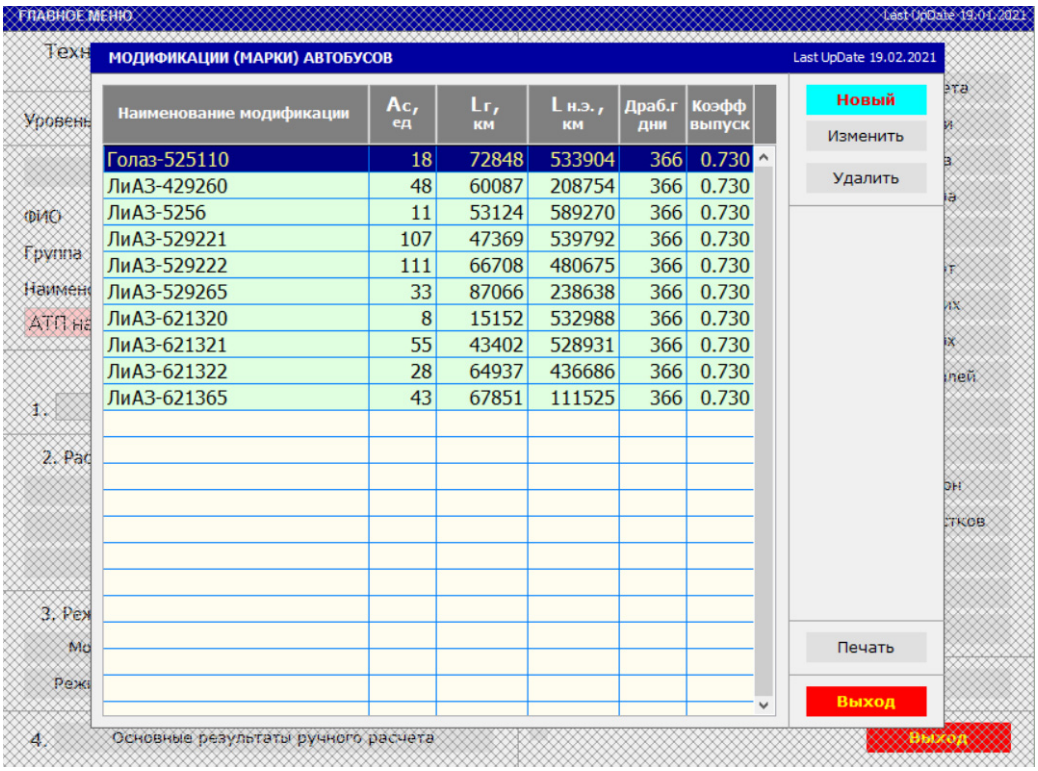


Рис. 3. Окно сформированных исходных данных о подвижном составе АТП в программе «Технологический расчет автобусного АТП»

На третьем этапе вносились исходные данные о режиме работы АТП в 2020 году – число дней работы всех подразделений АТП составило 366 дней (рис. 4).

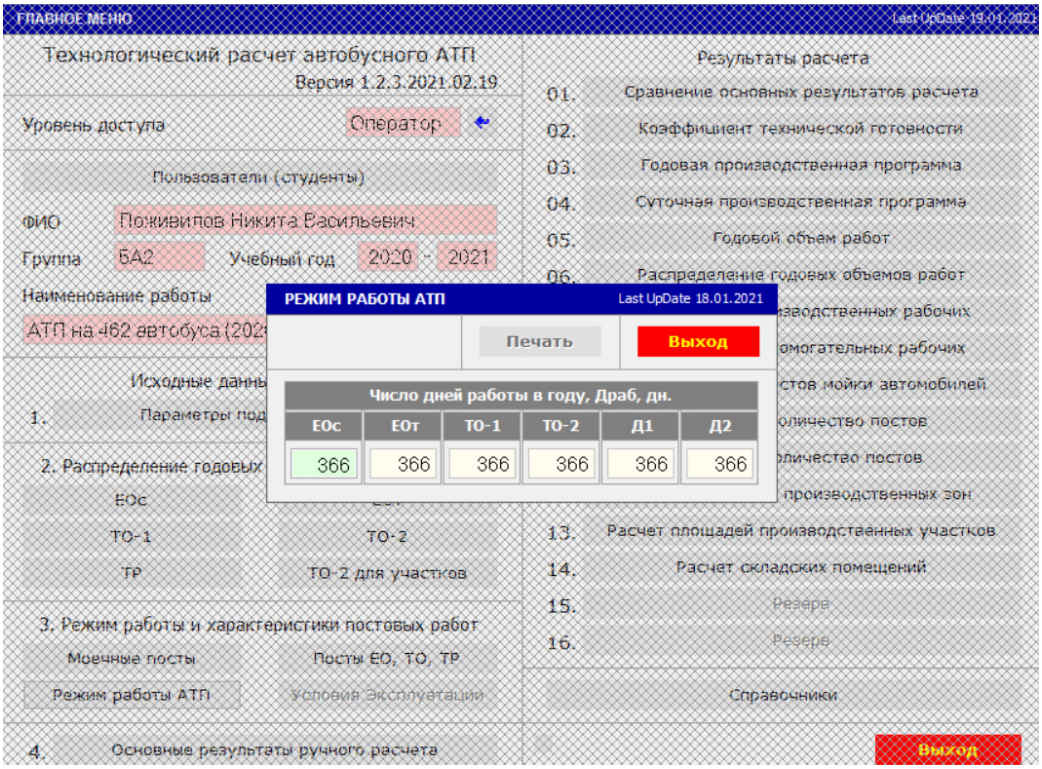
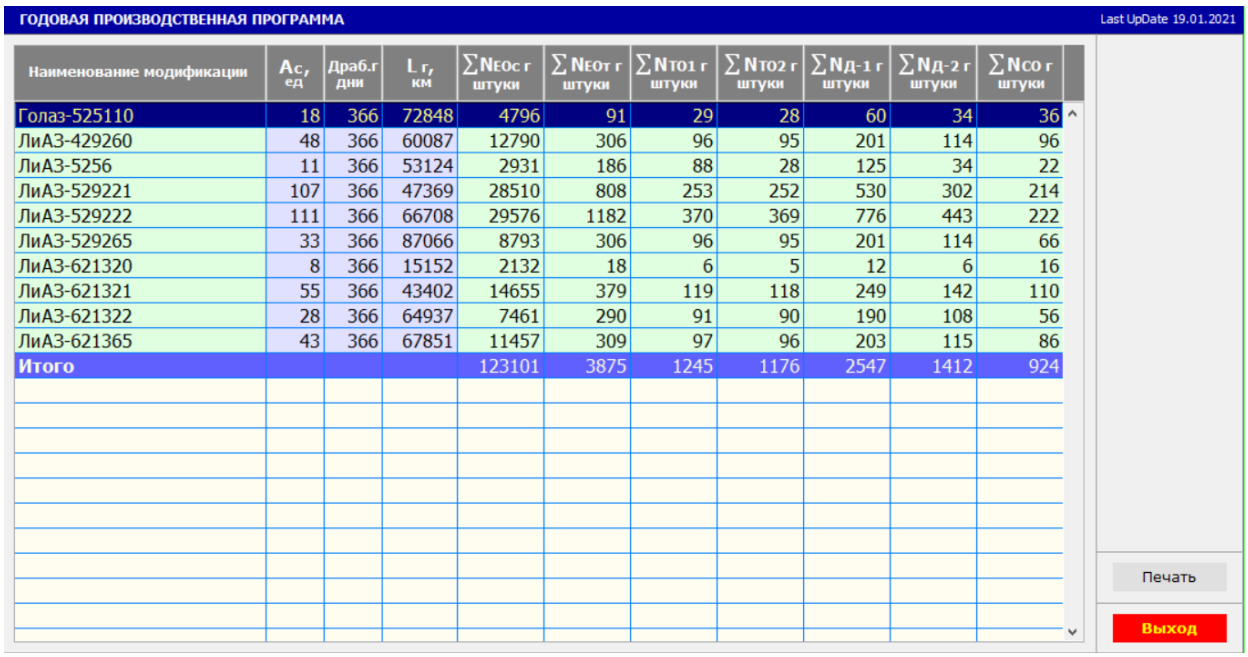


Рис. 4. Окно исходных данных по режиму работы АТП в программе «Технологический расчет автобусного АТП»

На четвертом этапе в автоматизированном режиме были получены расчетные данные годовой производственной программы работы по видам технического обслуживанию автобусов по модификациям (рис. 5).



Наименование модификации	Ac, ед	Драб.г дни	Lг, км	∑NЕОс г штуки	∑NЕОт г штуки	∑NТО1 г штуки	∑NТО2 г штуки	∑Nд-1 г штуки	∑Nд-2 г штуки	∑Nсо г штуки
Голаз-525110	18	366	72848	4796	91	29	28	60	34	36
ЛиАЗ-429260	48	366	60087	12790	306	96	95	201	114	96
ЛиАЗ-5256	11	366	53124	2931	186	88	28	125	34	22
ЛиАЗ-529221	107	366	47369	28510	808	253	252	530	302	214
ЛиАЗ-529222	111	366	66708	29576	1182	370	369	776	443	222
ЛиАЗ-529265	33	366	87066	8793	306	96	95	201	114	66
ЛиАЗ-621320	8	366	15152	2132	18	6	5	12	6	16
ЛиАЗ-621321	55	366	43402	14655	379	119	118	249	142	110
ЛиАЗ-621322	28	366	64937	7461	290	91	90	190	108	56
ЛиАЗ-621365	43	366	67851	11457	309	97	96	203	115	86
Итого				123101	3875	1245	1176	2547	1412	924

Рис. 5. Окно результатов расчета производственной программы подвижного состава по модификациям и видам обслуживания в программе «Технологический расчет автобусного АТП»

На пятом этапе были выгружены фактические данные производственной программы обслуживания ТО-1 и ТО-2 по модификациям автобусов АТП за 2020 год. Полученные данные группировались аналогично расчетным и представлялись в сводной таблице (табл. 2)

Таблица 2

Результаты сравнения расчетных и фактических значений производственной программы ТО-1 и ТО-2 линейных автобусов АТП в 2020 году

Модификация автобуса	ТО-1, шт.			ТО-2, шт.		
	расчет	факт	расхождение, %	расчет	факт	расхождение, %
ГОЛАЗ-525110	29	24	-17,2%	28	20	-28,6%
ЛиАЗ-429260	96	108	+12,5%	95	104	+9,5%
ЛиАЗ-525613	88	77	-12,5%	28	28	0,0%
ЛиАЗ-529221	253	255	+0,8%	252	261	+3,6%
ЛиАЗ-529222	370	436	+17,8%	369	329	-10,8%
ЛиАЗ-529265	96	118	+22,9%	95	88	-7,4%
ЛиАЗ-621320	6	4	-33,3%	5	0	-100,0%
ЛиАЗ-621321	119	115	-3,4%	118	119	+0,8%
ЛиАЗ-621322	91	72	-20,9%	90	75	-16,7%
ЛиАЗ-621365	97	99	+2,1%	96	95	-1,0%
ВСЕГО	**1245**	**1308**	**+5,1%**	**1176**	**1119**	**-4,8%**

На шестом этапе проводился анализ полученных результатов сводной таблицы сравнения расчетных и фактических значений производственной программы ТО-1 и ТО-2 линейных автобусов по модификациям.

По результатам расчета производственной программы ТО-2 удовлетворительные результаты отклонения фактических значений проведения ТО-2 от расчетных составили менее 10%, что является допустимым результатом, для следующих модификаций автобусов:

– ЛиАЗ-429260;
– ЛиАЗ-525613;
– ЛиАЗ-529221;
– ЛиАЗ-529265;
– ЛиАЗ-621321;
– ЛиАЗ-621365.

Отклонение фактических значений от плановых превысило 10% для следующих модификаций автобусов:

– ГОЛАЗ-525110;

– ЛиАЗ-529222;
– ЛиАЗ-621320;
– ЛиАЗ-621322

Аналогичный анализ для ТО-1 показал удовлетворительный показатель (расхождение в пределах 10%) лишь для трех модификаций автобусов:

– ЛиАЗ-529221;
– ЛиАЗ-621321;
– ЛиАЗ-621365.

Остальные модификации фактически проходят ТО-1 с отклонением от нормативных значений.

Стоит отметить, что для некоторых модификаций наличие расхождения факт-план выполнения ТО-1 и ТО-2 могут быть обоснованы, например, для модификации ЛиАЗ-621320, автобусы которой за рассматриваемый период 2020 год были полностью списаны, а значит плановые технические обслуживания, приходящиеся на завершающем этапе эксплуатации подвижного состава в АТП, могли не выполняться. Данные факторы объясняют значительные отклонения фактических значений от расчетных.

Также, стоит отметить, что небольшое количество автобусов одной модификации при расчете влияет на снижение достоверности данных, как в случае с автобусами ГОЛАЗ-525110 с общей численностью 18 единиц и достаточно большими интервалами периодичностью ТО-1 и ТО-2.

Значительные же расхождения фактических и расчетных значений проведения ТО-1 и ТО-2 для модификаций автобусов с большой численностью требуют внимания руководства АТП, в частности, центра управления производством для выявления причин и своевременного их устранения.

Завершающим этапом расчета стали рекомендации руководству АТП следующего содержания:

1. На АТП в целом наблюдается соблюдение графика проведения ТО-2 автобусов, за исключением автобусов модификаций ЛиАЗ-529222 и ЛиАЗ-621322. Рекомендуется выявить причины снижения на 10,8% и 16,7% соответственно количества фактически проведенных ТО-2.
2. Выполнение графика ТО-1 происходит хуже, чем выполнение графика ТО-2. Допустимые границы отклонений имеют лишь модификации ЛиАЗ-529221, ЛиАЗ-621321 и ЛиАЗ-621365.
3. По АТП в целом наблюдается незначительное отклонение фактического графика выполнения ТО-1 (+5,1%) и ТО-2 (-4,8%) от планового (расчетного) значения, что дает основание предположить, что корректирование графика постановки автобусов в ТО-1 и ТО-2 может быть перераспределено между модификациями без увеличения загруженности технической службы АТП.
4. Рекомендовано проводить подобные расчеты на регулярной основе для количественной оценки качества постановки автобусов в ТО-1 и ТО-2 и своевременного реагирования, и принятия управленческих мер на устранение негативных причин.

Заключение

1. Для анализа результатов работы технической службы АТП по части выполнения производственной программы по ТО и ТР подвижного состава необходимо выполнять технологических расчет АТП. Ручной расчет является достаточно трудоемким и сопряжен с возможными ошибками. Целесообразно разработать компьютерную программу, которая позволит в автоматизированном режиме проводить технологический расчет.
2. Научным коллективом научным коллективом преподавателей кафедры «Эксплуатация автомобильного транспорта и автосервис» и кафедры «Прикладная математика» Московского автомобильно-дорожного государственного технического университета (МАДИ) была разработана компьютерная программа «Технологический расчет автобусного АТП», которая позволяет в автоматизированном режиме производить расчет производственной программы обслуживания автобусов АТП, что дает возможность проводить расчеты для контроля показателей за прошедшие периоды и прогнозирования работы на плановые периоды работы АТП. На данный момент в программе реализована функция расчета производственной программы ТО и ремонта автомобилей АТП при вводе исходных данных.
3. Проведен расчет производственной программы обслуживания автобусов в «условном» Московском АТП, в результате выявлены незначительные отклонения фактического значения общего количества ТО-1 (+5,1%) и ТО-2 (-4,8%) от расчетного в разработанной компьютерной программе. Однако по отдельным модификациям автобусов наблюдаются значительные отклонения факта от нормы, например, для ТО-2 ЛиАЗ-529222 значения ниже на 10,8% и для ЛиАЗ-621322 ниже на 16,7%.
4. Руководству АТП рекомендуется на регулярной основе с периодичностью не реже 1 раза в полгода проводить подобный расчет, отслеживая результаты управленческих решений по корректировке графика постановки в ТО-1 и ТО-2. В первую очередь рекомендуется обратить внимание на автобусы модификаций значительной численности и с наибольшей долей отклонений фактических значений от расчетных, для ТО-2 это ЛиАЗ-621322, для ТО-1 это ЛиАЗ-529265 и ЛиАЗ-621322.
5. Программа «Технологический расчет автобусного АТП» требует дальнейшей доработки и тестирования в других этапах технологического расчета: расчет плановых значений коэффициента технической готовности, расчет необходимой численности ремонтных рабочих, постов для обслуживания и ремонта, площадей производственных и складских помещений и прочее. В результате программа может позволить рассчитывать целый ряд параметров работы для проверки качества работы АТП как за прошедший, так и на плановый период.

Литература

1. *Ватолина Е.В., Кадырова Н.Ю*. Исследование параметров экономичности и экологичности автомобилей // Материалы X международной научно-практической конференции, посвященной 85-летию со дня рождения д. т. н., профессора Л.Г. Резника: в 2 томах, 2017. С. 21-26.
2. *Азаров В.К., Гайсин С.В., Кутенёв В.Ф*. Концепция разработки универсальной методики объективной оценки комплексной безопасности автомобиля по обеспечению безопасности водителя, пассажиров и пешеходов // Журнал автомобильных инженеров, 2017. С. 44-48.
3. *Pozhivilov N.V., Maksimov V.A., Krylov G.A. and Zavgorodniy A.A*. Maintenance and repair management taking into account specialization, cooperation and unification within a united bus company consisting of several branches // *IOP Conference Series: Materials Science and Engineering*.Vol. 832, 2020. https://iopscience.iop.org/article/10.1088/1757-899X/832/1/012065.
4. *Поживилов Н.В., Крылов Г.А., Максимов В.А.* Модель рационального размещения производства ремонтно-профилактических воздействий в объединении автобусного транспорта // Актуальные проблемы эксплуатации автотранспортных средств: материалы XX Междунар. науч. практ. конф. Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. Владимир: Изд-во ВлГУ, 2018. С. 79-84.
5. Постановление Правительства РФ от 01.10.2020 N 1586 "Об утверждении Правил перевозок пассажиров и багажа автомобильным транспортом и городским наземным электрическим транспортом".
6. ОНТП-01-91, Общесоюзные нормы технологического проектирования предприятий автомобильного транспорта - М: Гипроавтотранс, 1991.
7. Автобус ЛиАЗ-429260. Руководство по эксплуатации. ООО «Ликинский автобусный завод», г. Ликино-Дулево. 2016 г. - 389 с.
8. Автобус ЛиАЗ-529265. Технология технического обслуживания. ООО «Ликинский автобусный завод», г. Ликино-Дулево. 2016. 230 с.
9. *Напольский Г.М.* Технологическое проектирование автотранспортных предприятий и станций технического обслуживания: 2-е изд. перераб. и доп. М.: Транспорт, 1993. 271 с.
10. *Максимов В.А., Поживилов Н.В., Павлий Я.А., Чокля А.В.* Определение удельной трудоемкости текущего ремонта автобусов ЛиАЗ-529222 // Грузовик. М., 2017. №8. С.10-13.
11. *Гулямов К.Х., Гуломзода А.Х.* Разработка и исследование повышающего преобразователя постоянного напряжения // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 4 (51). С. 55-61.
12. *Карелина М.Ю., Арифуллин И.В., Терентьев А.В*. Аналитическое определение весовых коэффициентов при многокритериальной оценке эффективности автотранспортных средств // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 3-9.
13. *Долина О.Н., Жидкова М.А., Шпилькина Т.А., Ахметжанова Э.У*. Реализация политики импортозамещения в автомобильной промышленности // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 2 (49). С. 22-28.
14. *Пузаков А.В., Осаулко Я.Ю.* Исследование влияния эксплуатационных факторов на тепловое состояние автомобильного генератора // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 16-23.
15. *Надараиа Ц.Г., Селиванов А.И., Шестаков И.Я., Фадеев А.А., Бабкина Л.А*. Химико-кинетический накопитель энергии и мотор-редуктор для электромобиля // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 1 (48). С. 12-17.
16. *Козлов А.Н.* Организация безопасной эксплуатации тяговой литий-ионной аккумуляторной батареи на транспортном средстве // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2016. № 1 (44). С. 14-19.
17. *Мельникова Т.Е., Мельников С.Е., Завязкина В.В.* Электромобили: перспективы и пути развития // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2019. № 3 (58). С. 22-26.
18. *Блудян Н.О.* Перспективы развития электрических автобусов // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2020. № 3 (62). С. 19-24.

CALCULATION OF THE PRODUCTION PROGRAM FOR MAINTENANCE OF THE ROLLING STOCK OF ATP BASED ON THE RESULTS OF THE CALCULATION IN THE "TECHNOLOGICAL CALCULATION OF THE BUS ATS"

Nikita V. Pozhivilov,
Cand. tech. Sci., Senior Lecturer, MADI, Russia,
nikita.pozhivilov@madi.ru

Viktor A. Maksimov,
doctor. tech. Sci., Professor, MADI, Russia,
vamaximov57@mail.ru

Grigory A. Krylov,
senior lecturer, MADI, Russia,
grigory_a_krylov@mail.ru

Abstract

The article discusses the features of the technological calculation of the bus ATP using a specially developed computer program that allows, in an automated mode, after entering the initial data, to obtain results, in particular, the production program for the maintenance and repair of the rolling stock of the enterprise, the distribution of work by production divisions, etc. The interface and the main capabilities of the computer program "Technological calculation of the bus ATP" are considered. Screenshots of the working windows of the program are provided. The program calculates the number of TO-1 and TO-2 buses of one "conditional" Moscow ATP, compares the calculated values with the actual ones. Based on the results of the analysis, recommendations are made to the ATP management to improve the organization and management of technological processes by adjusting the schedule for placing buses in TO-1 and TO-2.

Keywords: *bus, ATP, technological calculation, forecasting, production program of maintenance and repair of rolling stock, management structure.*