НАУЧНЫЙ ЖУРНАЛ

ТЕЛЕКОММУНИКАЦИИ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

№2-2020

(*Дата издания: декабрь 2020 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 №2-2020

«Цифровые технологии радиосвязи и телерадиовещания»

«Сетевые технологии и системы телекоммуникаций»

ПРОТОКОЛЫ И СТАНДАРТЫ ПЕРЕДАЧИ МЕДИАКОНТЕНТА ПО IP-СЕТЯМ

Валицкая Наталья Сергеевна,
магистрант МТУСИ, Москва, Россия
nvalitskaya@mail.ru
Власюк Игорь Викторович,
доцент кафедры ТиЗВ МТУСИ, к.т.н., Москва, Россия
ru3dlp@yandex.ru

Ключевые слова: Передача медиаконтента, IP, UDP, RTP, MPEG TS, SMPTE ST 2022, SMPTE ST 2110, ASPEN, NDI, Sony NMI.

В настоящее время в телевизионном вещании наблюдается тенденция перехода с SDI на IP-инфраструктуру. Данная работа посвящена анализу методов доставки медиаконтента по IP-сетям. Посчитаны накладные расходы, обусловленные пакетной передачей медиаконтента. Проанализированы преимущества и недостатки методов доставки данных. Приведены схемы передачи медиаконтента в соответствии со стандартами SMPTE ST 2022, SMPTE ST 2110, ASPEN, NDI и Sony NMI и сравнительная характеристика стандартов.

Введение

Для передачи медиаконтента в профессиональном телепроизводстве, как правило, используется SDI-интерфейс. В то же время, телевидение движется в сторону повышения скорости передачи контента: появляются видео разрешением 4К, 8К и более, внедрение HDR и HFR, требующие передачи большего количества данных, а с повышением скорости передачи растет количество необходимых кабелей SDI для передачи одного видеопотока: для передачи несжатого 4К-видеоконтента используется 4x3G-SDI. Существует интерфейс 12G-SDI, позволяющий транслировать видео разрешения 4К по одному кабелю, однако такой вариант предъявляет высокие требования к коаксиальным кабелям и, самое главное, к условиям их эксплуатации, что ограничивает распространение этого стандарта и при этом все равно не позволяет использовать одну линию связи в новейших стандартах.

Перспективным направлением развития техники производства телевизионной продукции является переход на IP-инфраструктуру, что позволяет упростить и сделать более гибкой структуру распределения и коммутации аудио- и видеоданных как в пределах телецентров, так и при работе с внешними линиями. В таком случае физический уровень отделен от логического, нет необходимости в соединении с помощью кабелей всех источников со всеми потребителями, используется коммутация пакетов. На данный момент процесс стандартизации IP-технологий передачи медиаконтента еще идет, существует несколько конкурирующих стандартов, которые постоянно актуализируются и каждый из них при этом имеет свои недостатки.

Поэтому в настоящее время представляется целесообразным провести сравнительный анализ стандартов для передачи медиаконтента студийного качества для делопроизводственных комплексов с целью выявления преимуществ определенных стандартов и технологий в конкретных условиях, а также сравнить указанные стандарты с позиции накладных расходов используемых стеков протоколов с учетом преимуществ, которые дает введение указанных дополнительных данных. Такой анализ будет способствовать осуществлению обоснованного выбора стандарта и соответствующего оборудования вещателями, а также позволит выявить целесообразность дальнейшего совершенствования технологии передачи метаданных в процессе телевизионного производства как на прикладном уровне (видео – и

аудиокодеки), так и на уровнях протоколов передачи данных (обеспечение точности синхронизации и временного тактирования потоков при воспроизведении, контроля и восстановления данных и т.п.)

Протоколы передачи медиаконтента

В IP-сетях используются три основных метода передачи пакетов трафика: unicast (передача данных от одного источника к одному получателю), multicast (передача пакетов группе адресатов - наиболее популярный вид маршрутизации в IPTV) и broadcast (данные принимаются всеми пользователями локальной сети) [1].

Для передачи медиаконтента по IP-сетям данные инкапсулируются в RTP, UDP и IP-пакеты, либо могут дополнительно использоваться транспортные потоки MPEG. Структура IP-пакета показана на таблице 1.

Таблица 1

Структура IP-пакета

IP-пакет (максимальная длина при передаче по Ethernet 1500 байтов)			
IP-заголовок (20 байтов)	UDP-заголовок (8 байтов)	RTP-заголовок (12 байтов)	Нагрузка RTP-пакета, например, 7 TS-пакетов MPEG по 188 байтов каждый (4 байта – заголовок, 184 – полезная нагрузка)

Вместе с RTP используется протокол контроля RTCP (Real-Time Transport Control Protocol) для определения качества обслуживания QoS (quality of service). В отличие от RTP протокол RTCP не передает медиаданные. Приложение может использовать информацию о времени задержки, потере пакетов, предоставляемую RTCP, для управления параметрами качества обслуживания, например, путем ограничения потока. Занимаемая полоса пропускания обычно около 5% от общей пропускной способности сеанса.

Полезной нагрузкой RTP-пакета могут быть пакеты транспортных потоков MPEG. MPEG TS (Transport Streams) – протокол передачи видео, звука и метаданных, описанный в стандарте MPEG2. TS – медиаконтейнер, инкапсулирующий пакеты элементарных потоков PES (Packetized elementary stream) и других данных. Элементарные потоки делятся на пакеты для введения в них сигналов синхронизации. Длина пакетов транспортных потоков равна 188 байтам (4 байта – заголовок, 184 – полезная нагрузка). PES-пакеты имеют заголовок, равный одному байту (8 бит), который должен совпадать с началом нагрузки транспортного пакета (для видео с B-кадрами размер заголовка равен 13 бит). Некоторые транспортные пакеты включают в себя необязательные поля адаптации, которые могут содержать 5 флагов, информацию о синхронизации, байты заполнения и т.д. Для синхронизации транспортных потоков используются PCR-метки (Program Clock Reference): в полях адаптации заголовков TS пакетов содержится информация о значении опорной частоты программы и кодера, которое должно находиться в пределах 27 МГц ± 810 Гц [2].

Как следует из рисунка 1, пакет состоит из заголовка и полезной нагрузки. Байты заголовков являются дополнительной тратой пропускной способности [3]. Посчитаем накладные расходы в соответствии с формулой 1.

$$C = \frac{\sum_{i=1}^{n} b_i}{b_{sum}} * 100\%, \quad (1)$$

где b_i – накладные расходы i-того протокола (заголовки, трейлеры и т.п.), байт; b_{sum} – длина IP-пакета, байт; n – количество протоколов, используемых в методе передачи данных; C – накладные расходы, %.

Накладные расходы для метода RTP/UDP/IP показывает формула 2.

$$C_1 = \frac{\sum_{i=1}^{3} b_i}{b_{sum1}} * 100\% = \frac{20+8+12}{1500} * 100\% = 2.7\%. \quad (2)$$

При использовании метода TS/RTP/UDP/IP длина IP-пакета меньше, поскольку нагрузка RTP-пакета состоит из пакетов транспортных потоков фиксированной длины. Нетрудно подсчитать, что при длине пакета MPEG TS 188 байтов с учетом ограничений, накладываемых Ethernet на размер

пакета и требования к неразрывности пакета MPEG TS, в полезной нагрузке IP-пакета не может быть больше семи пакетов MPEG TS. Тогда накладные расходы определяются по формуле 3:

_____ _____ . (3)

Данные расчеты показывают, что метод TS/RTP/UDP/IP имеет дополнительные расходы выше, чем RTP/UDP/IP.

RTP может восстановить порядок следования пакетов на большом интервале, однако, точность синхронизации недостаточно высокая, поэтому предпочтительнее дополнительно использовать транспортные потоки MPEG. Точность формирования PCR-меток, применяемых в MPEG TS, определяется частотой генератора: 1/27 МГц ≈ 37 нс.

Существует несколько конкурирующих стандартов передачи медиаданных по IP-сетям, которые будут рассмотрены далее.

Стандарты передачи медиаконтента

SMPTE 2022-2 и SMPTE 2022-4 описывают процесс инкапсуляции транспортных потоков MPEG в RTP, UDP и IP-пакеты с постоянным и переменным битрейтом соответственно.

Согласно стандарту SMPTE ST 2022-6, для передачи SDI сигналов форматов SD/HD/3G сперва производится их инкапсуляция в протокол HBRMT (High-Bitrate Media Transport Protocol), затем - в RTP, UDP и IP-пакеты [4]. Стандарт SMPTE ST 2022-6 предполагает передачу видео, звука и метаданных единым потоком. Недостаток данного способа транспортировки медиаконтента по IP-сетям заключается в необходимости эмбеддирования/деэмбеддирования аудиоданных для их обработки. Схема передачи данных по стандарту SMPTE ST 2022-6 показана на рисунке 1.

Рис. 1. Схема передачи данных по стандарту SMPTE ST 2022-6

В стандарте SMPTE ST 2022-5 предусмотрено наличие FEC [5]. Метод коррекции ошибок показан на рисунке 2. Одним из простых способов обнаружения/исправления ошибок является операция контроля четности, которая математически описывается с помощью побитовой логической операции XOR (исключающего «ИЛИ», т.е. сложения по модулю 2). Этот процесс может быть реализован над RTP-пакетами, если обрабатывать их как поток битов.

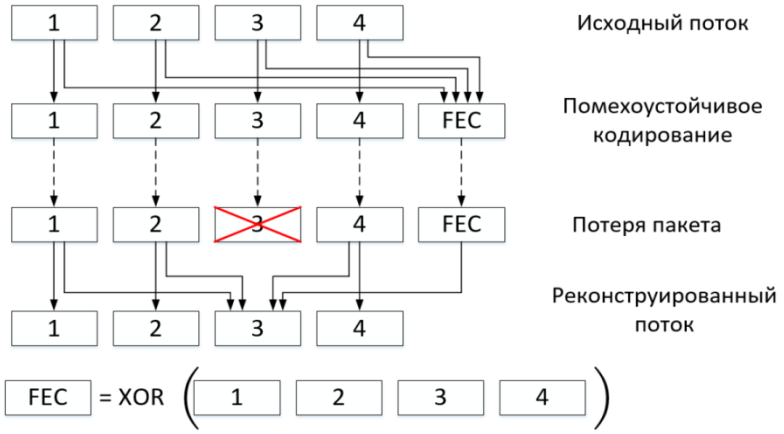


Рис. 2. Помехоустойчивое кодирование в стандарте SMPTE ST 2022-5

В стандарте SMPTE ST 2022-7 один и тот же поток может передаваться получателю двумя разными маршрутами [6]. В случае потери пакетов, например, основного потока, приемник автоматически переключается на резервный. В итоге на выходе имеем все необходимые данные, несмотря на то, что были потеряны пакеты основного потока. Данный процесс проиллюстрирован на рисунке 3.

В отличие от SMPTE ST 2022-6, стандарт SMPTE ST 2110 предполагает передачу видео, звука и метаданных тремя независимыми потоками, что исключает необходимость эмбеддирования/деэмбеддирования звука для его обработки. Стандарт состоит из нескольких документов, описывающих, например, передачу видео (ST 2110-20) [7], аудио (ST 2110-30) [8] и метаданных (ST 2110-40) [9]. Схема передачи данных по стандарту SMPTE ST 2110 показана на рисунке 4.

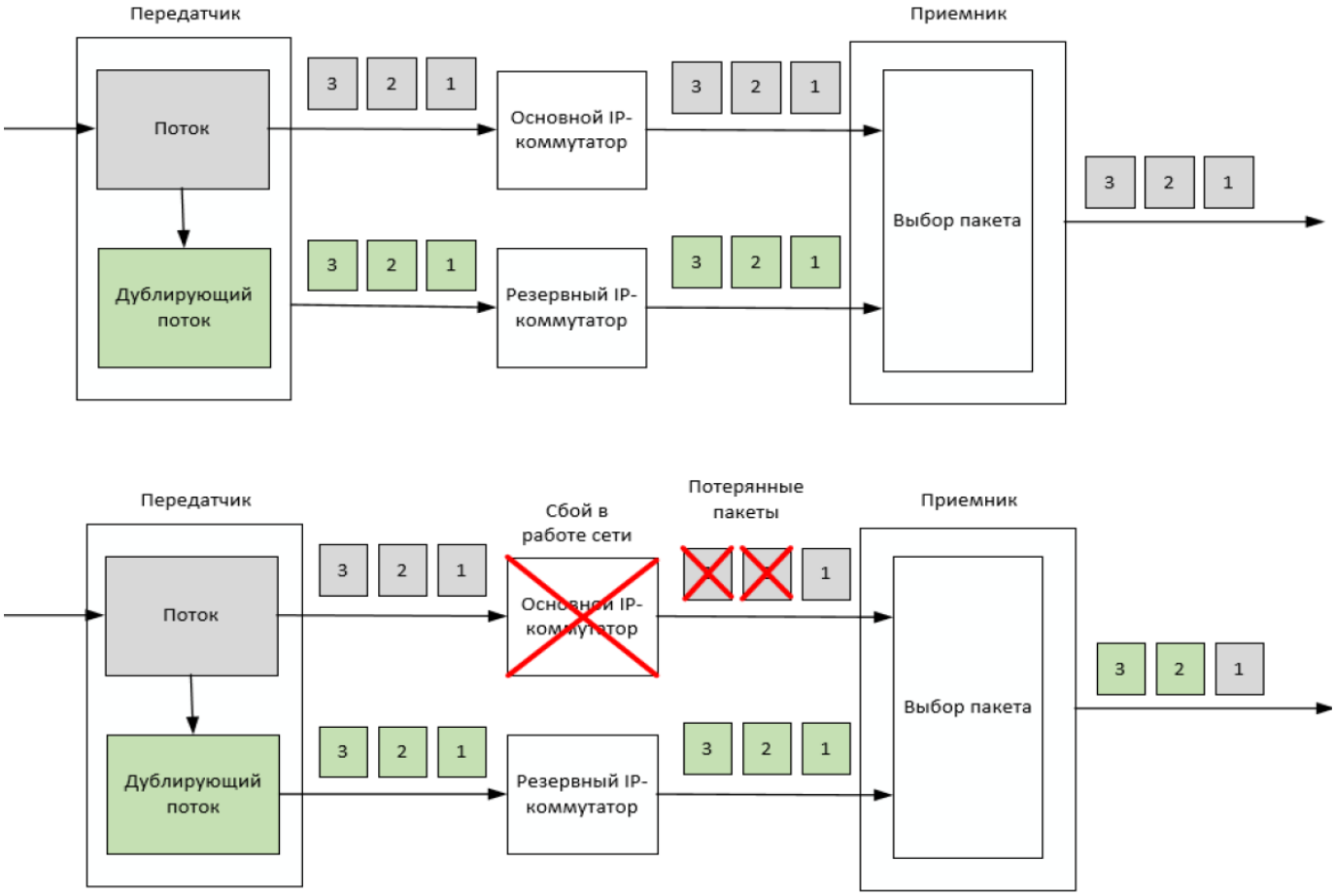


Рис. 3. Схема передачи данных по стандарту SMPTE ST 2022-7

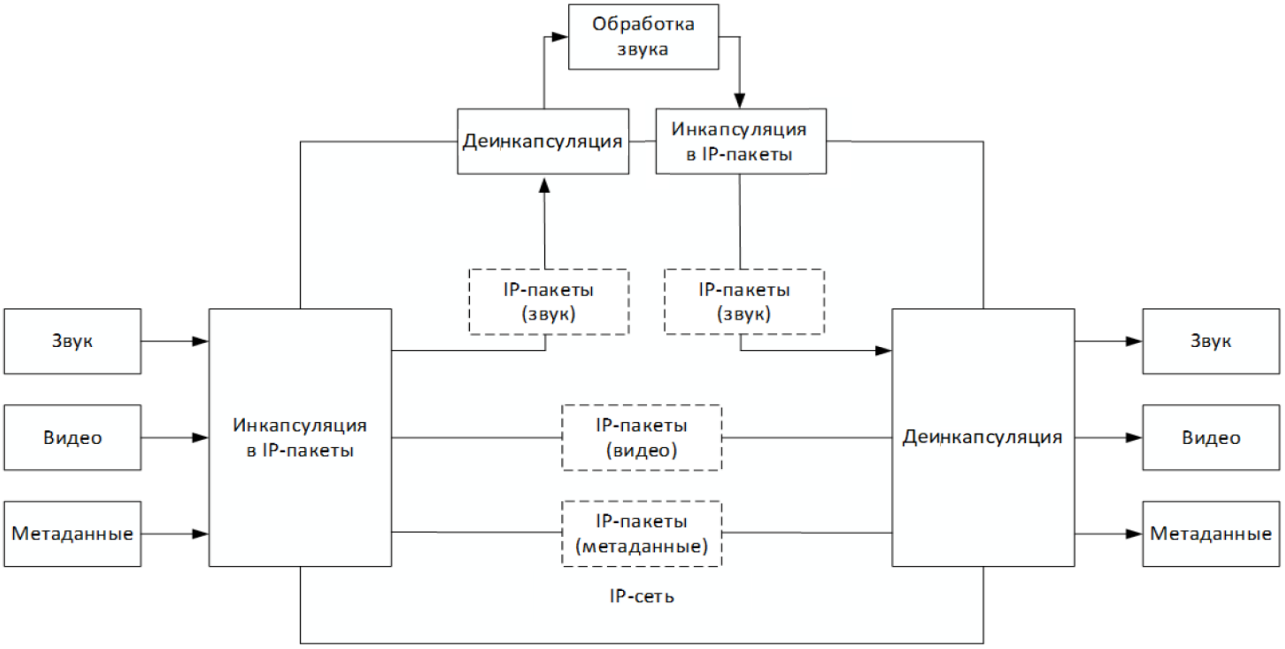


Рис. 4. Схема передачи данных по стандарту SMPTE ST 2110

Протокол ASPEN (Adaptive Sample Picture ENcapsulation), разработанный компанией Evertz, для передачи медиаконтента по IP-сетям, предполагает упаковку сигналов форматов SD/HD/3G/Ultra HD сначала в транспортные потоки MPEG, затем в RTP, UDP и IP-пакеты. Видео, звук и метаданные, как и в SMPTE ST 2110, доставляются тремя независимыми потоками. Стандарт SMPTE RDD-37 [10] описывает транспортировку видеоданных, SMPTE ST-302 [11] – звука, SMPTE ST-2038 [12] – дополнительных данных. Схема инкапсуляции медиаконтента по стандарту ASPEN приведена на рисунке 5. Поскольку максимальная длина IP-пакета при передаче по Ethernet равна 1500 байтов, а 20, 8 и 12 байт составляют заголовки IP, UDP и RTP пакетов соответственно, полезная нагрузка RTP-пакета представляет собой 7 TS пакетов по 188 байтов (4 байта – заголовок, 184 – полезная нагрузка).

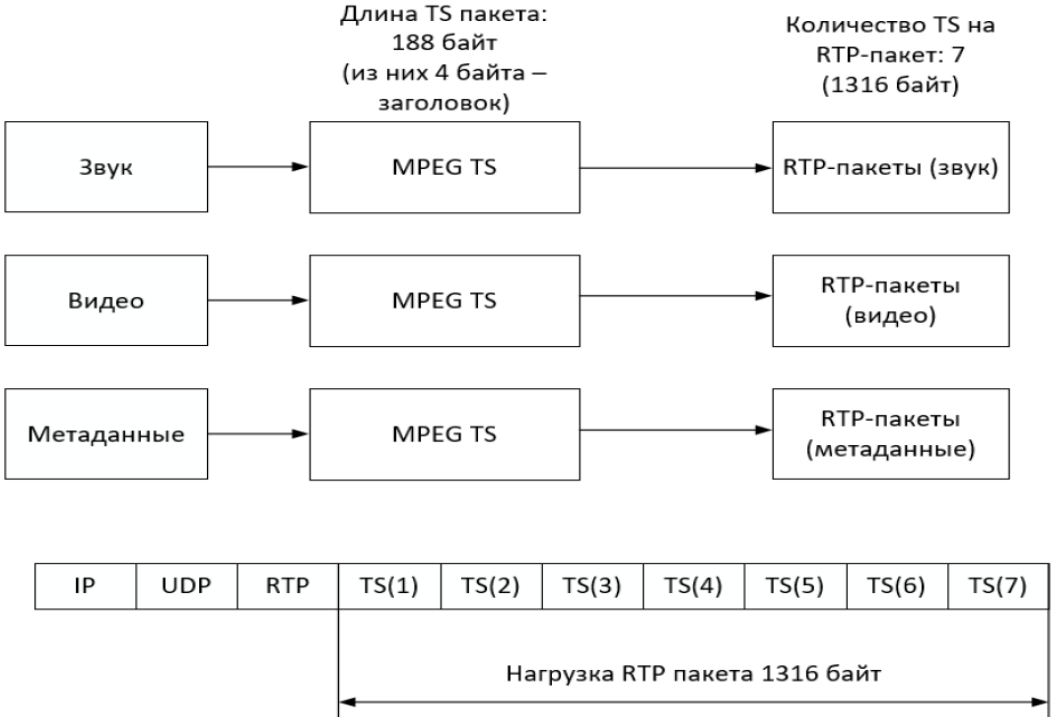


Рис. 5. Схема инкапсуляции данных по стандарту ASPEN

Стандарт NDI (Network Device Interface) разработан компанией NewTek. В отличие от стандартов SMPTE ST 2022, SMPTE ST 2110 и ASPEN, требующих 10-ти гигабитные сети, для передачи данных по стандарту NDI достаточно 1 Гбит. В данном стандарте используется сжатие SHQ 2/7, аналогичное внутрикадровому кодированию MPEG-2. Изначально NDI в качестве транспортного протокола использовал TCP, в более поздних версиях появились опции UDP unicast и multicast, в NDI 4 - «multi-TCP», позволяющий хостам подключаться к нескольким библиотекам в комплексе. Если не удается подключиться к одной, хост может по-прежнему взаимодействовать через другие библиотеки. Для передачи одного видео разрешением 1080i требуется полоса примерно в 100 Мбит. В более поздних стандартах NDI HX и NDI HX2 используется кодирование H.264, H.265, также требуется меньшая полоса пропускания для передачи. Модель NDI показана на рисунке 6.

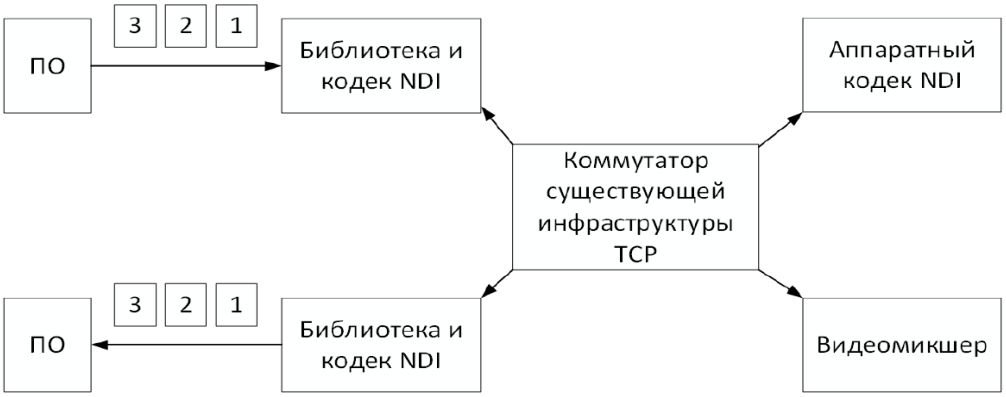


Рис. 6. Модель NDI

Корпорация Sony разработала свой сетевой медиаинтерфейс NMI (Sony Network Media Interface). Видео, звук и метаданные также передаются отдельными потоками. Как и в стандартах SMPTE 2022-5 и SMPTE 2022-7, NMI предполагает прямую коррекцию ошибок, но с учетом границ кадра, и резервирование, обеспечивающее автоматическое переключение между основным и резервным потоками.

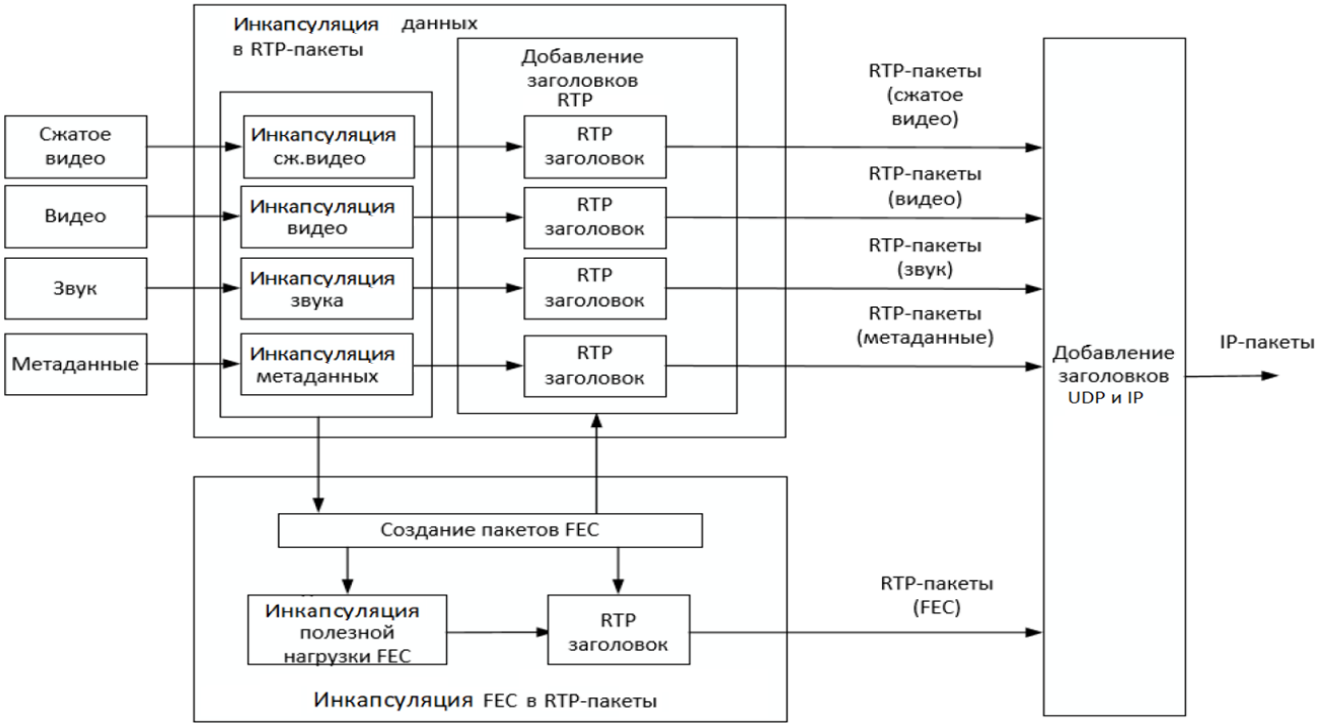


Рис. 7. Структура медиатранспорта NMI

Для видеокомпрессии используется LLVC (Low Latency Video Codec – видеокодек с низкой задержкой, основанный на вейвлет-преобразовании, принятом в JPEG2000), коэффициенты сжатия от 3:1 до 14:1 [13-14]. Структура медиатранспорта NMI показана на рисунке 7.

Сравнительная характеристика стандартов приведена в таблице 2.

Таблица 2

Сравнение стандартов передачи по IP

Параметр	**1) NDI; 2) NDI HX; 3) NDI HX2**	**SMPTE ST 2022-6**	**SMPTE ST 2110**	**ASPEN**	**NMI**
Особенности кодирования	Пакеты аудио, видео и метаданных	Пакеты битового потока SDI	Пакеты аудио, видео и метадан-ных	Несколько транспортных потоков MPEG	Пакеты аудио, видео и метаданных
Скорость передачи HD (1080i)	1) ~100 Мбит/с; 2) 8-20 Мбит/с; 3) ~1–50 Мбит/с	>1.5 Гбит/с	>1.1 Гбит/с	>1.5 Гбит/с	>1.5 Гбит/с до 14:1
Физический уровень	Гбит / беспроводной / 10 Гбит (NDI)	10 Гбит	10 Гбит	10 Гбит	10 Гбит/ Гбит
Протоколы обнаружения сервисов	1,3) Bonjour (mDNS), NDI Access (руководство), сервер (NDI4); 2) Автоматически через драйвер HX	NMOS (Networked Media Open Specifications)		JSON-RPC (JavaScript Object Notation Remote Procedure Call)	Plug & Play (NDCP- Networked Device Control Protocol)
Сжатие	1) SHQ 2/7; 2) H.264; 3) H.264 / H.265	Не заложено в стандарт			Нет / LLVC
Транспортный протокол	1,3)TCP/UDP/ Multi-TCP; 2) UDP (TCP)	UDP			
Тип соединения	1,3) Socket, Unicast / Multicast и FEC; 2) Unicast/Multicast	Multicast			

Заключение

Таким образом, можно утверждать, что метод TS/RTP/UDP/IP для передачи медиаконтента по IP-сетям предпочтительнее, чем RTP/UDP/IP. RTP позволяет восстановить порядок следования пакетов на большом интервале, при этом точность синхронизации недостаточно высокая. Использование транспортных потоков MPEG, конечно, увеличивает накладные расходы, но незначительно (на 2.3%), и, что более важно, улучшает точность синхронизации (джиттер составляет довольно малую величину: 37 нс). Такой способ передачи реализуется, например, в стандарте ASPEN.

Литература

1. *Хилл Б.* Полный справочник по Cisco/ Пер. с англ. Птицын К. М.; СПб.; К.: Издательство «Вильямс», 2004. 1088 с.

2. *Валицкая Н.С., Власюк И.В.* Методы синхронизации потоков в видеоинформационных системах // Телекоммуникации и информационные технологии, 2019. №2. С.51-57.

3. *MacAulay A., Felts B., Fisher Y.* IP Streaming of MPEG-4: Native RTP vs MPEG-2 Transport Stream [Электронный ресурс] // Envivio, Inc.(2005). URL: http://pdf.textfiles.com/manuals/STARINMANUALS/Envivio (дата обращения: 16.07.2020).

4. ST 2022-6:2012 - SMPTE Standard - Transport of High Bit Rate Media Signals over IP Networks (HBRMT)," in ST 2022-6:2012, vol., no., pp.1-16, 9 Oct. 2012, doi: 10.5594/SMPTE.ST2022-6.2012.

5. ST 2022-5:2013 - SMPTE Standard - Forward Error Correction for Transport of High Bit Rate Media Signals over IP Networks (HBRMT)," in ST 2022-5:2013, vol., no., pp.1-22, 27 Feb. 2013, doi: 10.5594/SMPTE.ST2022-5.2013.

6. ST 2022-7:2013 - SMPTE Standard - Seamless Protection Switching of SMPTE ST 2022 IP Datagrams," in ST 2022-7:2013, vol., no., pp.1-13, 30 Dec. 2013, doi: 10.5594/SMPTE.ST2022-7.2013.

7. ST 2110-20:2017 - SMPTE Standard - Professional Media Over Managed IP Networks: Uncompressed Active Video," in ST 2110-20:2017, vol., no., pp.1-22, 27 Nov. 2017, doi: 10.5594/SMPTE.ST2110-20.2017.

8. ST 2110-30:2017 - SMPTE Standard - Professional Media Over Managed IP Networks: PCM Digital Audio," in ST 2110-30:2017, vol., no., pp.1-9, 27 Nov. 2017, doi: 10.5594/SMPTE.ST2110-30.2017.

9. ST 2110-40:2018 - SMPTE Standard - Professional Media Over Managed IP Networks: SMPTE ST 291-1 Ancillary Data," in ST 2110-40:2018, vol., no., pp.1-8, 25 April 2018, doi: 10.5594/SMPTE.ST2110-40.2018.

10. RDD37:2016 - SMPTE Registered Disclosure Doc - Uncompressed Video Transport Over MPEG-2 Transport Stream," in RDD37:2016, vol., no., pp.1-18, 3 March 2016, doi: 10.5594/SMPTE.RDD37.2016.

11. ST 302:2007 - SMPTE Standard - For Television — Mapping of AES3 Data into an MPEG-2 Transport Stream," in ST 302:2007, vol., no., pp.1-9, 25 Oct. 2007, doi: 10.5594/SMPTE.ST302.2007.

12. ST 2038:2008 - SMPTE Standard - Carriage of Ancillary Data Packets in an MPEG-2 Transport Stream," in ST 2038:2008, vol., no., pp.1-7, 18 Sept. 2008, doi: 10.5594/SMPTE.ST2038.2008.

13. RDD 34:2015 - SMPTE Registered Disclosure Doc - LLVC — Low Latency Video Codec for Network Transfer," in RDD 34:2015, vol., no., pp.1-32, 8 Oct. 2015, doi: 10.5594/SMPTE.RDD34.2015.

14. *Власюк И.В., Любецкая В.Ю.* Анализ методов подавления артефактов звона, возникающих на изображениях в процессе кодирования с wavelet-преобразованием // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 53-58.

PROTOCOLS AND STANDARDS FOR THE TRANSMISSION OF MEDIA CONTENT OVER IP NETWORKS

Natalya S. Valitskaya,
Graduate MTUCI, Moscow, Russia
nvalitskaya@mail.ru
Igor V. Vlasyuk,
Associate professor of the TaAB Department MTUCI, PhD., Moscow, Russia
ru3dlp@yandex.ru

Keywords: *transmission of media content, IP, UDP, RTP, MPEG TS, SMPTE ST 2022, SMPTE ST 2110, ASPEN, NDI, Sony NMI.*

There is a trend of migration from SDI to IP now in TV broadcasting. This work is devoted to the analysis of methods for delivering media content over IP networks. The overhead costs due to packet transmission of media content have been calculated. The advantages and disadvantages of transport methods are analyzed. The schemes for the transmission of media content in accordance with the standards SMPTE ST 2022, SMPTE ST 2110, ASPEN, NDI, Sony NMI and the comparative characteristics of the standards are presented.

ИМИТАЦИОННАЯ МОДЕЛЬ ПРОЦЕССА ФОРМИРОВАНИЯ ИЗОБРАЖЕНИЯ В ГОЛОГРАФИЧЕСКОЙ РЛС

Зайцева Елена Владимировна,
Специалист Отдела ПК МТУСИ, Москва, Россия
e.v.zaitseva@mtuci.ru
Никоненко Алексей Владимирович,
м.н.с. НИО-48 МТУСИ, Москва, Россия
nikon74@mail.ru
Чиров Денис Сергеевич,
заведующий кафедрой РТС МТУСИ, д.т.н., профессор, Москва, Россия
chirov@srd.mtuci.ru

Ключевые слова: бортовая голографическая РЛС, модель ГРЛС, формирование изображения РЛС, обнаружение, радиолокационное наблюдение.

Обнаружение аномалий на морской поверхности является актуальной задачей двойного назначения. Активное развитие беспилотной авиации позволяет использовать для данных целей беспилотные летательные аппараты с бортовой голографической РЛС планового обзора с длинной вдолькрыльевой антенной. Преимуществом применения ГРЛС заключается в том, что она выполняет обзор пространства в зоне непосредственно под летательным аппаратом, что обеспечивает минимально возможные дальности до разведываемых объектов и позволяет получить высокую разрешающую способность, до долей метра. Работа с малыми излучаемыми мощностями определяет возможность создания малогабаритной и относительно дешевой аппаратуры. Вопросы использования БЛА с ГРЛС для детальной разведки частично освещены в литературе, однако ее применение на море до настоящего времени не было проработано теоретически и не имело технических решений. Открытым остается один из важных вопросов – оценка влияния движения морской поверхности на свойства создаваемого ГРЛС изображения. Для решения данной проблемы необходима разработка модели процесса формирования изображения движущейся поверхности в голографической РЛС, результатом разработки которой и посвящена данная статья. Рассмотрена структура модели и ее основных блоков.

Антропогенное давление на окружающую среду в последние два столетия резко возросло. Данное обстоятельство привело к необходимости контроля над средой обитания (биосферой). Экологический мониторинг достаточно широкое понятие и одной из его задач является наблюдение за происходящими в окружающей природной среде физическими, химическими и биологическими процессами. Одним из важных объектов экологического мониторинга являются моря и океаны. Наблюдение за аномалиями на морской поверхности позволяет осуществлять: контроль гидрологических процессов на морской поверхности, обнаружении движущихся подводных и надводных объектов, течений, экологического загрязнения шельфовых зон и т.д. В настоящее время все шире для решения различных задач экологического мониторинга применяются различные технические средства автоматизации, в том числе беспилотные летательные аппараты [1, 2]. Активное развитие беспилотной авиации позволяет использовать для данных целей беспилотные летательные аппараты (БЛА) с бортовой голографической РЛС (ГРЛС) планового обзора с длинной вдолькрыльевой антенной. Применение БЛА с ГРЛС для дистанционного зондирования Земли частично освещены в ряде источников [3, 4], однако применение ГРЛС на море до настоящего времени не было проработано теоретически и не имело технических решений. Основным проблемным вопросом является исследование оценки влияния движения морской поверхности на свойства

создаваемого ГРЛС изображения. Для решения данной проблемы необходима разработка модели процесса формирования изображения движущейся поверхности в голографической РЛС.

Рассматриваемая ниже имитационная модель предназначена для исследования потенциальных характеристик ГРЛС и для отработки ее алгоритмов функционирования [5]. Модель имеет блочную структуру, представленную на рисунке 1.

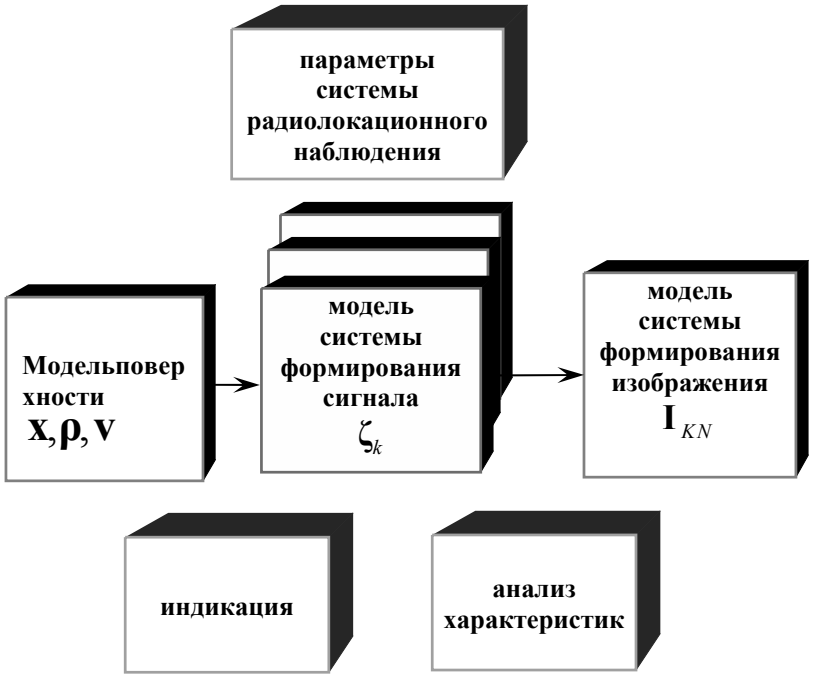


Рис. 1. Схема имитационной модели ГРЛС

При исследовании потенциальных характеристик системы радиолокационного наблюдения почти вся она, вплоть до выходных сигналов фильтровой системы, представляется как линейная. На схеме линейная часть системы соответствует блоку «модель системы формирования сигнала». Такие факторы, как влияние нелинейности и нестабильности узлов приемо-передающего тракта и влияние мультипликативных шумов, например образованных нелинейностью траектории полета ЛА и высокочастотными колебаниями ЛА на траектории (траекторными нестабильностями), не моделируются в прямом виде, а учитываются «в среднем» – путем изменения передаточной характеристики линейной системы.

Входной сигнал линейной системы генерирует «модель поверхности», которая представляется набором точечных отражателей, характеризуемых положением на плоской поверхности $\mathbf{x}$, величиной ЭПО $\boldsymbol{\rho}$ и скоростью собственного движения отражателей $\mathbf{v}$. Для каждого k – го азимутального канала формируется свой входной сигнал в виде параметров точечных отражателей $\mathbf{x}_k, \boldsymbol{\rho}_k, \mathbf{v}_k$. Их прохождение через модель ГРЛС рассматривается независимо друг от друга и каналы обработки считаются идентичными.

Все процессы распространения ЭМВ от поверхности до антенны, преобразования поля в электрический сигнал и его усиления, фильтрации системой доплеровских фильтров представляются единой линейной системой с передаточной характеристикой $\Phi_{\Phi}(x)$, которая по определению является реакцией системы на точечный отражатель и задается как характеристика ГРЛС. Так как система линейна, выходной сигнал ζ_k, образованный отражениями от поверхности в каждом из азимутальных каналов, формируется как сумма сигналов, образованных точечными отражателями.

Такой подход исключает из процесса моделирования операции расчета траекторного сигнала и расчета операции фильтрации, выполняемые прямым и обратным преобразованием Фурье.

Блок «параметры системы радиолокационного наблюдения»

Блок «параметры системы радиолокационного наблюдения» служит для задания исходных параметров, которые включают в свой состав:

1. Параметры системы моделирования, в том числе количество точек моделирования на поверхности $J \times K$ и расстояние между отражающими точками Δ_x, Δ_y.

2. Геометрические параметры системы радиолокационного наблюдения.

3. Параметры РЛС, в том числе вид и параметры передаточной функции $\Phi_\Phi(x)$ и количество элементов фильтровой системы N.

Блок «модель поверхности»

Блок «модель поверхности» представлен на рисунке 2. Индексы, написанные строчными буквами, определяют размерность вектора (матрицы).

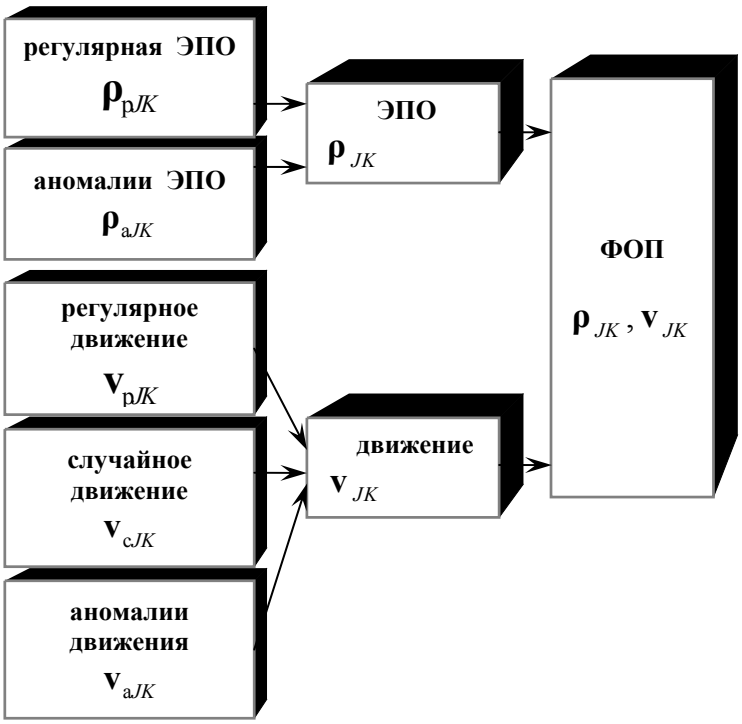


Рис. 2. Блок модель поверхности

В зоне обзора на моделируемой поверхности задается K азимутальных каналов, следующих с интервалом Δ_y. Этот интервал обычно выбирается равным разрешающей способности РЛС по азимуту δ_y.

В каждом азимутальном канале задается J эквидистантно расположенных отражающих точек, следующих с интервалом Δ_x. Величина этого интервала выбирается так, чтобы на элемент разрешения на неподвижной поверхности δ_x приходилось 5…10 точечных отражателей. Каждому точечному отражателю присваивается значение его ЭПО ρ_{jk} и радиальной составляющей скорости собственного движения v_{jk}, которые впоследствии формируют отражающую поверхность (ФОП).

ЭПО отражателей задается в виде некоррелированных в пространстве, независимых от точки к точке, комплексных случайных величин, определяющих комплексный коэффициент отражения точек. Закон распределения плотности вероятности этих величин может быть различный в зависимости от свойств моделируемой поверхности. Их фаза всегда распределена по равномерному закону в

интервале $\{-\pi,\pi\}$. Амплитуда может иметь различную дисперсию в пределах зоны обзора или иметь «подставку» в виде постоянной составляющей.

Радиальная составляющая скорости собственного движения отражателей включает две компоненты:

$\mathbf{v}_{\text{р}}$ – регулярную составляющую скорости, медленно изменяющуюся в пространстве по сравнению с размером элемента разрешения РЛС;

$\mathbf{v}_{\text{с}}$ – случайную составляющую скорости, некоррелированную в пространстве.

Случайная составляющая скорости является действительной случайной величиной, закон распределения плотности вероятности которой, зависит от свойств движущейся поверхности. Полная скорость движения поверхности является суммой регулярной и случайной составляющих:

$$\mathbf{v} = \mathbf{v}_{\text{р}} + \mathbf{v}_{\text{с}}. \qquad (1)$$

Блок «модель системы формирования сигнала»

Блок «модель системы формирования сигнала» представлен на рисунке 3 для одного из идентичных k – го азимутального канала.

Входным сигналом для блока являются J – размерные векторы параметров модели поверхности $\mathbf{x}_{kJ}\boldsymbol{\rho}_{kJ},\mathbf{v}_{kJ}$. Этот блок формирует комплексный выходной сигнал системы фильтрации в виде N – размерных векторов $\boldsymbol{\zeta}_{kN}$. Элементы этого вектора являются суммой выходного сигнала, отраженного от поверхности $\mathbf{Z}_{kN}$ и внутреннего шума приемника:

$$\boldsymbol{\zeta}_{kN} = \mathbf{Z}_{kN} + \boldsymbol{\xi}_{kN}, \qquad (2)$$

где $\boldsymbol{\xi}_{kN}$ – комплексный белый гауссовский случайный процесс.

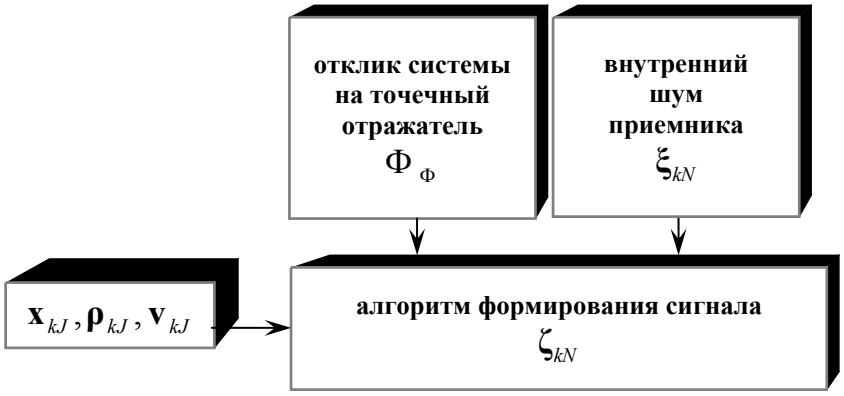


Рис. 3. Блок системы формирования сигнала в k – м азимутальном канале

Сигнал в одном азимутальном канале образуется как сумма сигналов, созданных точечными отражателями. Если неподвижный отражатель находится в центре зоны обзора и частота отраженного от него сигнала совпадает с центральной частотой настройки фильтра, отклик на него совпадает с передаточной характеристикой системы Φ_{Φ}. В фильтре, настроенном на частоту отражателя, возникает максимальный сигнал. В остальных фильтрах точечный отражатель образует сигналы, величина которых определяется уровнем боковых лепестков фильтра. Если частота сигнала не совпадает с частотой настройки фильтра, но находится в пределах главного лепестка его частотной характеристики, амплитуда сигнала отражателя падает.Для движущегося отражателя отметка сигнала возникает в фильтре, соответствующем сдвигу его изображения на величину

$$x_{\text{d}j} = R_k v_j / V_{\text{c}k}, \qquad (3)$$

где $V_{ck} = V_c \cos\alpha \cos\theta_k$. (4)

Сигнал от участка поверхности в одном азимутальном канале $\mathbf{Z}_{kN}$ образуется как сумма сигналов от всех J отражателей в канале (рисунок 4).При изображении неподвижной поверхности в каждом $n-$м фильтре присутствуют составляющие сигнала, образованные отражателями, частота которых попадает в его полосу пропускания, т.е. в элемент разрешения на поверхности. Они образуют суммарный полезный сигнал фильтра z_{cn}. Кроме того, в фильтре присутствуют сигналы от отражателей, принимаемые по боковым лепесткам, образующие суммарный помеховый сигнал $z_{\text{п}n}$.

Суммарный сигнал на выходе $k-$й фильтровой системы, образованный отражениями от поверхности, формируется как

$$\mathbf{Z}_{kN} = \mathbf{z}_{kcN} + \mathbf{z}_{k\text{п}N}. \quad (5)$$

При изображении движущейся поверхности сигналы отражателей смещаются по фильтрам, создавая распределение амплитуд на выходе фильтровой системы, отличающееся от картины для неподвижной поверхности. Изображение для движущейся поверхности на рисунке 4 построено для того же распределения величины коэффициента отражения, что для неподвижной поверхности. Однако заданное скоростное распределение сместило изображение вправо.

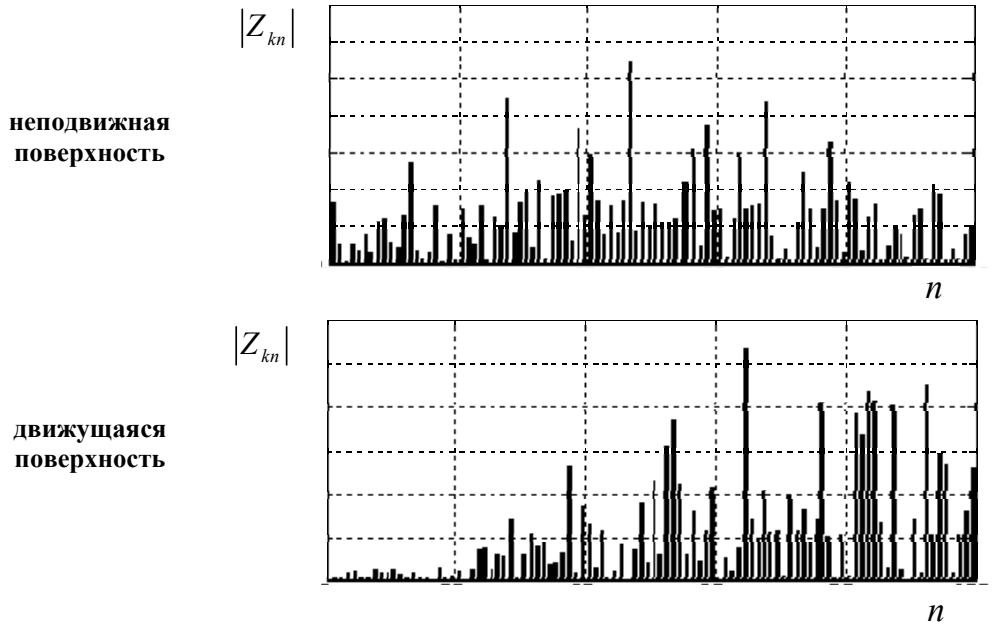


Рис. 4. Модель сигнала отраженного от поверхности на выходе системы фильтрации

Выход системы формирования сигнала в $k-$м азимутальном канале образован суммой отраженного от поверхности сигнала, помехи и внутреннего шума приемника:

$$\zeta_{kN} = \mathbf{z}_{kcN} + \mathbf{z}_{k\text{п}N} + \xi_{kN}. \quad (6)$$

Блок «модель системы формирования изображения»

В режиме обзора морской поверхности блок «модель системы формирования изображения» рассчитывает амплитуду выходного сигнала $I_{kn} = |\zeta_{kn}|$ или его интенсивность $I_{kn}^2 = |\zeta_{kn}|^2$, образуя матрицы изображений $\mathbf{I}_{KN}$ или $\mathbf{I}_{KN}^2$.

Блоки «анализ характеристик» и «индикация» используются на всех этапах моделирования.

Имитационная модель ГРЛС предназначена для исследования ее потенциальных характеристик при формировании изображения движущейся поверхности.

Заключение

Представленная в статье имитационная модель голографической РЛС имеет ряд преимуществ над другими известными способами экологического мониторинга, так как позволяет использовать меньшие дальности до разведываемых объектов. Но, пожалуй, основным её преимуществом является более высокая разрешающая способность, позволяющая более корректно исследовать морскую поверхность.

Литература

1. *Осанов В.А., Щурихин А.А., Кондратьев С.М., Михаленко Ю.А., Коняева О.С.* Разработка автоматизированной системы мониторинга атмосферного воздуха с использованием беспилотного летательного аппарата // T-Comm: Телекоммуникации и транспорт. 2019. Том 13. №5. С. 28-34.
2. *Чиров Д.С., Новак К.В.* Перспективные направления развития робототехнических комплексов специального назначения // Вопросы безопасности. 2018. № 2. С. 50-59.
3. *Кондратенков Г.С., Потехин В.А., Реутов А.А., Феоктистов Ю.А.* Радиолокационные станции обзора земли; Под ред. Кондратенкова Г. С. М.: Радио и связь, 1983. 272 с.
4. *Кондратенков Г.С., Запорожец Г.В., Никоненко. А.В.* Технический облик голографической РЛС малоразмерного беспилотного летательного аппарата при решении навигационных задач // Информационно-измерительные и управляющие системы. 2018. Т.16. №10. С. 25-29.
5. *Никоненко. А. В.* Алгоритмы моделирования процесса формирования изображения морской поверхности в голографической РЛС // Электромагнитные волны и электронные системы. 2015. №1. том 20. С. 11-15.

SIMULATION MODEL OF THE IMAGE FORMATION PROCESS IN A HOLOGRAPHIC RADAR

Elena V. Zaytseva,
Specialist of the Department AO MTUCI, Moscow, Russia
e.v.zaitseva@mtuci.ru
Denis S. Chirov,
Header of RTC Department MTUCI, Doctor of Technical Sciences, Professor, Moscow, Russia
chirov@srd.mtuci.ru
Alexey V. Nikonenko,
Junior researcher NIO-48 MTUCI, Moscow, Russia
nikon74@mail.ru

Keywords: *onboard holographic radar, GRL model, radar imaging, detection, radar surveillance.*

Detection of anomalies on the sea surface is an urgent dual-purpose task. The active development of unmanned aviation makes it possible to use unmanned aerial vehicles for these purposes with an airborne holographic radar of a planned view with a long along-wing antenna. The advantage of using the radar is that it performs a survey of the space in the area directly under the aircraft, which provides the minimum possible range to reconnaissance objects and allows you to obtain high resolution, up to fractions of a meter. Working with low radiated powers determines the possibility of creating small-sized and relatively cheap equipment. The issues of using a UAV with a radar for detailed reconnaissance are partially covered in the literature, but its use at sea has not yet been theoretically worked out and did not have technical solutions. One of the important questions remains open - the assessment of the influence of the sea surface movement on the properties of the image created by the radar. To solve this problem, it is necessary to develop a model of the process of forming an image of a moving surface in a holographic radar, the development of which is the result of this report. The report considers the structure of the model and its main blocks. The results of modeling and assessment of the adequacy of the developed model are presented.

СТАНДАРТЫ БЕСПРОВОДНОЙ СВЯЗИ ДЛЯ СИСТЕМЫ УМНЫЙ ДОМ

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

Ключевые слова: умный дом, smart city, Bluetooth, BLE, Wi-Fi, Z-Wave, ZigBee.

Рассмотрено функциональное назначение структурных элементов системы домашней автоматизации – умный дом. На основе анализа характеристик технологий беспроводной связи приведены критерии выбора наиболее перспективных базовых радиотехнологий для использования в проектных решениях домашней автоматизации. Приведены сравнительные характеристики технологий беспроводного управления системами домашней автоматизации и наиболее эффективные по технико-экономическим показателям стандарты и радиотехнологии, ориентированные на использование в системах умный дом

Умный дом – это гибкая система домашних автоматизированных устройств, обеспечивающая выполнение определенных действий по решению задач комфортного и безопастного пользования человеком домашней средой, Рис.1.

К числу основных задач, решаемых системой домашней автоматизации относятся: управление климатическими устройствами в доме (вентиляция и очистка воздуха, подержание комфортной температуры и влажности, регулировка мощности отопительных батарей); автоматическое управление освещённостью в помещениях; обеспечение безопасности проживания в доме (видеонаблюдение, дистанционно управляемые электронные замки, домофоны, контроль доступа и видеозапись, сигнализация и вызов группы реагирования и т.д.): контроль и автоматическое уведомление о возгорании, аварийных ситуациях в системах отопления, освещения и водоснабжения дома, и др. [1,9-20].

Рис. 1. Функциональны элементы системы домашней автоматизации

Структурно умный дом (smart house) включает три основных типа устройств, обеспечивающих автоматизацию экосистемы домашней среды человека (Рис.2) . Основная задача системы умный дом – на первых этапах внедрения частичная, а в перспективе, полная организация

комфортного и безопасного проживания людей на основе автоматизации управления инженерными и сервисными системами жилого помещения, [2].

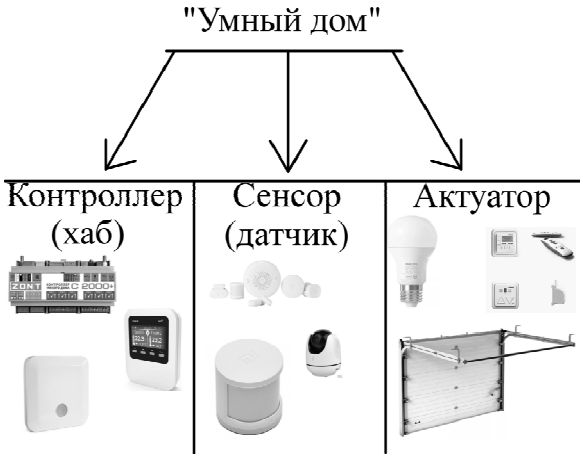


Рис. 2. Типы устройств используемых в системе умный дом

Контроллер (хаб) – главное управляющее устройство. Объединяет все элементы системы в единую структуру и обеспечивает её связь с внешней средой. Через контроллер поступают команды от пользователя в систему. Контроллер может не иметь панель интерфейса. Её может заменить телефон или планшет, используемые для передачи сигналов на контроллер, который транслирует их другим элементам системы.

Сенсоры (датчики) – устройства, обеспечивающие сбор информацию о параметрах и условиях функционирования подсистем жизнеобеспечения в помещениях дома.

Актуаторы (исполнители) – исполнительные устройства, которые осуществляют выполнение команд, сформированных программой или пользователем. Данный тип устройств является самым многочисленным. К ним, например, относятся умные (автоматические) выключатели и розетки, умные (автоматические) клапаны для труб тепло и водоснабжения, устройства климатического регулирования, автоматические двери, открывающиеся открываются от кнопки или датчика движения и т.д.

Для передачи и обмена данными между всеми типами этих устройств необходимо использовать беспроводную связь. Существует обширный перечень технологий, которые могут быть использованы для организации беспроводной связи между отдельными типами устройств умного дома. В качестве критериев выбора стандарта беспроводной технологии для системы умный дом следует использовать следующие показатели и характеристики:

- энергопотребление устройств;
- дальность действия:
- цифровая безопасность трафика;
- отказоустойчивость сети;
- простота подключения устройств и возможность масштабирования сети;
- отказоустойчивость и взаимная совместимость устройств.

Следует отметить, что процесс коммутации между отдельными устройствами умного дома для каждого стандарта определяется реализуемыми в нём уровнями семиуровневой эталонной модели OSI, [8]. При этом в некоторых стандартах не определены отдельные уровни модели OSI, что не обеспечивает функционал взаимодействия между устройствами, а также безопасность и стабильность обмена данными в сети. В частности, если не определён верхний уровень модели OSI, устройства, использующие одинаковый протокол не смогут взаимодействовать друг с другом.

Bluetooth (BLE)

Технология Bluetooth (IEEE 802.15.1) является основной технологией подключения периферийных устройств (беспроводные клавиатуры и мыши, гарнитуры, принтеры и т.д.) и обмена

данными в персональных вычислительных сетях. Практическое использование Bluetooth в сфере Интернета вещей стало возможным с выпуском в 2010 году версии Bluetooth Core 4.0, которая включает версию с низким энергопотреблением Bluetooth Low Energy (BLE), ориентированную на устройства с низким энергопотреблением [3].

Отличие BLE от широко известного классического Bluetooth заключается в том, что используемые устройства с автономным питанием от батареек соединяются только при необходимости отправки или получения в активном режиме небольших пакетов данных в течение короткого времени. Помимо низкого энергопотребления, BLE отличается значительной скоростью передачи данных – до 1 Мбит/с, а в для новой пятой версии (Bluetooth Smart) это значение увеличено до 2 Мбит/с, что значительно уменьшает вероятность возникновения коллизий, характерных для сверх загруженного диапазоне частот 2,4 ГГц. Так как большую часть времени устройства с BLE поддерживаются в спящем режиме и активируются только на короткое время для быстрого выполнения своей задачи, работа датчиков и переключателей без замены используемых малогабаритных батареек-таблеток длится более года. Важнейшим преимуществом технологии Bluetooth является её поддержка практически всеми моделями смартфонов, планшетов и ноутбуков. Bluetooth обеспечивает прямую связь между гаджетом и устройством. При использовании специального приложения гаджет становится «удаленным дисплеем» для интеллектуальной домашней сети умных устройств, добавление которых с учётом топологии Bluetooth («звезда») в систему умный дом предельно упрощается [4].

Bluetooth включает все уровни основной модели OSI и орган, контролирующий его разработку и лицензирование (SIG – Bluetooth Special Interest Group), имеет полномочия непосредственно и самостоятельно вносить любые изменения в стандарт.

Существенным недостатком радиотехнологии Bluetooth является использование полосы частот 2,4 ГГц, для которой затухание сигнала значительно выше, чем на частотах менее 1 ГГц, что ограничивает реальный радиус действия технологии Bluetooth Low Energy до 10 метров в помещении при наличии стен и других препятствий. Помимо этого диапазон 2,4 ГГц повсеместно используется бытовыми и промышленными устройствами, создающими постоянные помехи. Этот фактор, несмотря на использование в Bluetooth в ходе передачи данных динамического доступа к 40 каналам для выбора наименее зашумлённых, является существенным минусом при выборе оптимальной радиотехнологии для системы умный дом (рис. 3).

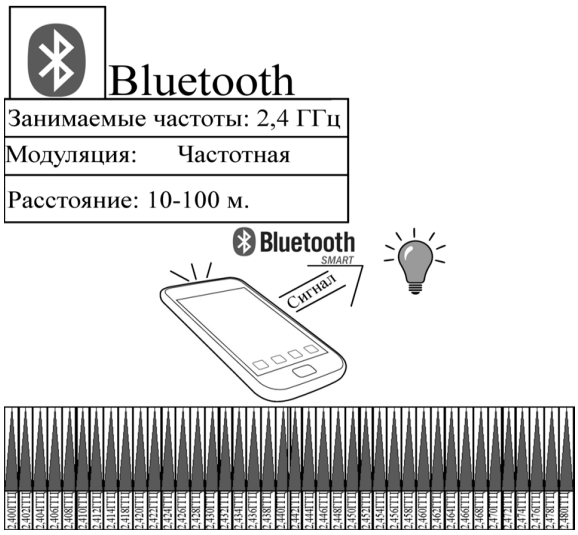


Рис. 3. Система Bluetooth smart (BLE)

Также важно то, что Bluetooth Smart был первоначально разработан для поддержания относительно простых сетей с топологией “звезда”, которая в отличие от ячеистой структуры сети мало походит для реализации управляемой датчиками гибкой и надежной среды домашней

автоматизации. С учётом этого Bluetooth Low Energy не имеет перспектив использования в ближайшие годы для массовой реализации проектных решений в области домашней автоматизации и тем более в офисных или в промышленных объектах.

Wi-Fi

Технология беспроводной связи Wi-Fi на первый взгляд является самой привлекательной для применения в домашней автоматизации и объединения в сеть различных IoT-устройств. Она базируется на семействе стандартов беспроводных сетей IEEE 802.11x (рис. 4), повсеместно применяемых в смартфонах, планшетах и ноутбуках, что очень важно для обеспечения использования управляющих приложений в системе умный дом и в сети с IoT-устройствами. При этом подключённый ПК или смартфон с выделенными правами администратора может выполнять функции панели управления всей системой «умный дом», [3].

Технология Wi-Fi обеспечивает скоростной обмен большими объёмами данных на расстояниях достаточных для покрытия домовой сетью. При увеличении площади можно увеличить число точек доступа или использовать ретрансляторы сигнала. Применение сети Wi-Fi с топологией «звезда» позволяет добавлять и удалять конечные устройства из сети, не оказывая влияния на её целостность и обмен данными.

Главное ограничение использования беспроводной сети Wi-Fi в системе умный дом связано с присущим ей значительным энергопотреблением из-за высокой пропускной способности, которая очевидно является избыточной для передачи простых управляющих команд типовым исполнительными устройствам системы. Автономные беспроводные сенсоры и исполнительные

устройства на основе Wi-Fi с питанием от батарей или аккумуляторов не смогут обеспечить приемлемой продолжительности функционирования в системе умный дом. Топология Wi-Fi-сети «звезда» также является серьёзным ограничением для систем домашней автоматизации, так как создаёт единую точку отказа - центральный маршрутизатор, сбой или выход из строя, которого нарушает взаимодействие отдельных узлов и приводит к отказу в работе всей системы. Ещё одним недостатком является относительно высокая стоимость Wi-Fi радиомодулей для домашней автоматизации. Помимо этого в стандарте Wi-Fi отсутствует прикладной уровень модели OSI , что не гарантирует штатного взаимодействия устройств разных производителей.

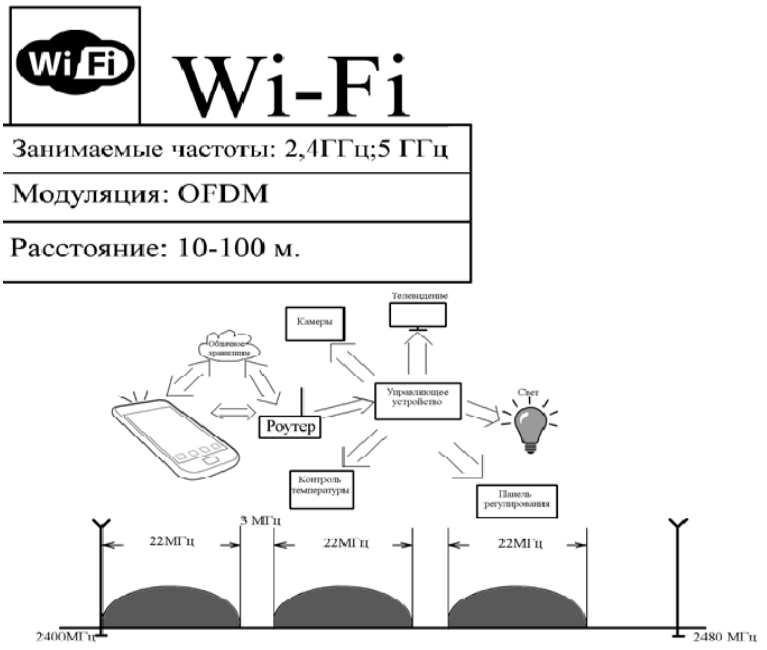


Рис. 4. Основные параметры системы умный дом с технологией Wi-Fi

В целом Wi-Fi не нашёл широко распространения в качестве базовой технологии при реализации проектных решений умного дома, за исключением условий, когда требуется надёжное соединение с облаком и не планируется использование новых умных устройств других стандартов.

Z-Wave

Являясь протоколом беспроводной связи с ультранизким энергопотреблением, стандарт Z-Wave был специально разработан для предоставления обычным пользователям возможности управления широким спектром датчиков и исполнительных устройств для умного дома.

В отличие от Wi-Fi и Bluetooth в протоколе Z-Wave используется ячеистая топология сети (mesh-сеть), что позволяет её узлам выполнять функции ретрансляторов и перенаправлять сообщения до требуемого адресата даже в случае, когда узлы находятся вне зоны прямой видимости. При выходе из строя любого узла сети сообщения автоматически будут передаваться через ретранслирующие узлы, что расширяет зону действия сети и повышает её надёжность. Оптимальный и альтернативные доступные маршруты, по которым может осуществляться передача сообщения между двумя устройствами через промежуточные узлы, определены заранее.

В логической сети Z-Wave может поддерживаться работа до 232 узлов, а при необходимости увеличения количества подключаемых устройств имеется возможность объединения нескольких сетей и функционирование без взаимных помех. При этом отдельные сети могут связываться друг с другом с помощью узловых устройств, выполняющих роль сетевых мостов.

Организация и построение сети Z-Wave начинается с основного контроллера, который обеспечивает добавление новых и удаление ненужных устройств, производит составление карт маршрутизации сообщений в соответствие с топологией сети, контролирует выполнение протоколов автоматизации и других процедур, обеспечивающих контроль функционирования и безопасность сети, (рис. 5). В сети также могут использоваться вторичные контроллеры, получающие от основного контроллера информацию о топологии сети. Новые устройства Z-Wave могут добавляться в сеть во время их инсталляции с помощью QR или пин-кодов. Протокол Z-Wave ориентирован на обмен короткими командами между устройствами, что минимально загружает радиоканал и минимизирует вероятность потери данных.

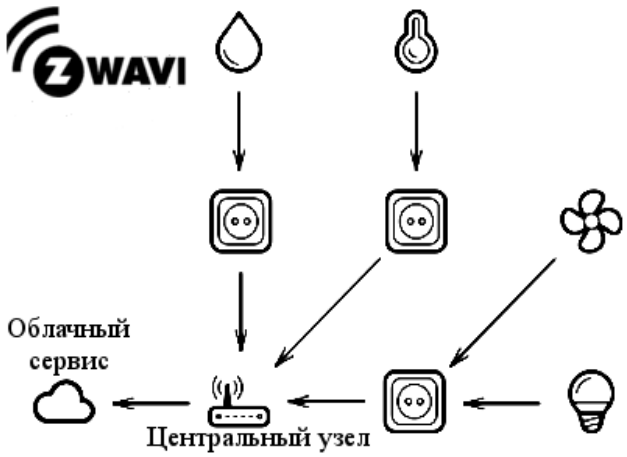


Рис. 5. Организация системы умный дом на основе Z-Wave

Z-Wave охватывает все уровни сетевой модели OSI от физического до прикладного, что гарантирует высокий уровень совместимости оборудования разных поставщиков. Помимо этого Z-Wave работает в нелицензируемой части диапазона 800-900 МГц, для которого стены и перекрытия не являются препятствием, а уровень помех от других устройств малого радиуса действия работающих в этом диапазоне крайне незначителен.

Важнейшим преимуществом технологии Z-Wave является высокий уровень безопасности обмена данными между устройствами за счёт использования стандартов шифрования и аутентификации аналогичной применяемым в системе онлайн-банкинга.

В целом по совокупности технико-экономических характеристик устройства с данной технологией являются наиболее эффективными среди устройств, используемых для домашней автоматизации. Определённый недостатком Z-Wave связан с несовместимостью произведённых в разных странах устройств из-за использования в них различных диапазонов частот, отличающихся от принятых в России.

ZigBee

Стандарт ZigBee также как и Z-Wave использует mesh-сети (рис. 6) и ориентирован на удаленный мониторинг и управление системой умный дом. Стандарт характеризуется низкими скоростями обмена данных и малым энергопотреблением. ZigBee в отличие от Z-Wave построен поверх стандарта IEEE 802.15.4 и набор его протоколов определяет только верхние уровни модели OSI: сетевой, транспортный и прикладной. Рабочим диапазоном частот для этого стандарта по всему миру является нелицензируемый диапазон 2,4 ГГц, при использовании которого максимальная скорость передачи данных составляет 250 Кбит [7].

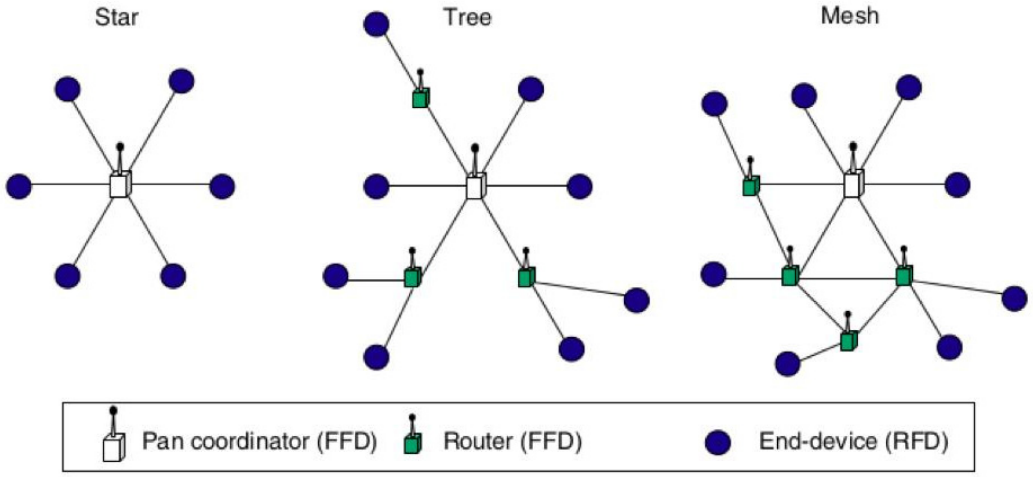


Рис. 6. Топологические схемы сети Zigbee

В ZigBee используется схема маршрутизации пакетов не от источника как в Z-Wave, а от адресата. Это определяет применение в mesh-сети ZigBee устройств трёх типов: координатора, формирующего и координирующего функционирование сети; постоянно активного маршрутизатора, обеспечивающего подключение до 32 оконечных устройств и динамическую маршрутизацию пакетов в сети; оконечных устройства, принимающих и отправляющих пакеты без возможности их ретрансляции (рис. 6). При этом аналогично Z-Wave обеспечивается перенаправление пакетов в случае отказа какого-либо из узлов и оперативное самовосстановление сети.

Существенным преимуществом ZigBee является его масштабируемость и возможность поддерживать до 65 000 узлов, что позволяет обеспечить охват значительной территории, при относительно небольшом (10-20 м в помещении) радиусе действия отдельных модулей.

С точки зрения безопасности в стандарте ZigBee возможно применение широкого спектра решений для обеспечения надёжной защиты, с использованием для шифрования и аутентификации данных 128-битного алгоритма AES и трёх типов ключей используемым, и тремя типами ключей.

В плане энергопотребления Zigbee уступает Z-Wave и даже Bluetooth, хотя отдельные устройства Zigbee сохраняют работоспособность без замены питающих элементов более двух лет. Экономия энергии достигается благодаря тому, что большую часть времени модули системы находятся в спящем режиме, а на пробуждение и выход из спящего режима затрачивается около 15 мс.

Существенный недостаток ZigBee связан с использованием только одного радио частотного канала, что определяет подверженность помехам создаваемым другими устройствами, работающими в перегруженном диапазоне частот 2,4 ГГц, который повсеместно используется беспроводными устройствами Wi-Fi и Bluetooth. Помимо этого большинство преимуществ технологии ZigBe при использовании для автоматизации умного дома нивелируются из-за несовместимости продуктов и решений разных вендоров.

В таблице 1 приведены основные характеристики стандартов беспроводной связи, используемых в системах домашней автоматизации [5].

Таблица 1

Сравнительные характеристики стандартов беспроводной связи,
используемых в системах домашней автоматизации

Технология	**Wi-Fi**	**Bluetooth Low Energy (BLE)**	**Z-Wave**	**ZigBee**
Стандарт	IEEE 802.11	IEEE 802.15.1	ITU-T G.9959	IEEE 802.15.4
Диапазоны частот	2400 МГц	2400 МГц	869 МГц (для России)	868 МГц, 902-928 МГц, 2400 МГц
Скорость передачи	250 Мбит/с	3 Мбит/с	10-100 кбит/с	50-240 кбит/с
Расстояние	10-100 м	10 метров	10-30 м	10-75 метров
Энерго-потребление	Высокое	Среднее	Низкое	Низкое
Топология сети	Дерево, звезда	Дерево, звезда	Ячеистая	Ячеистая
Совместимость	Совместимость устройств разных производителей не гарантирована из-за отсутствия прикладного уровня модели OSI	Хорошая, благодаря охвату всех уровней модели OSI	Охвачены все уровни модели OSI. Отличная совместимость устройств различных производителей	Отсутствует совместимость ZigBee- продуктов разных брендов

Как видно из таблицы по скорости передачи ZigBee превосходит Z-Wave, но уступает Wi-Fi, поэтому оптимальным решением при создании большой системы умный дом может стать использование сразу двух стандартов.

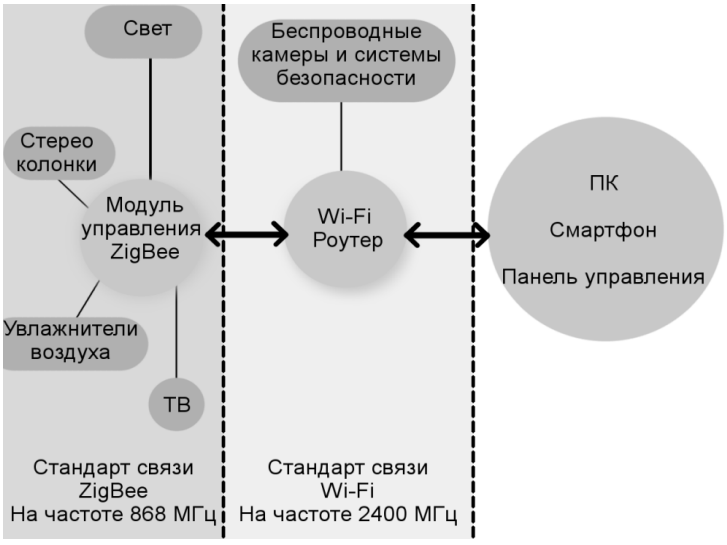


Рис. 7. Возможная реализация системы умный дом с совместным использованием технологий ZigBee и Wi-Fi

В частности, можно использовать Wi-Fi для связи со смартфоном или ПК с целью получения команд, и для подключения и передачи данных с камер (скорость ZigBee всё еще не позволяет передавать видео файлы в хорошем качестве [6]), а непосредственную автоматизацию дома производить на базе устройств стандарта ZigBee 0

Заключение

В системах домашней автоматизации с использованием беспроводных технологий управления наибольшее распространение получили четыре основных стандарта беспроводной связи. Не смотря на популярность и широкое распространение технологий Bluetooth и Wi-Fi они в настоящее время по совокупности технико-экономических и эксплуатационных характеристик существенно уступают стандартам беспроводного доступа Z-Wave и ZigBee, которые были разработаны и развиваются с учётом ориентации на эффективное использование в системах умный дом.

Литература

1. URL: https://www.popmech.ru/diy/396512-pyat-deystvitelno-poleznyh-funkciy-umnogo-doma/
2. URL: https://skomplekt.com/zwave_intro.htm/
3. *Росляков А.В., Ваняшин С.В., Гребешков А.Ю.* Учебное пособие "Интернет вещей". Самара: ПГУТИ, 2015.
4. *Тесля Е.В.* «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире, «Питер», 2008.
5. *Волгунов А.Д.* Обзор функциональных возможностей и перспектив развития систем домашней автоматизации // Молодой ученый. 2015. № 8.
6. *Егунов В.А.,* Ал-Саади Х.А. Управление «умным домом» с использованием беспроводного канала связи // Известия ВолгГТУ: Межвуз. сб. науч. ст. 3. Т. 20. № 6(133). Волгоград, 2014.
7. *Сандимиров С.А.* Создание современной концепции системы "Умный дом" // Молодой ученый: международный научный журнал. 2018. № 29 (215). С. 28-32 // Издательство "Молодой ученый", о-во с ограниченной ответственностью. Чита, 2018.
8. *Линь Л.Т., Дык Б.М.,Чыонг Н.Д.и др. Хю Н.Б., Хыонг Л.Ч* Сетевая модель OSI // Научные исследования. 2017. № 1 (12). С. 15-18.
9. *Ярощук В., Чмыхало Р.* Домашняя автоматизация // Современные проблемы радиоэлектроники и телекоммуникаций. 2018. № 1. С. 262(2).
10. *Пушкарев А.В., Орлов В.Г.* Эволюция технических средств формирования и доставки ТВЧ на мобильные терминалы пользователей // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 1. С. 11-16.
11. *Корионов И.П., Орлов В.Г.* Пользовательские аспекты безопасности в сетях LTE // Телекоммуникации и информационные технологии. 2017. Т. 4. № 2. С. 16-21.
12. *Гуров В.В., Орлов В.Г.* Обзор и сравнение протоколов MPTCP и CMT-SCTP // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2015. № 1. С. 115-119.
13. *Фадеев А.Н., Орлов В.Г.* Базовый стандарт для беспроводных сенсорных сетей // Телекоммуникации и информационные технологии. 2016. Т. 3. № 2. С. 65-68.
14. *Григорьев И.Д., Орлов В.Г.* Механизмы качества обслуживания в VDL MODE 4 // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2017. № 1. С. 129-133.
15. *Тихвинский В.О.* Пятый элемент мобильного мира: итоги MWC-17 // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 4-11.

16. *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.

17. *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.

18. *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.

19. *Константинов А.С., Пестряков А.В.* Анализ фундаментальных ограничений максимальной скорости передачи информации в сети LTE-advanced // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 12. С. 60-63.

20. *Поборчая Н.Е., Пестряков А.В.* Синтез и анализ алгоритмов оценки искажений сигнала в системе с MIMO в условиях априорной неопределенности // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 10. С. 13-20.

SELECTING WIRELESS COMMUNICATION STANDARDS FOR THE SMART HOUSE SYSTEM

Vladimir G. Orlov,
Chief specialist Department of OoRWoS PhD., MTUCI, Moscow, Russia
v.g.orlov@mtuci.ru
Sergey P. Tiumin,
Specialist Department of OoRWoS MTUCI, Moscow, Russia
s.g.tiumin@mtuci.ru

Keywords: *smart home, smart city, Wi-Fi, Bluetooth, BLU, Z-Wave, ZigBee.*

The functional purpose of the structural elements of the home automation system - smart home - is considered. Based on the analysis of the characteristics of wireless communication technologies, the criteria for choosing the most promising basic radio technologies for use in design solutions for home automation are given. The comparative characteristics of wireless control technologies for home automation systems and the most efficient standards and radio technologies in terms of technical and economic indicators, focused on use in smart home systems, are given.

РАЗРАБОТКА МОДЕЛИ ФОРМИРОВАТЕЛЯ СИГНАЛА С OCDM МОДУЛЯЦИЕЙ

Саттарова Анжела Ильдаровна,
инженер ФГУП НТЦ "Орион", Москва, Россия
ang.satt.97@gmail.com
Мирошникова Наталия Евгеньевна,
доцент кафедры РТС МТУСИ, к.т.н., Москва, Россия
n.e.miroshnikova@mtuci.ru

Ключевые слова: подводная беспроводная связь, акустическая беспроводная подводная связь, OCDM, ЛЧМ (Линейная частотная модуляция), ПЛИС

Рассмотрены вопросы моделирования устройства формирования сигнала с OCDM (Orthogonal chirp-division multiplexing) модуляцией. Приведена математическая модель сигнала с OCDM модуляцией, результаты моделирования формирователя OCDM сигнала в пакете прикладных программ MATLAB, а также результаты симуляции устройства формирования сигнала с OCDM модуляцией на ПЛИС Spartan-6 XC6SLX45.

Появление в водной среде искусственных сооружений, в частности, нефте- и газодобывающих структур, вызвало необходимость непрерывного контроля их поведения и, соответственно, автономных датчиков, способных накапливать и передавать информацию на пункты ее обработки. Недостатками подводной беспроводной акустической связи являются высокий уровень шумов и сильное многолучевое распространение [1-4]. Для борьбы с данными недостатками в подводном беспроводном акустическом канале все чаще применяют технологию OFDM (Orthogonal frequency-division multiplexing), позволяющую осуществлять передачу даже при достаточно сложных условиях распространения в канале. Подводный акустический беспроводной канал существенно отличается от радиоканала высоким уровнем шума окружающей среды, ограниченной полосой пропускания и сильно влияющим эффектом многолучевого распространения, что делает передачу данных через него очень сложной задачей [5-7]. Задержки в подводном акустическом беспроводном канале могут достигать десятков и сотен миллисекунд на большой глубине. Эффект Доплера при условии низких скоростей распространения сигнала (≈ 1500 м/с) значителен, что не позволяет моделировать его влияние сдвигом по частоте, как это часто делается для радиоканала, здесь необходимо учитывать масштабирование сигнала также времени, а не только по частоте [2, 8, 9]. Кроме того, на каждом пути распространения следует предусматривать не только относящееся к нему значение задержки, но и доплеровский масштаб, что часто не учитывается в работах по передаче сигналов в подводном беспроводном акустическом канале.

Использование OFDM модуляции в подводной беспроводной акустической связи было глубоко исследовано в литературе с целью повышения скорости передачи данных подводной телеметрии [10]. Такие системы продемонстрировали высокую спектральную эффективность в реальных подводных экспериментах, а также чувствительность к доплеровскому разбросу, который нарушает ортогональность поднесущих, приводя к межсимвольной интерференции. Таким образом, системы подводной беспроводной связи на основе OFDM часто требуют усовершенствованных алгоритмов компенсации межсимвольной интерференции [11-14].

Совсем недавно была предложена новая схема модуляции под названием OCDM в области волоконно-оптической связи [15, 16]. Основной принцип OCDM состоит в мультиплексировании нескольких сигналов с линейной частотной модуляцией (ЛЧМ сигналов), которые взаимно ортогональны друг другу и совместно используют одинаковую полосу пропускания и временной интервал.

Появление ЛЧМ сигналов, нашедших массовое применение в широкополосных системах связи, привнесло возможность использования простых, хорошо известных схем приема, основанных на согласованной фильтрации, что сделало такую схему особенно приспособленной для реализации в системах подводной связи [17, 18], при этом не оказывая негативного влияния на устойчивость системы к пагубным факторам, присутствующим в канале. Кроме того, технология OCDM имеет много общего с системой OFDM, что позволяет легко адаптировать существующие системы подводной беспроводной связи. Для дальнейшего анализа характеристик систем с OCDM модуляцией требуется построить математическую модель такой системы.

Основы построения OCDM систем

Фундаментом, лежащим в основе системы OCDM, является преобразование Френеля. Соответственно, цифровая реализация системы OCDM основывается на использовании дискретного преобразования Френеля (DFnT) также как при генерации OFDM сигнала используется дискретное преобразование Фурье (DFT). Таким образом, обратное преобразование Френеля (IDFnT) используется при формировании сигнала OCDM в передатчике, а прямое преобразование Френеля DFnT восстанавливает сигнал OCDM в приемнике.

Преобразование Френеля является интегральным преобразованием из классической оптики [1]. Это преобразование, которое математически описывает оптическую дифракцию ближнего поля. В случае, когда монохроматическая плоская волна с длиной волны λ сталкивается с щелью (решеткой), масштаб которой сопоставим по размеру с λ, результирующая дифракционная картина на пластине на расстоянии z определяется как:

$$\hat{s}(\tau) = F_a\{s(t)\}(\tau) = \frac{e^{-j\frac{\pi}{4}}}{\sqrt{a}} \int s(t) e^{j\frac{\pi}{a}(\tau - t)^2} dt, \quad (1)$$

где F_a {} (·) обозначает преобразование Френеля параметра $a = \lambda z$, являющегося нормированным расстоянием Тэлбота, а s (t) - комплексный коэффициент пропускания решетки. Ядро преобразования Френеля определяется как:

$$\varphi_a(t) = e^{-j\frac{\pi}{4}} e^{-j\frac{\pi}{a}t^2} \quad (2)$$

Дискретная форма преобразования Френеля (DFnT) формируется с помощью матрицы [19]:

$$\Phi(m,n) = \frac{1}{\sqrt{N}} e^{-j\frac{\pi}{4}} * \begin{cases} e^{j\frac{\pi}{N}(m-n)^2} & N \equiv 0 (\mathrm{mod}\, 2) \\ e^{j\frac{\pi}{N}(m+\frac{1}{2}-n)^2} & N \equiv 1 (\mathrm{mod}\, 2) \end{cases} \quad (2)$$

Матрица DFnT является унитарной, и ее другие важные свойства, такие как собственное разложение, можно найти в [19].

Математическая модель OCDM сигнала

В большинстве практических приложений рассматривается частотно-модулированный сигнал, частота которого изменяется линейно, а фаза изменяется со временем квадратично:

$$\psi(t) = e^{j(\pi a t^2 + \varphi_0)} \quad (3)$$

где α – скорость импульсов ЛЧМ.

Мгновенная частота такого сигнала:

$$f(t) = \frac{1}{2\pi} \frac{d}{dt} \left[\pi a t^2 + \varphi_0\right] = at \quad (4)$$

Чтобы использовать преобразование Френеля для формирования сигнала OCDM, необходимо установить некоторые ограничения. Во-первых, формы ЛЧМ-сигналов, используемые для передачи информации, должны быть ограничены по времени. Во-вторых, нужно адаптировать

пространственный эффект Тэлбота от оптики к временному аналогу OCDM. Основываясь на работе [19], форма «базового» ЛЧМ сигнала определяется как

$$\psi_0(t) = \prod_T(t)\varphi_a^*(t)\Big|_{a=\frac{T^2}{N}} = e^{j\frac{\pi}{4}}e^{j\pi\frac{N}{T^2}t^2}, 0 \le t \le T \tag{5}$$

где

$$\prod_T(t) = \begin{cases} 1 & 0 \le t \le T \\ 0 & otherwise \end{cases} \tag{6}$$

это прямоугольная функция.

Можно видеть, что (5) является сигналом ЛЧМ с периодом $\alpha = \frac{T^2}{N}$, а его произведение ширины полосы частот во времени составляет около $BT = N$. Можно получить набор из N отдельных ЛЧМ-сигналов с использованием основного ЛЧМ, описываемого формулой (5), а k-й сигнал ($k = 0,1,...,N-1$) будет иметь вид:

$$\psi_k(t) = \prod_T(t)\varphi^*_{\frac{T^2}{N}}(t - k\frac{T}{N}) = e^{j\frac{\pi}{4}}e^{-j\pi\frac{N}{T^2}(t-k\frac{T}{N})^2}, 0 \le t \le T \tag{7}$$

Легко доказать, что формы ЛЧМ ψ_k (t) в (7) взаимно ортогональны,

$$\int \psi_m^*(t)\psi_n(t)dt = \int_0^T e^{j\pi\frac{N}{T^2}(t-m\frac{T}{N})^2} e^{j\pi\frac{N}{T^2}(t-n\frac{T}{N})^2} = \delta(m-n) \tag{8}$$

Формула (7) задает набор из N ортогональных ЛЧМ-сигналов в заданных полосе частот и периоде.

В системе OCDM амплитуду и фазу каждого отдельного ЛЧМ-сигнала можно использовать для модуляции. Таким образом, могут быть использованы амплитудно-импульсная модуляция (PAM), PSK и QAM. В зависимости от типа модуляции символы выбираются из кодового алфавита из χ символов для представления информационных бит. Подобно символу OFDM, который состоит из группы поднесущих, передаваемых блок за блоком, модулированные одиночные ЛЧМ-сигналы также передаются в блоке. В блоке OCDM k-й символ, модулирующий k-й ЛЧМ, равен $x(k) \in \chi$. Таким образом, формируемый сигнал можно записать как:

$$s(t) = \sum_{k=0}^{N-1} x(k)\psi_k(t) \qquad 0 \le t \le T \tag{9}$$

На Рис. 1 представлены структурные схемы передатчика и приемника OCDM.

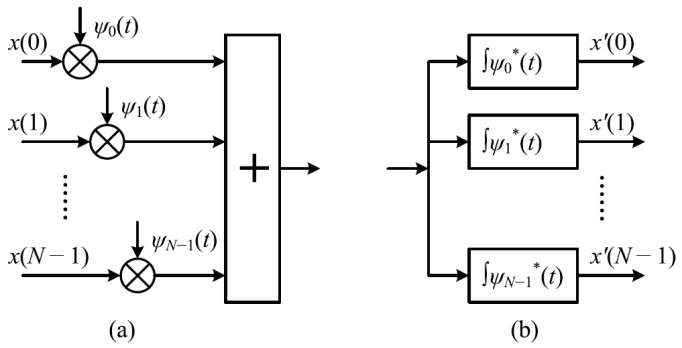


Рис. 1 Структурная схема приемника и передатчика OCDM (а) мультиплексирование и (б) демультиплексирование набора из N модулированных ортогональных ЛЧМ-сигналов.

Согласно (8), передаваемый сигнал x(m) может быть извлечен с помощью согласованного фильтра в m-й ветви, как показано на рис. 1 (б):

$$x'(m) = \int_0^T s(t)\psi_m^*(t)dt = \sum_{k=0}^{N-1} x(k)\delta(m-k) = x(m) \tag{10}$$

Матричная модель OCDM сигнала

В дискретном случае в моменты $\frac{mT}{N}$ из формулы (9) получаем:

$$s_m^k = s_k(t)_{t=m\frac{T}{N}} = \sum_{n=0}^{N-1} x_n^k \psi_n(\frac{mT}{N}) = e^{j\frac{\pi}{4}} \sum_{n=0}^{N-1} x_n^k e^{-j\frac{\pi}{N}(m-n)^2} \tag{11}$$

Из вышеприведенного выражения краткая матричная форма модуляции OCDM может быть выражена как:

$$s_k = \Phi^H x_k \tag{12}$$

$$s_k = \left[s_0^k \ldots s_{N-1}^k\right]^T, x_k = \left[xs_0^k \ldots x_{N-1}^k\right]^T \tag{13}$$

Унитарная матрица Ф, которая представляет собой так называемую матрицу дискретного преобразования Френеля (DFnT), определенную следующим образом для четного числа N:

$$\{\Phi\}_{m,n} = \frac{1}{\sqrt{N}} e^{-j\frac{\pi}{4}} e^{j\frac{\pi}{N}(m-n)^2} \tag{14}$$

На этапе демодуляции операция DFnT описывается следующим образом:

$$\hat{x}_k = \Phi s_k \tag{15}$$

Моделирование процесса формирования OCDM сигнала в среде MATLAB

В качестве входной информационной последовательности модели устройства формирования OCDM сигнала использовалась псевдослучайная последовательность, сгенерированная при помощи стандартной функции randi. В качестве метода модуляции использовался QAM-4. Число модулированных ЛЧМ сигналов N=64.

В результате моделирования были построены графики для трех немодулированных одиночных ЛЧМ-сигналов на интервале длительности одного информационного символа T , построенные по формуле 7, а также их суммы до дополнительных операций (рис. 2). Для удобства были взяты сигналы с k= 7 (красная линия), k=37(синяя) и k=57(зеленая), так как различия между ними хорошо различимы и виден характер изменения частоты во времени. На рисунке 3 продемонстрировано введение защитного интервала, а добавление циклического префикса представлено на рис. 4. График одиночных ЛЧМ-сигналов и их суммы после сглаживания фронтов приведен на рис. 5.

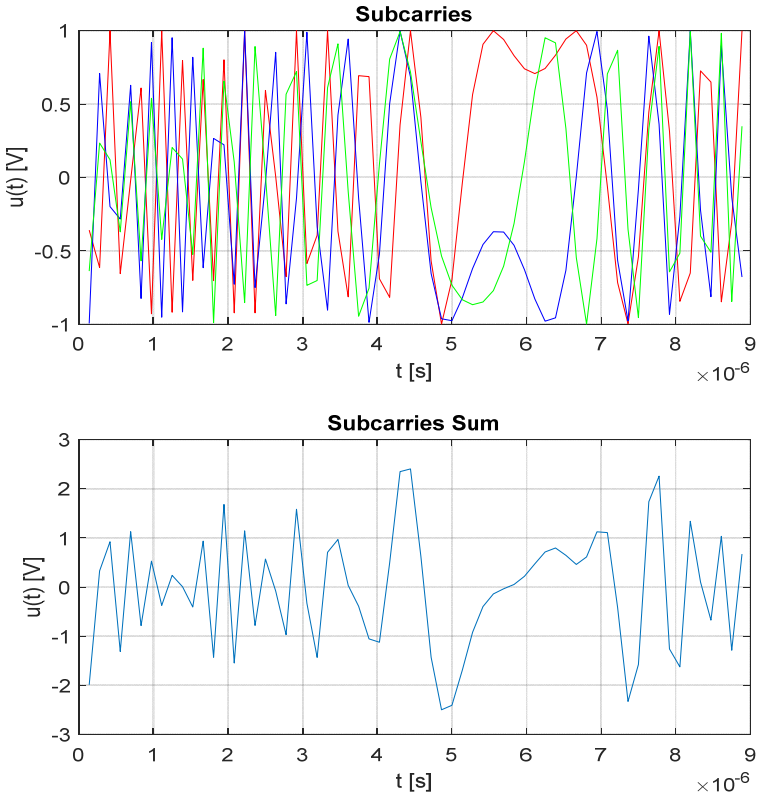


Рис. 2 Графики немодулированных ЛЧМ-сигналов и их суммы на интервале [0, T]

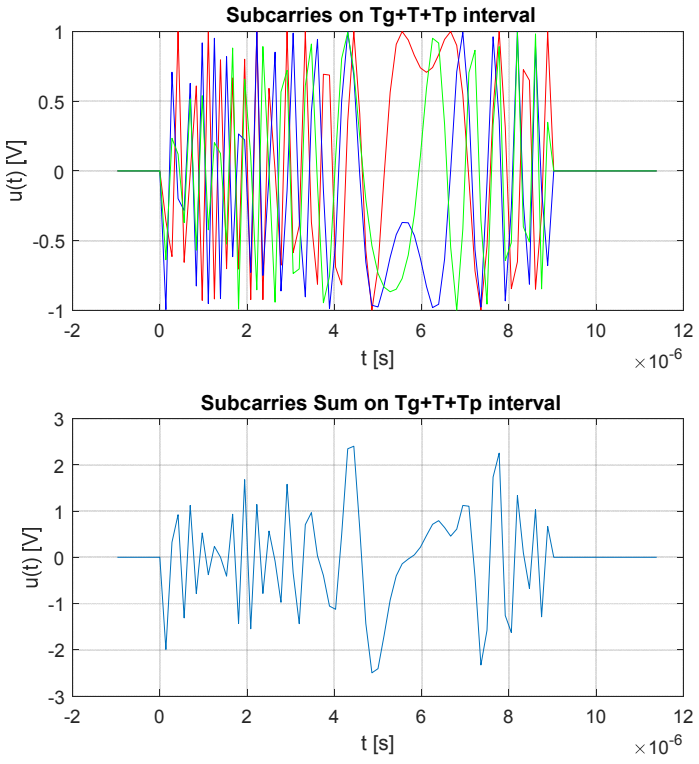


Рис. 3 Графики одиночных ЛЧМ-сигналов после добавления защитного интервала

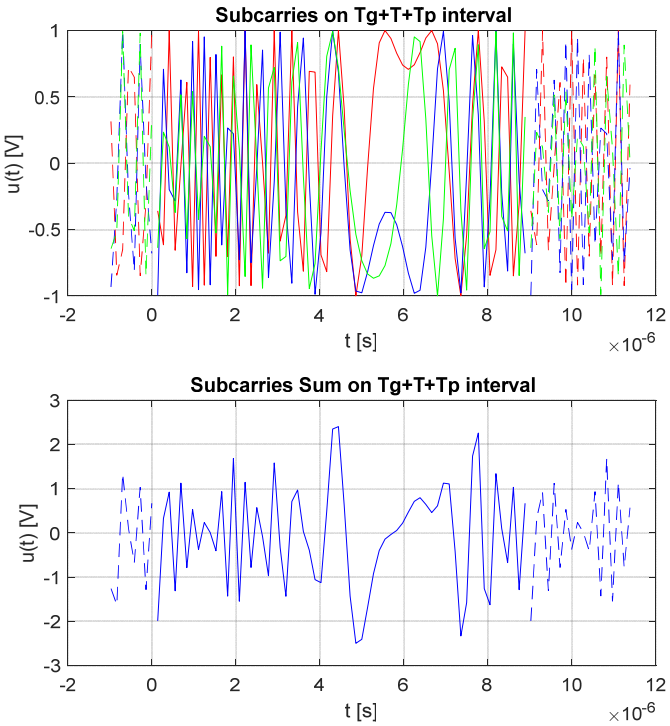


Рис. 4 Графики одиночных ЛЧМ-сигналов после добавления циклического продолжения их на защитный интервал и интервал постфикса

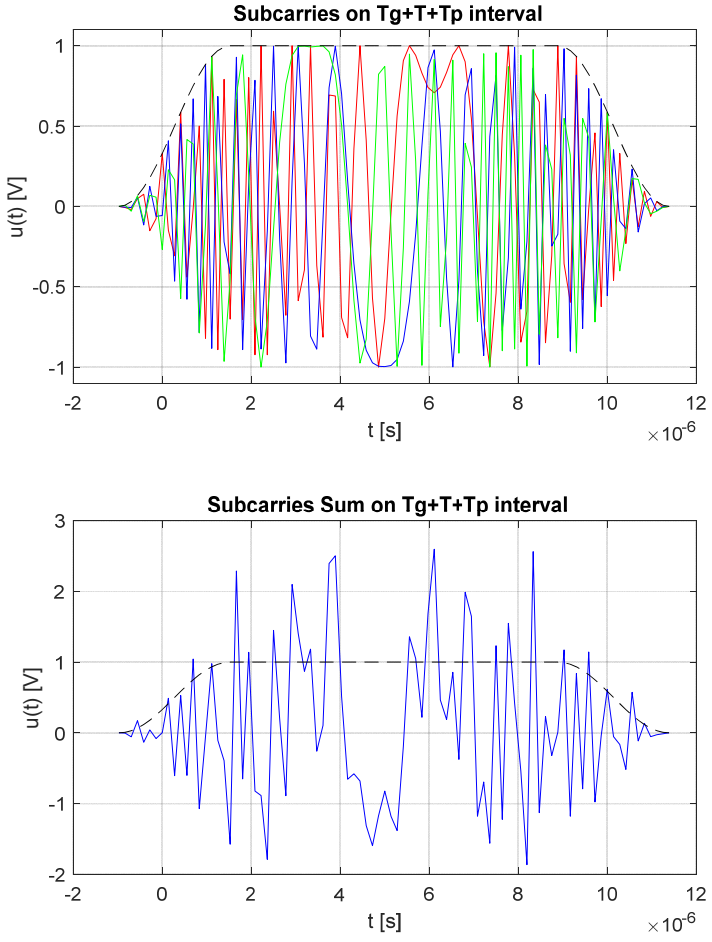


Рис. 5 Графики трех одиночных ЛЧМ-сигналов и их суммы после сглаживания фронтов

На Рис. 6 приведено формирование спектров трех последовательных OCDM символов построение их огибающих, которые отдаленно напоминают спектр аналитического ЛЧМ-сигнала, и огибающей их суммы.

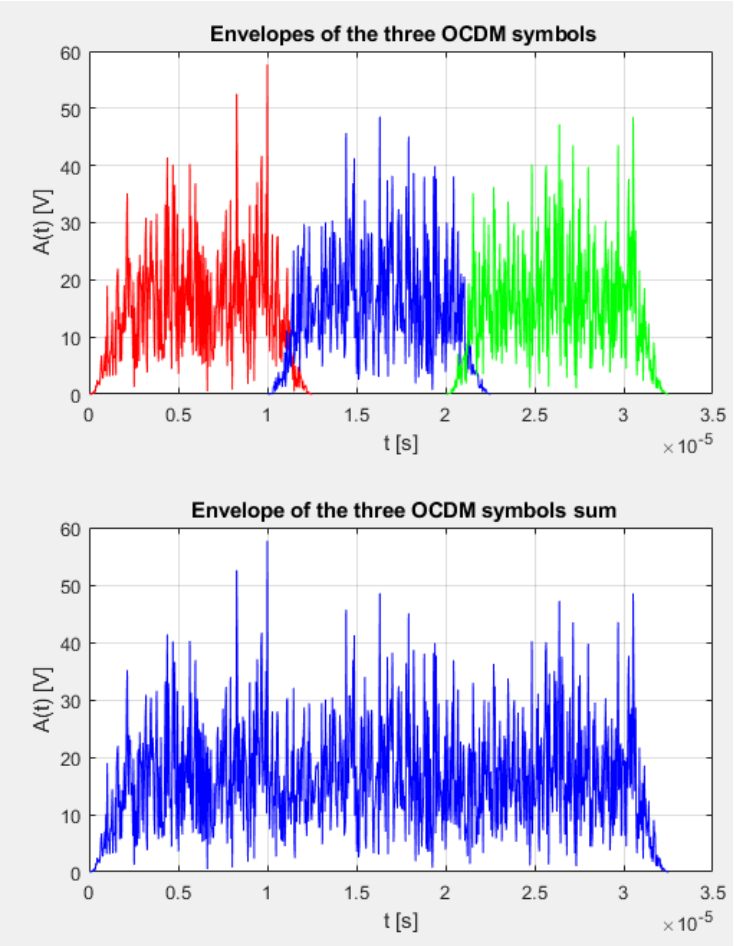


Рис. 6 Формирование спектров трех последовательных OCDM символов построение их огибающих и огибающей их суммы

Реализация устройства формирования OCDM сигнала на ПЛИС

Устройство формирования OCDM сигнала было реализовано в среде разработки XILINX ISE Design Studio на языке VHDL для демонстрации возможности его формирования на ПЛИС. Был реализован структурный блок, осуществляющий QPSK модуляцию входных данных. В результате тестирования его работы были получены выходные сигналы, соответствующие подаваемым на вход битовым последовательностям. Каждой входной двухбитовой последовательности ставилась в соответствие восьмибитовая последовательность, в зависимости от точки сигнального созвездия. Результаты моделирования представлены на рис. 7.

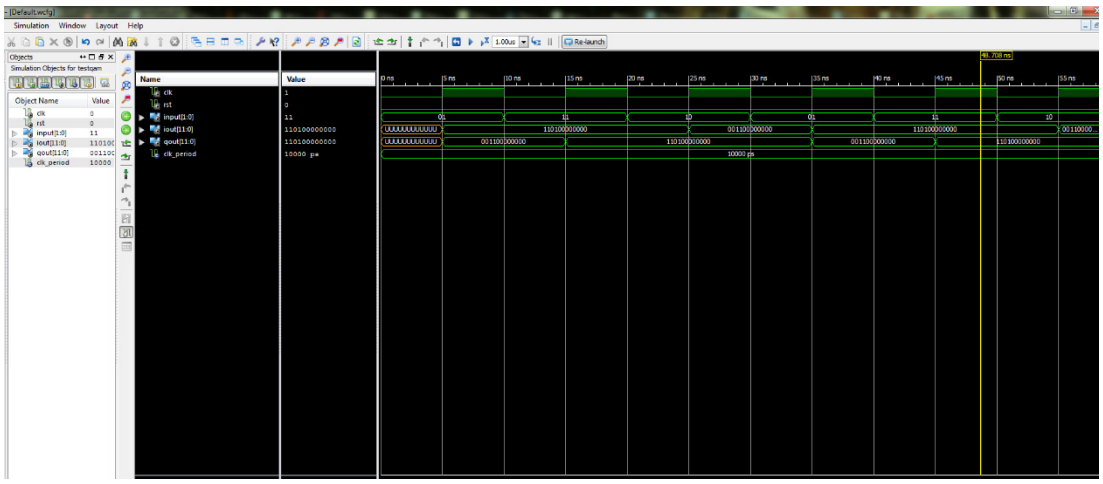


Рис. 7 Диаграммы работы QAM модулятора.

При реализации устройства, выполняющего обратное дискретное преобразование Френеля (IDFnT), были использованы предварительно рассчитанные в пакете прикладных программ MATLAB и записанные в постоянную память поворачивающие множители.

В результате симуляции были получены временные диаграммы сигналов на промежуточных стадиях преобразования Френеля, которые представлены на Рис. 8, а также временные диаграммы итогового результата работы, представленные на Рис. 9. На вход подается восемь 16-битных значений от QAM модулятора. Всего шестнадцать отсчетов (8 действительной части и 8 мнимой части комплексного отсчета). Каждый этап соответствует вычислению двухточечного преобразования Френеля.

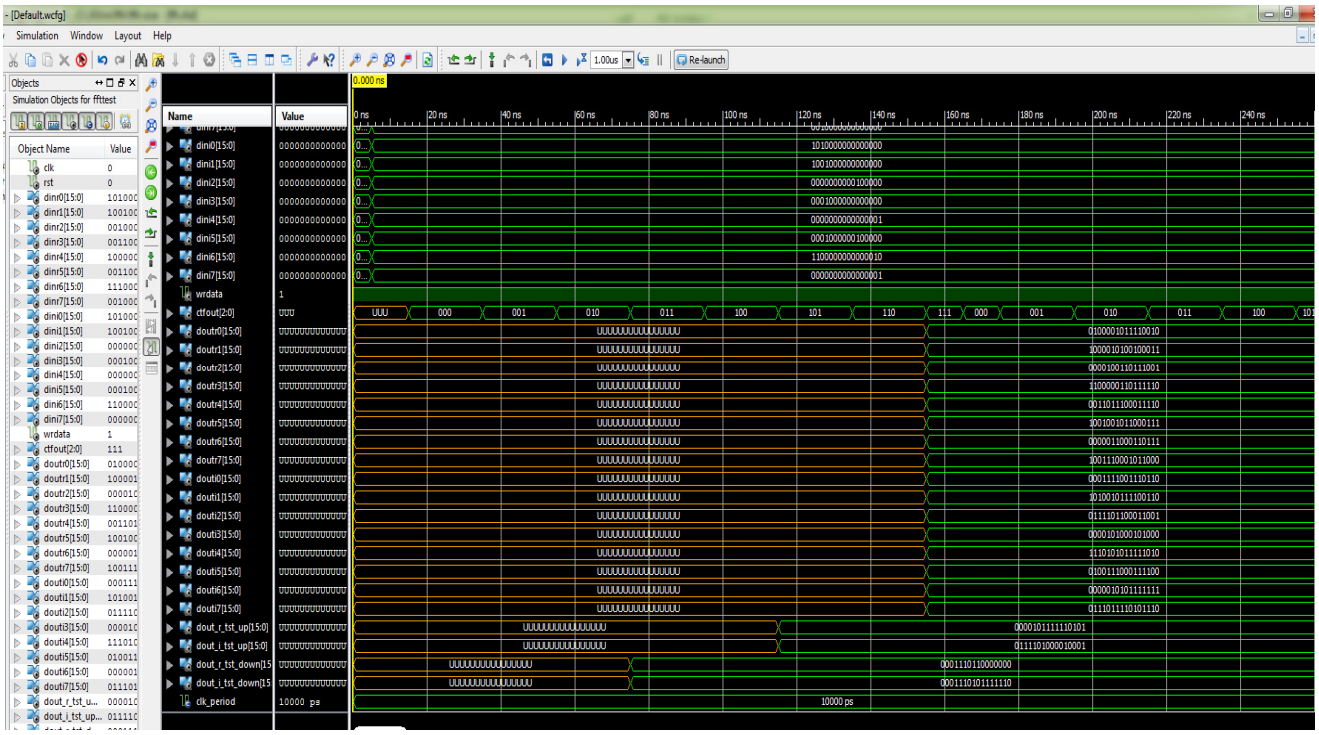


Рис. 8 Стадии преобразования Френеля

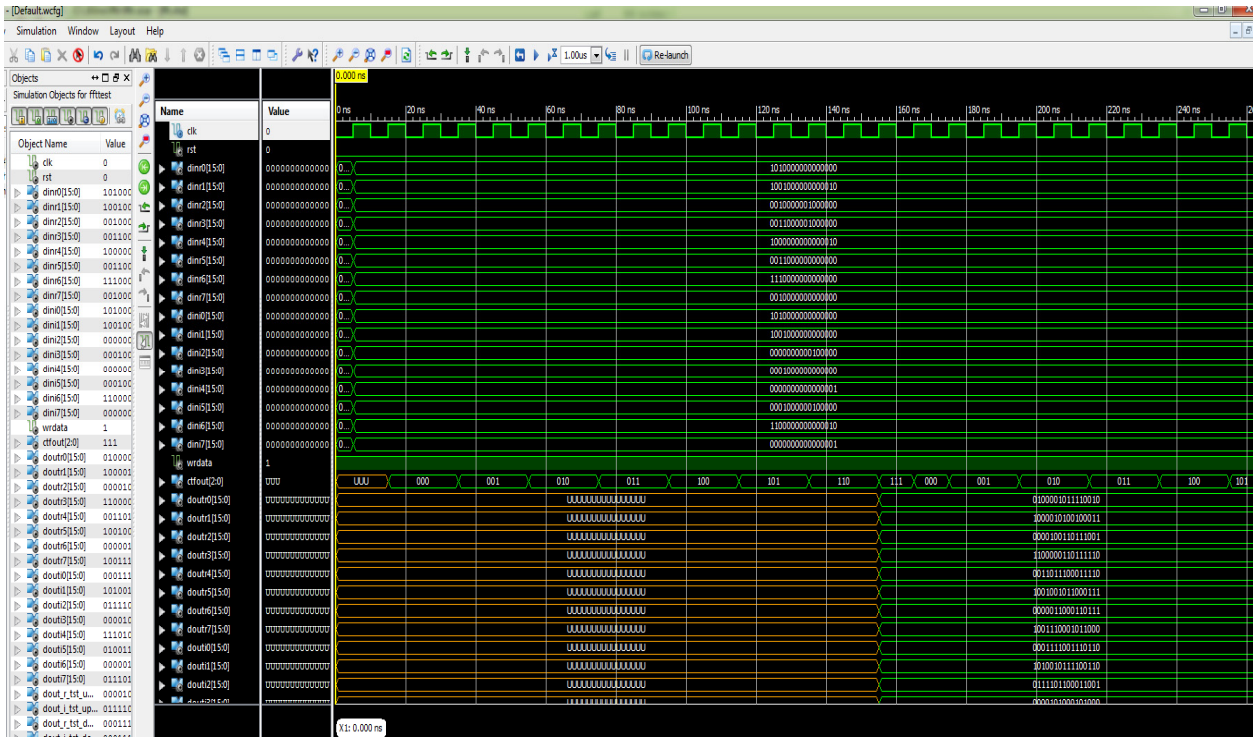


Рис. 9 Результат на выходе преобразования Френеля

Вычисление преобразования Френеля осуществляется с помощью быстрого преобразования Фурье с пересчетом поворачивающих множителей на каждой стадии. Для простоты, в проекте было реализовано преобразование Френеля на 8 одиночных ЛЧМ-сигналов. Таким образом, вычисление преобразования Френеля осуществляется в три этапа. Каждый этап занимает два такта счетчика. Таким образом на 7 такт производится выгрузка итогового значения из памяти, что видно из Рис. 9.

Заключение

Целью работы являлось построение имитационной модели устройства формирования OCDM сигнала. Для создания модели была использована матричная форма преобразования Френеля. Было произведено моделирование системы, осуществляющей генерацию OCDM сигнала при помощи пакета прикладных программ MATLAB, были получены осциллограммы промежуточных этапов генерации OCDM сигнала. Было реализовано программное описание формирователя OCDM сигнала с разложением на 8 ЛЧМ-сигналов для ПЛИС Spartan-6 XC6SLX45. Была произведена симуляция работы системы, для проверки правильности работы. Были получены итоговые и промежуточные значения сигнала на выходе системы

Литература

1. *H. F. Talbot,* “Facts relating to optical science. No. IV,” Philos. Mag.Ser. 3, vol. 9, no. 56, pp. 401-407, Dec. 1836.

2. *L. Rayleigh,* “On copying diffraction-gratings, and on some phenomena connected therewith,” Philos. Mag. Ser. 5, vol. 11, no. 67, pp. 196-205, Mar. 1881.

3. *J. T. Winthrop and C. R. Worthington,* “Theory of Fresnel images. I. Plane periodic objects in monochromatic light,” J. Opt. Soc. Amer.,vol. 55, no. 4, pp. 373-381, 1965.

4. *J. Wen, Y. Zhang, and M. Xiao,* “The Talbot effect: Recent advances in classical optics, nonlinear optics, and quantum optics,” Adv. Opt. Photon., vol. 5, no. 1, pp. 83-130, Mar. 2013.

5. *M. G. Solonenko, C. D. Mobley,* ``Inherent optical properties of Jerlov water types`` in Applied Optics Vol. 54, Issue 17, pp. 5392-5401 (2015) https://doi.org/10.1364/AO.54.005392

6. *M. Stojanovic.* Acoustic (Underwater) Communications. In Wiley Encyclopedia of Telecommunications; American Cancer Society: New York, NY, USA, 2003; doi:10.1002/0471219282.eot110.

7. *T.C. Yang,* Properties of underwater acoustic communication channels in shallow water. J. Acoust. Soc. Am. 2012, pp. 129-145.

8. *S. Chen, C. Tong, J. Liu,* Research on computer simulation about underwater acoustic communication channel. Modern Electronics Technique, 2008, no. 8, pp. 88–89.

9. *H. Deng, Y. Liu, H. Cai,* Time-varying UWA channel with Rayleigh distribution. Technical Acoustics, 2009, vol. 28, no. 2, pp. 109-112.

10. *F. Russo,* "Demodulator structures for pulse-frequency-modulated signals," IEEE Trans. Aerosp. Electron. Syst., vol. AES-12, no. 2, pp. 127-130, Mar. 1976.

11. *R. L. Brewster and W. W. S. Jibrail,* "Detection of FSK and DPSK data signals by pulse compression," IEE Proc. F Commun., Radar Signal Process., vol. 129, no. 4, pp. 273-280, Aug. 1982.

12. *J. Pinkney, R. Behin, A. Sesay, and S. Nichols,* "High-speed DQPSK chirp spread spectrum system for indoor wireless applications," Electron. Lett., vol. 34, no. 20, pp. 1910-1911, Oct. 1998.

13. *B. Li, S. Zhou, M. Stojanovic, L. Freitag, P. Willett,* Multicarrier Communication Over Underwater Acoustic Channels With Nonuniform Doppler Shifts. IEEE J. Ocean. Eng. 2008, 33, pp. 198-209.

14. *S. Zhou, Z. Wang,* OFDM for Underwater Acoustic Communications; John Wiley & Sons: Hoboken, NJ, USA, 2014.

15. *A. Kadri, R. K. Rao, and J. Jiang,* "Low-power chirp spread spectrum signals for wireless communication within nuclear power plants," Nucl. Technol., vol. 166, no. 2, pp. 156-169, May 2009.

16. *X. Ouyang, J. Zhao,* Orthogonal Chirp Division Multiplexing. IEEE Trans. Commun. 2016, pp. 46-57.

17. *J. R. Klauder, A. C. Price, S. Darlington, and W. J. Albersheim,* "The theory and design of chirp radars," Bell System Tech. J., The, vol. 39, no. 4, pp. 745–808, Jul. 1960.

18. *R. J. Dengler et al.,* "600 GHz imaging radar with 2 cm range resolution," in Proc. IEEE MTT-S Int. Microw. Symp. (IMS), Honolulu, HI, USA, Jun. 2007, pp. 1371-1374.

19. *X. Ouyang, C. Antony, F. Gunning, H. Zhang, and Y. L. Guan.* (2015). "Discrete Fresnel transform and its circular convolution." [Online]. Available: http://arxiv.org/abs/1510.00574

SIMULATION OF SYSTEM WITH OCDM MODULATION

Angela I. Sattarova,
Engineer FSUE STC "Orion", Moscow, Russia
ang.satt.97@gmail.com
Natalia E. Miroshnikova
Associate Professor of RTS Department MTUCI, Ph.D., Moscow, Russia
n.e.miroshnikova@mtuci.ru

Keywords: *underwater wireless communication, acoustic wireless underwater communication, OCDM, Linear Frequency Modulation, FPGA*

The article discusses the issues of modeling a communication system with OCDM (Orthogonal chirp-division multiplexing) modulation. A mathematical model of a signal with OCDM modulation, the results of modeling an OCDM signal in MATLAB application package, as well as the results of a simulation of a signal with OCDM modulation on a Spartan-6 XC6SLX45 FPGA are presented.

РАЗРАБОТКА ФУНКЦИОНАЛЬНОЙ МОДЕЛИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ NARROW BAND INTERNET OF THINGS (NB-IOT)

Артвел Регис Музата,
главный преподаватель и эксперт по ЭиТ, политехнического колледжа Хараре Зимбабве и колледжа Летаба ТПО Южная Африка
artwero@yahoo.com
Степанов Михаил Сергеевич,
доцент кафедры ССиСК МТУСИ, к.т.н., Москва, Россия
mihstep@yandex.ru

Одним из наиболее популярных решений для реализации концепции “Умный город” является технология Narrow Band Internet of Things (NB-IoT), которая может работать поверх сетей мобильной связи четвертого поколения LTE. Данная статья посвящена построению функциональной модели сети Интернета Вещей на базе технологии NB-IoT. Приведено описание общих принципов осуществления межмашинного взаимодействия, рассмотрена трехуровневая концептуальная архитектура Интернета Вещей. Обозначены основные проблемы внедрения и развития Интернета Вещей. Предложена функциональная модель сети сотовой связи стандарта LTE, обслуживающей трафик от камер видеонабюдения и большого количества “умных” датчиков, передающих данные с использованием технологии NB-IoT. Дано ее формализованное описание, которое ляжет в основу математической модели данной системы.

Введение

Быстрый рост плотности населения в городах вызывает необходимость развития инфраструктуры для оказания гражданам цифровых услуг нового поколения. Соответственно, наблюдается стремительное увеличение числа различных “умных” цифровых устройств (смартфонов, камер видеонаблюдения, счетчиков, датчиков и т.д.), которые, в свою очередь, объединяются в масштабные сети в соответствии с концепцией Интернета Вещей и взаимодействуют друг с другом без участия человека.

Интернет Вещей можно определить как сеть, состоящую из множества рассредоточенных физических интеллектуальных устройств, которые способны производить и обрабатывать информацию, а также обмениваться ей с другими устройствами. При этом, чаще всего, эти устройства отличают низкие возможности хранения и низкая вычислительная мощность. Взаимодействие происходит без участия человека. Одной из основных целей данной концепции является улучшение различных аспектов функционирования “умных” городов, в том числе, повышение надежности и безопасности их инфраструктуры. [1, 7-12]

С понятием Интернета Вещей неразрывно связана модель повсеместных вычислений (ubiquitous computing). Она заключается в том, что вычислительные устройства интегрируются в повседневные вещи, окружающие человека, и, таким образом, делают их интеллектуальными или “умными”. Их соединение в рамках сети осуществляется посредством фиксированных или мобильных сетей.

На рисунке 1 представлена архитектурная модель Интернета Вещей, состоящая из трех уровней – уровня восприятия, сетевого и прикладного. На первом уровне располагаются различные устройства, которые собирают и передают данные на вышестоящий уровень посредством Интернет соединения. В качестве примеров таких устройств можно привести метки радиочастотной идентификации (RFID), счетчики, камеры наблюдения, датчики, системы глобального позиционирования (GPS) и др. Число “умных” устройств в мире постоянно увеличивается, и по прогнозам [2,3] в 2025 должно превысить 75

миллиардов (рисунок 2). Основная функция сетевого уровня заключается в передаче информации с первого уровня на третий. Применяемые для этой цели технологии делятся на два вида, в соответствии с радиусом действия. К первому типу (малый радиус действия) относятся такие телекоммуникационные протоколы как Bluetooth и ZigBee. Примерами технологий второго типа (дальний радиус действия) можно назвать WiFi, сети сотовой связи различных поколений (2G, 3G, 4G), NB-IoT, LoRaWAN и другие. На уровне приложений данные собираются и анализируются.

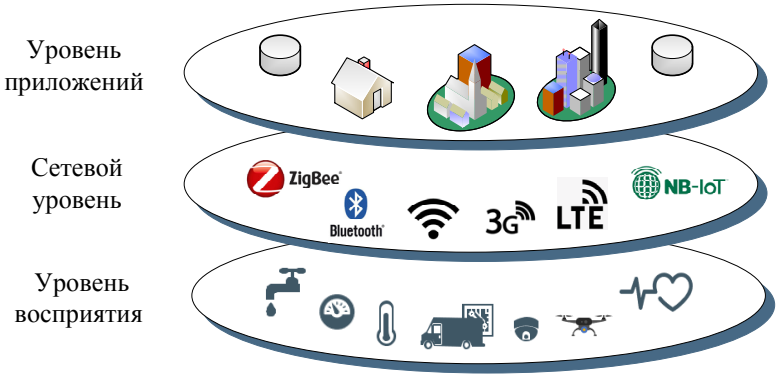


Рис. 1. Архитектурная модель Интернета Вещей

Для поддержания и масштабирования глобальной мультисенсорной инфраструктуры используемые технологии следует постоянно развивать. Вычислительные возможности “умных’ устройств должны увеличиваться, при этом необходимо сохранять их компактность и низкое энергопотребление. В связи с этим последние несколько лет в телекоммуникационной отрасли наблюдается рост инвестиций в научно-исследовательскую деятельность, направленные на совершенствование технологической составляющей решений Интернета Вещей. Немаловажную роль в работе сетей межмашинного взаимодействия играют средства управления “умными” устройствами, с помощью которых осуществляется их мониторинг, администрирование и диагностика.

В качестве примера популярных приложений Интернета Вещей можно привести различные решения для обеспечения безопасности и “умные” сети электроснабжения (Smart Grid), которые в автоматическом режиме перераспределяют электроэнергию, позволяя оптимизировать ее расход.

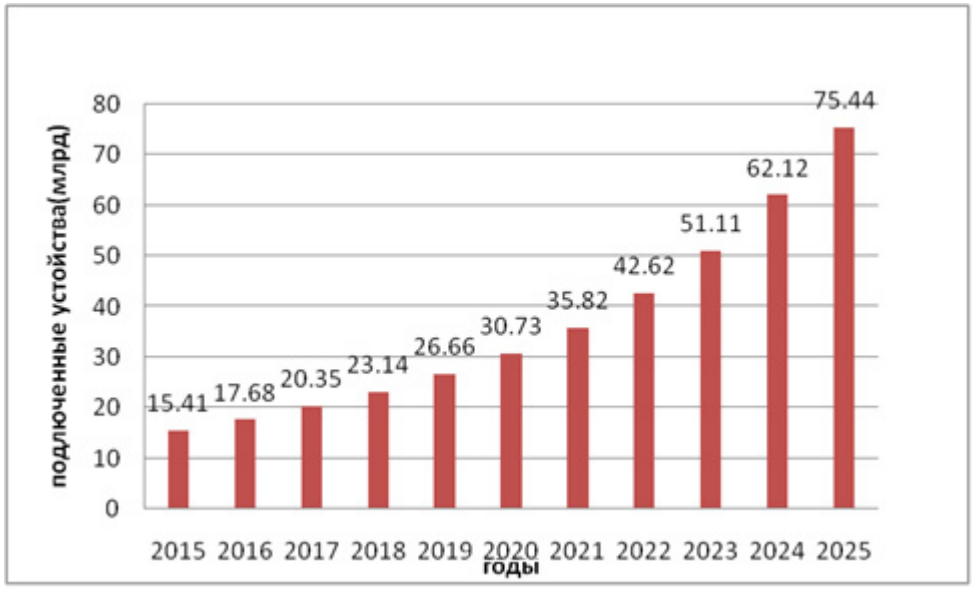


Рис. 2. Прогноз роста числа подключенных устройств Интернета вещей (IoT), (в миллиардах)

Проблемы внедрения и развития Интернета Вещей

Массовое подключение большого числа датчиков и сенсорных сетей к Интернету становится возможным благодаря переходу к 6-ой версии протокола IP. С точки зрения межмашинного взаимодействия, в IPv6 решена главная проблем её предшественника – ограничение адресного пространства. Новая версия основного протокола маршрутизации обеспечивает население Земли достаточным количеством адресов для взаимодействия миллиардов всевозможных устройств.

В настоящий момент существует ряд трудностей, препятствующих повсеместному внедрению решений Интернета Вещей. К ним относятся:

- Информационная безопасность и конфиденциальность данных;
- трудности в использовании уникальной идентификации;
- невозможность проводить крупномасштабные тестирования;
- недостаток работающих бизнес моделей в области Интернета Вещей.
- проблема обеспечения сетевой надежности.

Остановимся на последнем пункте списка. Интернет Вещей можно охарактеризовать как комбинацию нескольких интегрированных технологий, которые работают вместе в гетерогенной среде. Данные технологии представляют собой интерфейс между человеком и интеллектуальными устройствами, и их непрекращающееся развитие в скором времени приведет к тому, что беспилотный транспорт, роботизированные производства и “умные” дома станут обыденным явлением. Очевидно, что обеспечение надежности подобных систем и их безопасности для человека является первостепенной задачей. Здесь также существует ряд моментов, на которые следует обращать внимание при проектировании сетей межмашинного взаимодействия. Наиболее важным из них остается управление потоками информации, получаемыми одновременно от миллионов датчиков, и ресурсами (пропускной способностью), которая используется для передачи данных [3-5].

Обмен информацией между интеллектуальными устройствами происходит по каналам связи, в которых возможно возникновение помех. Их причинами могут стать:

- негативное влияние от смежных каналов связи;
- физические препятствия между передающей и приемной сторонами;
- негативное влияние от других технологий радиосвязи, с которыми “умные” устройства делят нелицензированные частотные диапазоны.

Для решения проблемы надежности передачи информации в каналах связи применяются различные механизмы. Наиболее простым является возможность повторной отправки сообщений, потерянных вследствие радиопомех [4, 6].

Негативное влияние на надежность сетей Интернета Вещей также оказывают перегрузки, которые могут произойти в случае передачи большого объема данных в режиме реального времени.

Построение сетей Интернета Вещей на основе технологии NB-IoT

Технология LTE (Long-Term Evolution) относится к четвертому поколению сетей сотовой связи. Впервые она была определена в серии документов Release 8, выпущенной консорциумом 3GPP в 2008 г. Увеличение пропускной способности каналов связи и скорости передачи данных в LTE достигается путем использования других радиоинтерфейсов и структурs пакетов, нежели в предыдущих системах UMTS/GSM и CDMA. Особое внимание уделяется использованию методов кодирования для систем с несколькими антеннами MIMO (Multiple Input Multiple Output), а также схеме модуляции с множественным доступом с частотным разделением каналов с одной несущей (SC-FDMA), используемой в восходящем канале связи, и многому другому.

В семействе технологий радиодоступа, разрабатываемых 3GPP, существует и стандарты для межмашинного взаимодействия. К ним относится технология Narrow Band Internet of Things (NB-IoT), описанная в Release 13 в 2016 году. Ее основным назначением является обеспечение подключения к сети большого количества “умных” устройств. Безусловно, главным преимуществом данного стандарта является возможность его использования поверх существующих мобильных сетей. В общем

случае для развертывания сети NB-IoT достаточно лишь обновить программное обеспечение оборудования LTE. Это, в том числе, помогает сократить время вывода на рынок новых услуг, что положительно сказывается на финансовых показателях компании. Экономическая эффективность также достигается за счет невысокой стоимости интеллектуальных устройств и их низкого энергопотребления.[3] Еще одним преимуществом является возможность передачи данных от устройств через сотовую сеть в тех местах, где проводные технологии по той или иной причине не доступны. Это особенно актуально в том случае, когда в качестве источников трафика выступают камеры наблюдения, один из ключевых элементов приложений “умной” безопасности с жесткими требованиями к качеству передачи.

Следует отметить, что выпустив спецификацию и определив режимы работы NB-IoT, 3GPP не предоставил руководящих указаний относительно того, как должно осуществляться совместное использование ресурсов между трафиком LTE и трафиком NB-IoT. Чаще всего проблема в этой области возникает при совместной передаче данных от “умных” устройств и трафика мобильных абонентов с различными требованиями по задержке.

Рассмотрим функциональную модель системы, которая состоит из некоторого количества камер для обеспечения видеонабюдения, и большого количества “умных” датчиков, контролирующих расход электроэнергии, температуру и т.д. [4-5] Схема функциональной модели приведена на рисунке 3. Предположим, что датчики подключены с использованием технологии NB-IoT. По изложенным выше причинам понятно, что подобное решение может эффективно работать в рамках одной беспроводной мобильной сети. Объем доступного радиоресурса соты LTE, необходимого для обслуживания поступающего трафика. в направлении восходящей линии связи измеряется в ресурсных единицах. LTE-устройства и NB-IoT-устройства являются источниками сеансов передачи данных, полученных в процессе видеосъемки и измерения характеристик работы наблюдаемых технических систем соответственно.

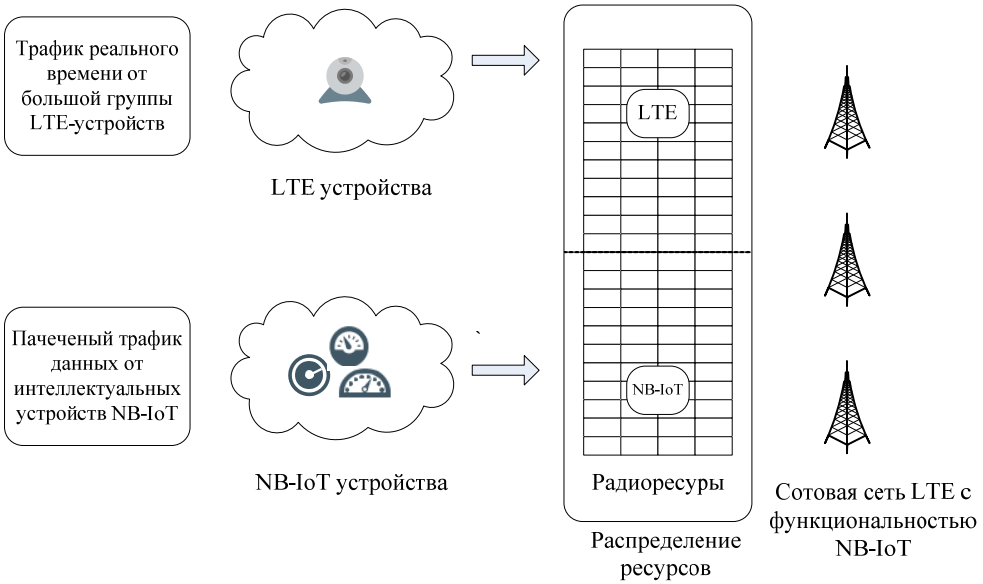


Рис. 3. Функциональная модель сети сотовой связи стандарта LTE с функционалом NB-IoT

На основе представленной функциональной модели в дальнейшем планируется построение математической модели совместного использования ресурса передачи данных в сети LTE с функциональностью NB-IoT. В ней будет рассмотрено два типа трафика. Источниками первого типа трафика являются камеры видеонаблюдения, и его потоки следуют либо модели Пуассона (если число источников велико), или модели Энгсета (если число источников мало). Второй тип трафика поступает от различных видов “умных” счетчиков. В этом случае, поток от NB-IoT-устройств следует модели Пуассона с групповым поступлением запросов и возможностью ожидания начала обслуживания, если все ресурсные единицы заняты. Средние времена осуществления различных событий в системе имеют

экспоненциальное распределение. Данную модель и полученные на ее основе характеристики планируется использовать для оценки эффективности передачи трафика в гетерогенных беспроводных сетях и для подготовки рекомендаций по их оптимизации.

Выводы

Таким образом, в статье:

1. Было дано описание концепции Интернета Вещей, приведены основные области применения и архитектурная модель.

2. Отмечено преимущество использования для межмашинных соединений технологии NB-IoT, которая может работать на сетях LTE

3. Предложена функциональная модель сети сотовой связи стандарта LTE, обслуживающей трафик от камер видеонабюдения и большого количества “умных” датчиков, использующих протокол NB-IoT.

В дальнейшем планируется построение математической модели данной системы, разработка методик оценки ее характеристик и использование полученных результатов для решения задач оптимизации сетей беспроводной связи.

Литература

1. *Talari, Saber, Miadreza Shafie-khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti and João P. S. Catalão.* Review of Smart Cities Based on the Internet of Things Concept, MDPI, 2017.

2. *Alam Tanweer.* A Reliable Communication Framework and Its Use in Internet of Things (IoT), 2018.

3. *Jimaa, Shihab & Chai, Michael & Chen, Yue & Alfadhl, Yasir.* (2011). LTE-A an overview and future research areas. The Proc of IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2011, Shanghai, China, October 10-12, 2011, pp. 395-399.

4. *Stepanov S., Stepanov M., Tsogbadrakh A., Ndayikunda J., Andrabi U.* Resource Allocation and Sharing for Transmission of Batched NB IoT Traffic over 3GPP LTE // The Proc of the 24th Conference of Open Innovations Association (FRUCT). Moscow Technical University of Communications and Informatics, April 8-12, 2019, Moscow, Russia, pp. 422-429.

5. *Степанов С.Н., Степанов М.С.* Эффективный алгоритм оценки требуемого объема ресурса беспроводных систем связи при совместном обслуживании гетерогенного трафика устройств интернета вещей // Автоматика и телемеханика. 2019. № 11. С. 108-126.

6. *Григорьев И.Д.,ОрловВ.Г.* Методы контроля качества обслуживания в мобильных самоорганизующихся сетях // Фундаментальные проблемы радиоэлектронного приборостроения. 2015. Т. 15. № 5. С. 292-296.

7. *Дудина В.А., Журко А.М., Степанов М.С.* Модель контакт-центра с учетом навыков операторов и нетерпеливости абонентов // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. № 12. С.43-48.

8. *Stepanov S.N., Shishkin M.O., Sosnovikov G.K, Stepanov M.S., Vorobeychikov L.A., Zhurko H.M.* The Analysis of Call Center Model in Case of Overload // T-Comm, 2019, vol. 13, no.11, pp. 68-76.

9. *Степанов М.С.* Определение и свойства входных параметров обобщенной модели контактцентра // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 7. С. 25-30.

10. *Пшеничников А.П., Степанов М.С.* Моделирование процесса обслуживания вызовов в современных контакт-центрах // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2015. № 1. С. 271-273.

11. *Степанов М.С., Степанов С.Н., Журко А.М.* Построение математической модели контакт-центра с учетом системы IVR // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 2. С. 253-255.

12. *Денисова М.А., Степанов М.С.* Оценка числа устройств IVR и операторов в контакт-центре с использованием метода декомпозиции // Телекоммуникации и информационные технологии. 2019. Т. 6. № 1. С. 49-54.

THE ANALYSIS OF THE PRINCIPLES OF CONSTRUCTION OF INTERNET OF THINGS NETWORKS BASED ON THE NB-IOT TECHNOLOGY

Artwell Regis Muzata,
Principal Lecturer and Eximiner in EaT, Harare polytechnic College Zimbabwe and Letaba TVET College South Africa,
artwero@yahoo.com
Mikhail S. Stepanov,
associate professor of CNaSS Department MTUCI, PhD., Moscow, Russia,
mihstep@yandex.ru

Key words: *Internet of Things, NB-IoT, LTE, machine-to-machine communication, functional model, data transmission.*

The rapid increase in urban population density necessitates the development of infrastructure for the provision of new generation digital services to citizens. Accordingly, there is a rapid increase in the number of "smart" digital devices (smartphones, video surveillance cameras, meters, sensors, etc.), which, are combined into large-scale networks in accordance with the concept of the Internet of Things that interact with each other without human participation. One of the main trends in the field of inter-machine communication is the use of technologies compatible with existing mobile networks, in particular, the Narrow Band Internet of Things (NB-IoT) standard. This article discusses the basic principles of the Internet of Things and the main problems of its implementation and development. A functional model of a cellular network of LTE standard with NB-IoT functionality is presented. The problem of congestion in the joint transmission of data from smart devices and the traffic of mobile subscribers with different delay requirements is noted, tasks for further research are formulated

ИССЛЕДОВАНИЕ ВЛИЯНИЯ МЕТОДОВ ШИФРОВАНИЯ НА КАЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ КАНАЛА СВЯЗИ

Ермолаев Дмитрий Алексеевич,
магистрант МТУСИ, Москва, Россия
ermolaev.andrei2014@yandex.ru
Попов Валентин Геннадьевич,
магистрант МТУСИ, Москва, Россия,
valentin1732@mail.ru
Кремер Аркадий Соломонович,
заведующий кафедры ТЭОД МТУСИ, к.т.н., доцент, Москва Россия
kremer@rans.ru

Ключевые слова: IPsec, DES, 3DES, AES, AH, ESP, EVE-NG, Cisco, влияние методов шифрования, качество связи, алгоритмы шифрования.

Представлены результаты исследования качественных характеристик канала связи при использовании шифрования и аутентификации посредством фреймворка IPsec. Для этого был разработан виртуальный стенд в среде эмуляции EVE-NG с использованием образа маршрутизатора Cisco 3725, реализующий схему сети Site-to-Site VPN.

В настоящее время в корпоративном сегменте широко применяется шифрование трафика. При больших его объёмах процесс шифрования может создавать значительную нагрузку на оборудование, а также влиять на качественные характеристики канала связи.

В работе будет рассмотрено: влияние процесса шифрования при использовании алгоритмов DES и AES на CPU оборудования, увеличения размера IP пакетов и их количества, изменение величины задержки и потерь. Для проведения эксперимента был построен виртуальный лабораторный стенд, реализующий схему сети Site-to-Site VPN over Internet в среде эмуляции EVE-NG с использованием образов оборудования Cisco.

Архитектура IPsec

В современных сетях передачи данных, услуга VPN предоставляется с использованием следующих технологий: открытого стандарта OpenVPN, фреймворка IPsec и протокола PPTP (Point-to-Point Tunneling Protocol). В работе мы рассмотрим IPsec. IPsec – это набор протоколов (Framework) для обеспечения защиты передаваемых данных, поверх протокола IP (рис. 1).

С использованием IPsec достигается концепция безопасности CIA Triad: Confidentiality, Integrity, Availability – конфиденциальность, целостность, доступность. IPsec обеспечивает Antireplay (все пакеты нумеруются и если пакет уже приходил, то второй пакет с таким же номером будет отброшен).

Создание защищенного соединения в IPsec происходит посредством протокола IKE (Internet Key Exchange, в реализации на оборудовании Cisco называется ISAKMP - Security Association and Key Management Protocol) и состоит из двух фаз:

Первая фаза. С использованием протокола IKE устанавливается IKE Security Association. Политика IKE SA содержит в себе набор параметров для создания служебного логического канала между узлами. Этот канал необходим только для обмена служебной информацией. В общем виде этапы первой фазы выполняются в следующем порядке:

- Обмен и проверка политик IKE SA на соответствие
- Генерация общего секретного ключа по алгоритму Диффи-Хеллмана
- Создание зашифрованного логического канала для передачи служебной информации

- Аутентификация узлов

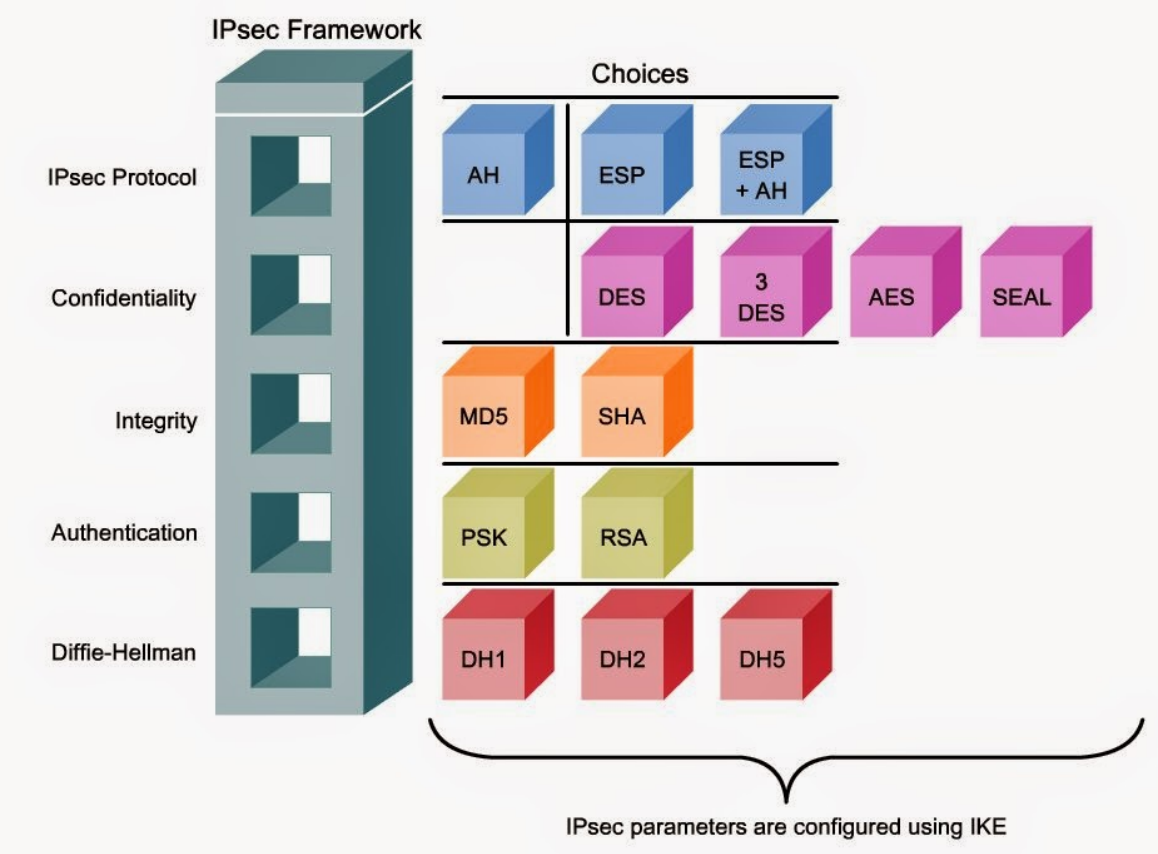


Рис. 1. Варианты протоколов и параметров конфигурации IPsec

Вторая фаза. IKE осуществляет согласование общей политики IPsec (в реализации Cisco – transform-set). В случае её согласования поднимается основной туннель. Далее IKE получает общие секретные ключи (так же используя алгоритм Диффи-Хеллмана из первой фазы) для алгоритмов протоколов IPsec (AH и/или ESP), так же устанавливает IPsec Security Association, но уже для основного туннеля. В общем виде этапы второй фазы выполняются в следующем порядке:

- Обмен и согласование IPsec SA по служебному каналу
- Создание основного защищённого логического туннеля для пользовательского трафика
- (Периодически) Пересмотр IPsec SA, для согласования в случае изменения
- (Опционально) выполняется обновление ключей по алгоритму Диффи-Хеллмана

Фреймворк IPsec возможно конфигурировать для двух режимов работы: туннельного и транспортного.

В транспортном режиме шифруется поле данных IP-пакета, адреса источника и назначения остаются неизменными. Транспортный режим используется при обеспечении защиты туннелей, организованных иным способом (например, GRE туннель).

При использовании туннельного режима работы IPsec, шифруется весь исходный IP пакет, затем полученная криптограмма добавляется к новому IP пакету, при этом IP адрес источника изменяется. Частный случай применения туннельного режима работы - объединение нескольких участков частной сети через Интернет.

В текущей работе был использован туннельный режим, при котором шифруется весь исходный трафик.

Моделирование сети

Для проведения эксперимента был реализован виртуальный стенд (рис. 2) в среде эмуляции EVE-NG с использованием образа маршрутизатора Cisco 3725.

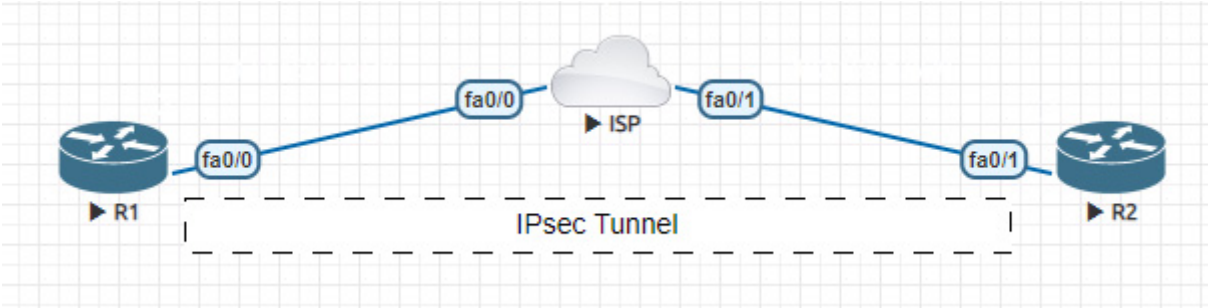


Рис. 2. Виртуальный стенд

R1 – 172.168.0.2/30, R2 – 192.168.1.2/30, ISP - шлюз провайдера

Пример типовой конфигурации IPsec для маршрутизатора Cisco представлен на рисунке 3:

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 180
crypto isakmp key SECRET address 192.168.1.2
!
!
crypto ipsec transform-set ESP-AES esp-aes 256 esp-sha-hmac
!
crypto map R1SEC 10 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set ESP-AES
 match address 120
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.168.0.2 255.255.255.252
 speed 100
 full-duplex
 crypto map R1SEC
```

Рис. 3. Типовая конфигурация IPsec

В эксперименте используется для первой фазы (служебного туннеля) шифрование AES с длиной ключа 256 bit, аутентификация PSK, Диффи-Хеллман группа 5 и время обновления туннеля и ключей 180 секунд. Эти параметры останутся неизменными на протяжении всего эксперимента.

Изменение непосредственно алгоритма шифрования основного туннеля происходит редактированием самого transform-set (IPsec SA).

Для набора статистики было сгенерировано 1000 ICMP-hello пакетов размером 1300 байт (1280 байт ICMP + 20 байт IP заголовок) в режиме без шифрования и с применением алгоритма AES, DES и 3DES (при шифровании пакетов, так же были проведены опыты при размере пакета 1400 и 1500 байт). Мониторинг осуществлялся с использованием ПО WireShark с виртуального интерфейса Fa0/0 маршрутизатора R1.

Таблица 1

Результаты эксперимента

	Задержка при передаче пакетов, мс	**Увеличение размера пакета, Байт**	**Потери, %**	**CPU, %**
Шифрование отсутствует	19,912	0	0	5.2
ESP-AES + AH	22,074	~20(ESP)+24(AH)	0.005	6.4
ESP-DES + AH		~20(ESP)+24(AH)	0.005	5.9
ESP-3DES + AH		~20(ESP)+24(AH)	0.005	6.001

Использование шифрования и аутентификации не оказало значительного влияния на CPU и задержку (график задержки представлен на Рисунке 5 и 6) при передаче/приёме, даже при увеличении размера пакета.

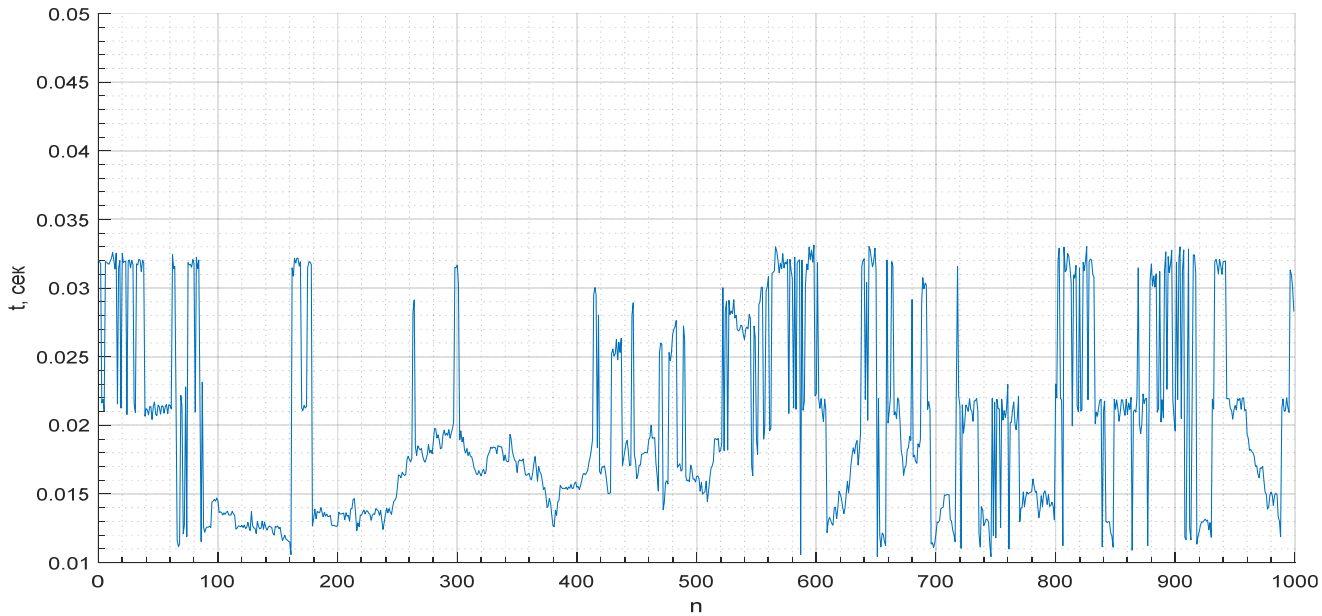


Рис. 4. График задержки в сети без использования IPsec

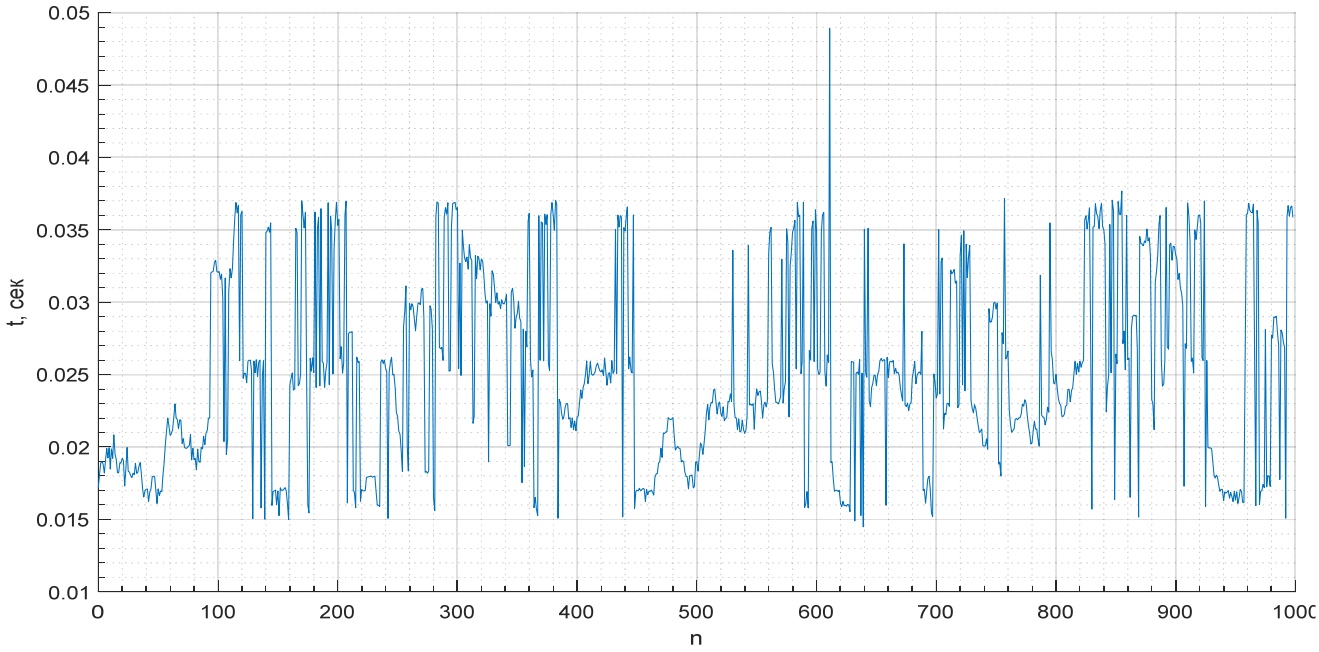


Рис. 5. График задержки в сети с использованием IPsec

Увеличение размера исходящего пакета так же было фиксированным и не зависело от размера изначального пакета. Это связано с тем, что AES, DES и 3DES – блочные шифры и размер блока после шифрования практически не изменяется. Однако, в случаях, когда исходный пакет превышает 1450 байт, использование шифрования и аутентификации приведёт к выходу за рамки максимального значения размера IP-пакета (поскольку добавляется заголовок ESP и AH, так же возможно округление последнего блока до кратного значения), что вызовет фрагментацию. Для предотвращения подобного эффекта в реализации IPsec в Cisco IOS есть функция компрессии, что позволяет уменьшить размер исходящего пакета в 8-9 раз.

Потери пакетов отсутствуют при передаче, однако, в реализации IPsec для Cisco IOS версии младше 12.4 присутствует следующая особенность.

После настройки всех параметров IPsec (применения конфигурации на оборудовании), зашифрованное соединение не будет установлено, пока не придёт запрос на передачу первого пакета. Как только приходит трафик, удовлетворяющий crypto acl (фактически простой acl), начинается выполнение фазы 1 и 2, за время согласование IKE SA и IPsec SA первые несколько пакетов теряются (рис. 7).

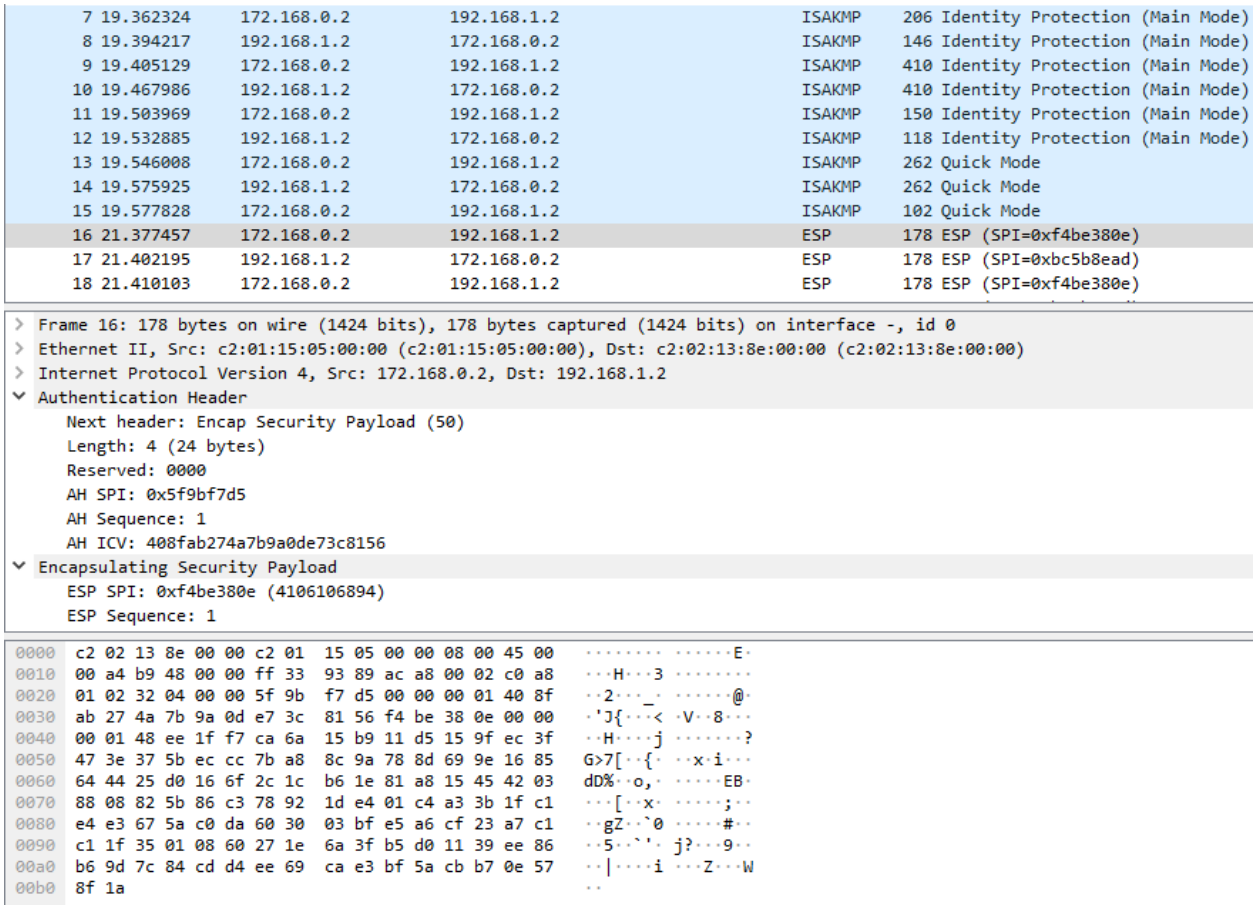


Рис. 6. Первая и вторая фаза IPsec, структура зашифрованного пакета

Использование отечественных алгоритмов

В данной работе рассмотрено использование только зарубежных алгоритмов шифрования, однако использование отечественных алгоритмов при построении систем в соответствии с ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624 четко определены.

Отечественная компания КРИПТОПРО предлагает программное решение для ОС Windows и Unix-подобных систем, в котором реализован фреймворк IPsec с применением алгоритмов,

сертифицированных ФСБ РФ. В качестве аппаратного решения возможно применение МСЭ производителей S-Terra и Check Point.

Литература

1. *S. Kent*. IP Encapsulating Security Payload (ESP). RFC 4303. BBN Technologies, December 2005. 43 p.

2. *V. Manral*. Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), RFC 4835, IP Infusion Inc. April 2007. 9 p.

3. IPsec, IP security [электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/IPsec.

RESEARCH OF THE INFLUENCE OF ENCRYPTION METHODS ON THE QUALITATIVE CHARACTERISTICS OF THE COMMUNICATION CHANNEL

Dmitry A. Ermolaev,
Graduate MTUCI, Moscow, Russia
ermolaev.andrei2014@yandex.ru
Popov G. Valentin,
Graduate MTUCI, Moscow, Russia
valentin1732@mail.ru
Dr.Arkadi Kremer
Associate professor of ToEDE Department MTUCI, PhD., Moscow, Russia
kremer@rans.ru

Keywords: *IPsec, DES, 3DES, AES, AH, ESP, EVE-NG, Cisco, influence of encryption methods, communication quality, encryption algorithms.*

The results of the study of the qualitative characteristics of the communication channel when using encryption and authentication using the IPsec framework are presented. For this, a virtual stand was developed in the EVE-NG emulation environment using the Cisco 3725 router image, which implements the Site-to-Site VPN network scheme.

ПРИМЕНЕНИЕ КОНЦЕПЦИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ ДЛЯ ПОСТРОЕНИЯ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ СЕТЕЙ

Калмыков Никита Сергеевич,
младший специалист АО "Позитивные Технологии", Москва, Россия
nikitakalmi25@gmail.com
Докучаев Владимир Анатольевич,
заведующий кафедрой СИТиС МТУСИ, д.т.н., профессор, Москва, Россия
v.a.dokuchaev@mtuci.ru

Ключевые слова: транспортная программно-конфигурируемая сеть, T-SDN, SD-WAN, программно-конфигурируемая территориально-распределенная сеть, ЦОД, полоса пропускания по требованию, OpenFlow.

В связи с постепенным переходом все большего числа приложений и сервисов в центры обработки данных, неуклонно растет объем передаваемой информации и возникает потребность в увеличении пропускной способности каналов связи и снижении стоимости эксплуатации и инсталляции сети. Одним из таких решений является программно-конфигурируемые сети (ПКС). В данной работе затронуты аспекты построения транспортных ПКС и проведен анализ решений от нескольких производителей. Также были исследованы положительные и отрицательные стороны программно-конфигурируемых территориально-распределенных сетей (SD-WAN).

Введение

В последние годы наблюдается тенденция переноса как можно больших вычислительных ресурсов с клиентских мощностей на «облачные» платформы и вычислительные мощности ЦОД (центров обработки данных). Вследствие такого рода изменений в архитектуре сервисов и приложений резко возрастают объемы передаваемых данных, в частности в сторону «последней мили». В качестве примера можно привести различные стриминговые сервисы, где на оконечное устройство возложена лишь задача воспроизведения готового потока видео и звука. В таких сценариях работы помимо большого объема данных важна еще и минимальная задержка при передаче.

Помимо различных сценариев для домашней работы, не менее важным вариантом использования удаленных вычислений является так называемая инфраструктура как услуга (Infrastructure-as-a-Service; IaaS). При таком сценарии работы, компания арендует в ЦОД определенный набор платформ, мощностей и объемов данных. Такой вариант использования «облачных» технологий позволяет отказаться от содержания собственных вычислительных мощностей, что зачастую позволяет сэкономить на оборудовании, площадях и инженерном штате.

Для территориально распределенных компаний одной из важнейших задач является объединение всех филиалов в единую сеть. Зачастую используются дорогостоящие каналы MPLS, предоставляемые различными операторами связи, однако благодаря применению технологий программно-конфигурируемых сетей, возникло такое явление как SD-WAN (программно-конфигурируемая территориально-распределенная сеть). SD-WAN решения позволяют выполнять балансировку трафика сразу по нескольким путям передачи, например – по LTE и обычному широкополосному соединению. Динамическое распределение трафика позволяет снизить затраты на дорогостоящие каналы связи, не теряя в качестве передачи и минимизируя время простоя при неиспользовании каких-либо каналов передачи.

В каждом из приведенных сценариев значительную роль может играть технология программно-конфигурируемых сетей, в одном из трех основных вариантов использования на данный

момент. «Классический» SDN (программно-конфигурируемая сеть) – может быть использован для нужд виртуализации экосистемы ЦОД. Транспортный SDN – используется для объединения ЦОД или построения мультивендорной транспортной сети операторов связи. Отдельно стоящие решения SD-WAN – могут применяться распределенными компаниями со множеством филиалов, или же для соединения ЦОД.

Программно-конфигурируемые сети

В основе концепции ПКС лежит идея разделить уровень передачи данных и уровень управления. Такие решения на основе разных протоколов уже достаточно давно существуют на рынке, однако наибольшую популярность завоевали решения, базирующиеся на открытом протоколе OpenFlow.

История ПКС берет свое начало в 90-х годах, когда были добавлены некоторые функции программирования к сетям. Вся история ПКС может быть представлена в виде трех этапов:

1. С середины 90-х годов до начала 2000-х. Данный этап ознаменован появлением так называемых «активных сетей», где впервые была реализована возможность программно вносить какие-либо изменения;
2. С 2001 по 2007 годы были попытки реализации разделения уровней передачи данных и управления, разрабатывались открытые интерфейсы между этими плоскостями;
3. С 2007 по 2010 года были успешно реализованы множество сетевых операционных систем, а главной вехой для ПКС стало появление интерфейса API OpenFlow. Этот момент можно считать отправной точкой для начала широкого распространения концепции ПКС.

Наиболее значимой частью ПКС является контроллер ПКС, на него возложены функции управления всей сетью. Остальные же устройства сети не принимают участия в принятии решений об отправке пакетов, адресации, и т.д.

В настоящее время на рынке достаточно большое число разных контроллеров ПКС, которые могут управлять набором маршрутизаторов и коммутаторов при помощи протокола OpenFlow, или ему подобного.

Протокол OpenFlow определяет правила потока для каждого сетевого устройства путем рассылки модифицированной таблицы передачи, таким образом, что плоскость управления может управлять плоскостью передачи данных. Правила потока могут содержать в себе различные установки для сетевых устройств, такие как:

- MAC – адреса устройств источника и назначения;
- IP-адреса устройств источника и назначения;
- параметры протокола TCP для устройств источника и назначения;
- данные о виртуальной (логической) локальной сети VLAN в общей инфраструктуре;
- различные метки и метрики, например QoS или метки MPLS;
- другую необходимую информацию для составлений правил потока.

Основная ценность OpenFlow заключается в том, что он реализуется автоматически через контроллер ПКС в сети, позволяет забрать на себя управление плоскостью передачи, значительно упрощает и ускоряет работу с настройкой сетевого оборудования, а также расширяет функциональные возможности сетевых устройств. Практически каждый крупный производитель телекоммуникационного оборудования обладает собственными решениями и оборудованием для построения ПКС. В числе производителей такого оборудования можно обозначить следующих гигантов: Cisco, Huawei, Juniper, Nokia, и многие другие.

Продукция каждого из производителей в основном функционале схожа, но разница заключается в числе решений, и в различной специализации оборудования. Таким образом Nokia в основном предлагает решения для транспортных ПКС. Juniper в свою очередь в основном предоставляет решения для корпоративных сетей, включающих в себя SD-WAN и SD-Branch. Cisco и

Huawei предлагают наиболее обширный набор решений, включающий в себя как решения для распределенных офисов компаний, так и решения для использования в ЦОД.

В центрах обработки данных [1,2, 12-13] ПКС главным образом помогает построить так называемый SDDC (программно-конфигурируемый ЦОД). Такие ЦОД позволяют гораздо более эффективно реализовать виртуализацию различных составляющих сети и серверной части. Помимо того, такая система позволяет объединять ЦОД в сеть, что значительно повышает катастрофоустойчивость системы и расширяет возможности резервирования данных. Еще одним значительным преимуществом применения ПКС в ЦОД с обширной и разнородной инфраструктурой, является возможность значительно упростить управление и внедрение нового оборудования и сервисов. Применение подхода ПКС позволяет построить на базе разнородной инфраструктуры от разных производителей виртуализованную среду с гибким разделением ресурсов, вычислительных мощностей и т.д. Важным свойством ПКС для ЦОД является возможность создания виртуальной сети, которая может предоставлять необходимые для приложений сервисы в нужное время, т.е. осуществляя функционал полосы пропускания по требованию (Bandwidth-On-Demand – BOD), что весьма важно для больших объемов трафика на сети ЦОД. Производители телекоммуникационного оборудования стараются поставить на рынок комплексные, экосистемные решения, которые будут во всем удовлетворять пользователя, тем самым не вынуждая переходить на гетерогенную среду. Однако существует достаточно большое количество решений на базе открытого ПО, которое можно полностью настроить под нужды компании, при этом не упираясь в продукцию одного производителя. Однако для крупных компаний такой подход может оказаться неприемлем в силу того, что покупая ПО и оборудование проприетарное – покупатель всегда может обратиться за поддержкой, техническим обслуживанием и сопровождением к поставщику, а в случае с открытыми продуктами, нет компании ответственной за ПО и оборудование.

Во множестве компаний системы такого рода функционируют уже достаточно длительное время. В России же аналогичные шаги по внедрению осуществляют ограниченное число компаний, но в будущем оно будет только расти. В числе первых можно выделить Ростелеком, который проводил тестирования по внедрению ПКС на собственных ЦОД [3]. Помимо работы по внедрению технологий ПКС для ЦОД, у Ростелекома есть и проекты, касающиеся программно-конфигурируемой транспортной инфраструктуры – T-SDN. Одним из таких тестовых запусков было пробное развертывание мультивендорной транспортной сети в условиях лаборатории [4]. А затем был создан и отдельный участок сети с использованием технологий ПКС на юге страны [5].

Программно-конфигурируемые распределенные сети

Как было упомянуто выше – одним из важных трендов для корпоративных сетей становится технология SD-WAN. Для обычной сети WAN характерны такие проблемы как: высокая стоимость и сложность эксплуатации, недостаточная масштабируемость и гибкость, в ряде случаев недостаточная пропускная способность и недостатки в области информационной безопасности. Решить многие проблемы позволяет применение основных принципов ПКС, но в данном случае на распределенную сеть. Такая сеть отличается от обычной WAN тем, что конфигурирование сети происходит не на уровне аппаратных маршрутизаторов, а на программном уровне. Как и в ПКС уровень управления сетью отделен от уровня передачи данных, и применяется централизованное управление потоками трафика и маршрутами в сети. Таким образом, становится возможным программно подобрать наиболее дешевый и незагруженный канал без потери качества передачи.

Значительным плюсом централизованного управления является упрощение масштабируемости сети, возможность мониторинга в реальном времени всех сегментов сети, а значит и возможность оперативного реагирования на любые изменения.

Подобные решения наиболее выгодны для использования территориально распределенным организациям, в местах, где возможна нестабильность каналов связи: несколько физических каналов можно объединить в один логический, с программной балансировкой трафика в зависимости от текущих условий.

Однако, несмотря на преимущества технологии SD-WAN, она несет в себе и значительные сложности для компаний. Согласно аналитическому отчету компании AVANT [6], технология признана наиболее требовательной по вносимым изменениям в устоявшиеся модели и решения. Такие данные в отчете представлены на основе опроса большого числа респондентов среди руководителей ИТ направлений разных областей. Необходимо сказать, что пока еще технология SD-WAN, в отличие от более широко известной ПКС, не имеет достаточно четкого описания, а потому в ее представлении возникают разногласия. Достаточно большая часть опрошенных людей высказала свои опасения насчет безопасности новой технологии, в сравнении ее с MPLS. Однако также многих руководителей в особенности малого бизнеса прельщает значительное снижение расходов на выделенные каналы MPLS.

Программно-конфигурируемые транспортные сети

В связи с быстрым развитием ЦОД и появлением множества услуг и сервисов на их основе (Платформа как сервис - Platform as a Service – PaaS, Инфраструктура как сервис -Infrastructure as a Service – IaaS, и т.д.) возникла необходимость соединять между собой центры обработки данных. Такие соединения ЦОД были названы DCI – Data center interconnect. Однако для реализации облачных сервисов необходимо обеспечить маршрут в высокой пропускной способностью и низкими задержками между ЦОД. Для таких соединений с гарантированной пропускной способностью может быть использована технология, названная программно-конфигурируемой транспортной сетью (T-SDN). Такие сети позволяют реализовать сервис Bandwidth on demand (BoD), полоса пропускания по требованию.

В традиционной архитектуре транспортной сети выделяются три уровня управления:

- Уровень централизованной системы эксплуатации (OSS)
- Уровень системы управления сетью (NMS)
- Уровень системы управления элементами сети (EMS)

А также уровень самой транспортной сети, реализованной либо на стеке IP/MPLS, беспроводной радиосвязи или оптической сети (WDM, OTN).

В традиционной транспортной сети существует иерархия уровней управления, от OSS к EMS. Таким образом, выполнение спектра различных задач проходит по всей иерархии, от OSS к сетевым элементам, таким как маршрутизаторы, коммутаторы или оптические коммутаторы, через уровни системы управления сетью и управления элементами сети. Вследствие этого, решение иерархических задач при традиционной схеме сети является процессом трудоемким и длительным. Процесс создания нового маршрута для потока может занимать несколько часов, или даже дней, в случае необходимости перенастройки оптических транспондеров.

В свою очередь, в программно-конфигурируемых транспортных сетях взаимодействие между приложениями и контроллером ПКС происходит через специальный сервисно-ориентированный интерфейс (REST-API), который обеспечивает удобство управления и упрощает команды. Помимо того, используются протоколы реального времени такие как OpenFlow и PCEP (Path Computation Element Protocol), позволяющие эффективно взаимодействовать контроллеру с сетевыми устройствами в режиме реального времени [7].

В качестве примера готового решения программно-конфигурируемой транспортной сети можно привести решение от компании Huawei. У Huawei наработан достаточно большой опыт в создании ПКС, поэтому собственная архитектура [8] транспортной ПКС была разработана и испытана [9,10]. Совместно с компанией Telefónica в 2018 году Huawei протестировали T-SDN решение на сети оператора в Испании, оно было призвано решить проблемы, связанные с внедрением достаточно крупной оптической сети с использованием ROADM – переконфигурируемого оптического мультиплексирования ввода/вывода, так как возникали сложности в эксплуатации и техническом обслуживании. Еще одним успешным внедрением стало создание совместно с China Unicom Beijing выделенной линии на основе T-SDN для правительственного и бизнес использования.

Еще одна одним примером может служить контроллер T-SDN от компании Netcraker [11]. Компанией было создан продукт, имеющий модульную структуру, и позволяющий реализовать следующие функции:

- Автоматизированное развертывание сервисов в сети по запросу клиента
- Мониторинг сетевых устройств, ошибок и уведомлений
- Автоматическое переключение на защитный маршрут в случае выхода из строя порта устройства, либо перерасчет пути в случае невозможности ухода устройством на защитный маршрут.

Заключение

Рынок решений как для транспортной ПКС, так и для SD-WAN еще далеко не полностью оформился, у многих производителей есть что предложить покупателям, но переход на новое оборудование достаточно дорог и не все компании могут себе его позволить. Однако определенная заинтересованность в таких решениях существует, поскольку их использование позволяет выиграть в долгосрочной перспективе, а потребность в передаче растущих объемов данных будет только расти. Поэтому при построении сети и закупке нового оборудования учитывать возможность внедрения ПКС на сеть компании будет достаточно предусмотрительно.

Литература

1. *Докучаев В.А., Кальфа А.А., Мытенков С.С., Шведов А.В.* Анализ технических решений по организации современных центров обработки данных // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №6. С. 16-24.
2. *Докучаев В.А., Кальфа А.А., Маклачкова В.В.* Архитектура центров обработки данных / Под ред. профессора В.А. Докучаева. М.: Горячая Линия – Телеком, 2020.
3. Александр Хвостов рассказал об опыте Ростелеком-ЦОД по внедрению и эксплуатации SDN. [Электронный ресурс] // Ростелеком – Центры обработки данных. Пресс-центр. URL: https://www.rtk-dc.ru/press/aleksandr-khvostov-rasskazal-ob-opyte-rostelekom-tsod-po-vnedreniyu-i-ekspluatatsii-sdn/ (дата обращения: 28.01.2020).
4. *Андреева М.* "Ростелеком" протестировал T-SDN. [Электронный ресурс] // Издательство ComNews. URL: https://www.comnews.ru/content/109407/2017-09-05/rostelekom-protestiroval-t-sdn (дата обращения: 28.01.2020).
5. *Устинова А.* "Ростелеком" испытал SDN-решение. [Электронный ресурс] // Издательство ComNews. URL: https://www.comnews.ru/content/114541/2018-08-21/rostelekom-ispytal-sdn-reshenie (дата обращения: 28.01.2020).
6. Аналитический отчёт компании AVANT про SD-WAN. [Электронный ресурс] // AVANT COMMUNICATIONS URL: https://goavant.net/sdwan-report (дата обращения: 02.02.2020).
7. *Деарт В.Ю., Фатхулин Т.Д.* Анализ транспортных программно-конфигурируемых сетей (T-SDN) с управляемым оптическим уровнем с целью получения модели, позволяющей оценить возможность предоставления сервиса bandwidth on demand // T-Comm: Телекоммуникации и транспорт. 2018. Том 12. №4. С. 35-42.
8. Решение T-SDN от компании Huawei. [Электронный ресурс] // DocPlayer.net URL: https://docplayer.net/19131771-Embracing-changes-becoming-open-huawei-transport-sdn-solution.html (дата обращения: 05.02.2020).
9. China Unicom Beijing и Huawei успешно развернули выделенную линию для правительства и предприятий на базе T-SDN. [Электронный ресурс] // Huawei Technologies Co., Ltd. URL: https://www.huawei.com/en/press-events/news/2018/3/Huawei-BeijingUnicom-TSDN-Private-Line (дата обращения: 05.02.2020).

10. Cranford N. Huawei, Telefónica завершают тесты T-SDN для оптической сети. [Электронный ресурс] // RCR Wireless News. URL: https://www.rcrwireless.com/20180115/huawei-telefónica-complete-t-sdn-tests-for-photonic-mesh-tag27 (дата обращения: 08.02.2020).

11. Контроллер для T-SDN от компании Netcracker. [Электронный ресурс] // Блог компании Netcracker на habr.com. URL: https://habr.com/ru/company/netcracker/blog/276643/ (дата обращения: 08.02.2020).

12. *Докучаев В.А., Ерёменко В.А., Маклачкова В.В., Мытенков С.С., Шевелёв С.В.* Профессиональные квалификации специалистов по контролю качества информационно-коммуникационных систем // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 11. С. 62-67.

13. *Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Mytenkov S.S.* Features of supporting decision making in modern enterprise infocommunication systems // T-Comm. 2019. Т. 13. № 3. С. 71-74.

SOFTWARE-DEFINED NETWORKS CONCEPT APPLICATION FOR GEOGRAPHICALLY DISTRIBUTED NETWORKS DEVELOPMENT

Nikita S. Kalmykov,
Graduate MTUCI, Moscow, Russia
nikitakalmi25@gmail.com
Vladimir A. Dokuchaev,
Head of the NIT&S Department MTUCI, Doctor of Technical Sciences (Tech), Professor, Moscow, Russsia
v.a.dokuchaev@mtuci.ru

Keywords: *transport software-defined network, T-SDN, SD-WAN, software-defined geographically distributed network, data center, on-demand bandwidth, OpenFlow.*

Due to the gradual transition of more and more applications and services to data centers, the volume of transmitted information is steadily growing and there is a need to increase the bandwidth of communication channels and reduce the cost of network operation and installation. One of these solutions is software-defined networks (SDN). In this paper, the aspects of building transport SDN are touched upon and solutions from several manufacturers are analyzed. The positive and negative aspects of software-defined geographically distributed networks (SD-WAN) were also studied.

РЕАЛИЗАЦИЯ ФУНКЦИЙ РАДИОМАЯКА В ТЕХНОЛОГИИ BLUETOOTH

Касса Александра Гилен-Анна,
магистрант МТУСИ, Москва, Россия
kassaalexandra@gmail.com
Пшеничников Анатолий Павлович,
профессор кафедры ССиСК МТУСИ, к.т.н., профессор, Москва, Россия
pshenichnikov@mtuci.ru

Ключевые слова: Bluetooth, Bluetooth с низким энергопотреблением (BLE), Bluetooth-маяк, функции радиомаяка, iBeacon, Eddystone, AltBeacon.

Представлена реализация функций радиомаяка в технологии Bluetooth. Рассмотрена архитектура технологии Bluetooth Low Energy. Приведены этапы развития технологии Bluetooth от версии 4.0 до версии 5.2. Показаны рекламные каналы, используемые маяком в диапазоне частот 2402-2480 МГц. Описаны функции и сферы применение радиомаяков Bluetooth Low Energy для получения данных об окружающей среде, микро локации и ориентации.

Технология Bluetooth с низким энергопотреблением

Технология Bluetooth с низким энергопотреблением (BLE-Bluetooth Low Energy), иногда называемая «Bluetooth Smart», представляет собой облегченное подмножество классического Bluetooth и была представлена консорциумом Bluetooth SIG (Special Interest Group) как часть основной спецификации Bluetooth 4.0. Это – беспроводная технология персональных сетей WPAN (Wireless Personal Area Network). Существует множество беспроводных протоколов, доступных для инженеров и дизайнеров продуктов, но главная особенность BLE – возможность связи с очень низким энергопотреблением. В настоящее время это, безусловно, самый простой способ разработать приложения для взаимодействия с любой современной мобильной платформой (iOS, Android, телефоны Windows и т. д.). Архитектура BLE показана на рис. 1 [1,2].

Стек BLE состоит из двух основных архитектурных компонентов: хост (ведущий) и контроллер. Каждый из которых содержит различные стек-слои.

Физический слой (PHY – Physical Layer). Передатчик использует модуляцию GFSK (Gaussian frequency shift keying) и работает в нелицензированной полосе частот 2,4 ГГц. Используя этот уровень PHY, BLE обеспечивает скорость передачи данных от 1 Мбит/с до 3 Мбит/с (Bluetooth v5.0). В нем используется приемопередатчик со скачкообразной перестройкой частоты. Указаны два варианта уровня PHY, а именно некодированные и закодированные данные. Топология дуплекса с временным разделением (TDD) используется в обоих режимах PHY.

Уровень связи (Link Layer) отвечает за рекламу, сканирование и создание/поддержание соединений. Роль устройств BLE изменяется в одноранговых и широковещательных режимах. Как правило, режим прямого тестирования (Direct Test Mode) – это часть канального Link Layer.

Интерфейс хост-контроллера (HCI – Host Controller Interface) определяет серию команд, которые хост может использовать для связи с контроллером, и события, которые контроллер использует для связи с хостом. Значительная часть интеллекта BLE реализуется контроллером. Это позволяет ведущему устройству дольше оставаться в состоянии сна и пробуждаться по сигналу контроллера.

Рис. 1. Архитектура Bluetooth LE

Протокол управления логическим каналом и адаптации (L2CAP – Logical Link Control & Adaptation Protocol) отвечает за протокол мультиплексирования, управление потоком и сегментацию, повторную сборку блоков данных.

Атрибуты протокола Attribute Protocol (ATT) – один из основных механизмов, с помощью которого приложения подключенных Bluetooth-устройств взаимодействуют друг с другом, используя PDU, определенные протоколом и процедурами в спецификациях более высокого уровня. Этот уровень позволяет устройству BLE предоставлять определенные элементы данных или атрибуты.

Менеджер по безопасности (SMP – Security Manager). Этот уровень диспетчера безопасности предоставляет методы для сопряжения устройств и распределения ключей. Он предлагает услуги для других уровней стека протоколов для безопасного подключения и обмена данными между устройствами BLE.

Общий профиль атрибутов (GATT – Generic Attribute Profile). Этот уровень представляет собой служебную структуру, которая определяет подпрограммы для использования ATT. Обмен данными между двумя устройствами BLE осуществляется с помощью этих подпрограмм. Приложения и/или профили будут напрямую использовать GATT.

Общий профиль доступа (GAP – Generic Access Profile). Этот уровень напрямую взаимодействует с прикладным уровнем и/или содержащимися в нем профилями. Он управляет обнаружением устройств и службами, связанными с подключением устройств BLE, а также поддерживает запуск функций безопасности.

Приложения. Уровень управляет обнаружением устройств и службами, связанными с подключением устройств BLE. Уровни стека протокола BLE при необходимости взаимодействуют с приложениями и профилями. Взаимодействие приложений в системе Bluetooth обеспечивается

профилями. Профиль определяет вертикальные взаимодействия между уровнями, а также одноранговые взаимодействия определенных уровней между устройствами. Все профили / приложения работают поверх уровней GAP / GATT стека протоколов BLE.

BLE - это технология беспроводной персональной сети, разработанная и поддерживаемая консорциумом Bluetooth Special Interest Group (SIG). Чтобы оценить маяки BLE, важно понимать разницу между классическим Bluetooth и Bluetooth Low Energy. Классический Bluetooth потребляет большую мощность и передает данные на большие расстояния, что подходит для гарнитур и динамиков. Bluetooth Low Energy передает меньше данных в меньшем диапазоне частот, следовательно, потребляет гораздо меньше энергии. Маяки BLE передают небольшие объемы данных через равные промежутки времени.

Развитие технологии Bluetooth насчитывает более 20 лет. Есть разные версии Bluetooth. Версия 4.0 и выше называется BLE. Последней из серии в настоящее время является версия 5.2. Основные этапы совершенствования этой технологии, начиная с версии 4.0 (табл. 1) [3].

Таблица 1

Основные этапы развития технологии Bluetooth

Версия	**Дата**	**Свойства**
4.0	2010	Режим низкого потребления энергии, шифрование.
4.1	2013	Сосуществование с мобильной беспроводной связью.
4.2	2014	Конфиденциальность уровня соединения, профиль поддержки IPv6.
5.0	2016	Скорость 1, 2 или 3 Мбит/с, низкое потребление энергии, дополнительная функция 802.11 для скорости до 24 Мбит/с, mesh-сеть.
5.1	2019	Определение точного местоположения устройства. Одно из устройств должно иметь массив из нескольких антенн.
5.2	2020	Динамическая оптимизация мощности передачи, синхронизация по времени каналов передачи.

Одним из наиболее важных аспектов Bluetooth Low Energy является передача рекламы. Объявления BLE также важны для маяков, которые стали популярными для определения местоположения объектов. Применение BLE при распространения рекламы позволяет снизить энергопотребление, ускорить соединение и повысить надежность.

Рекламная коммуникация – это когда устройство BLE отправляет пакеты всем окружающим устройствам. Затем принимающее устройство может действовать на основе этой информации или подключаться для получения дополнительной информации. В основном это то, что делают маяки: они просто передают пакеты, используя рекламные каналы 37, 38 и 39, как показано на рис. 2 [4].

Каналы 37, 38 и 39 используются только для отправки рекламных пакетов. Остальное используется для обмена данными при подключении (эта часть не является предметом нашей темы). Спектр 2,4 ГГц для Bluetooth составляет от 2402 МГц до 2480 МГц. BLE использует 40 каналов шириной 1 МГц, пронумерованных от 0 до 39.

Каналы 37, 38 и 39 распределены по спектру 2,4 ГГц. Если заблокирован только один рекламный канал, другие каналы, скорее всего, будут свободными, потому что они разделены полосой пропускания в несколько МГц. Большое расстояние между рекламными каналами помогает BLE лучше справляться с помехами от Wi-Fi, классического Bluetooth, микроволновых печей и других устройств для обеспечения успеха рекламы.

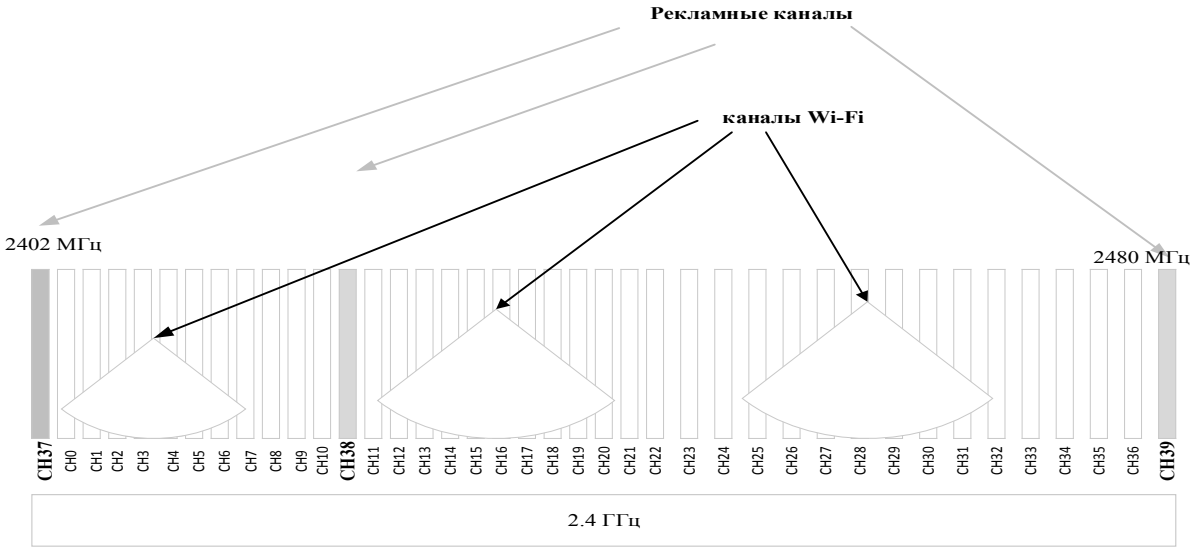


Рис. 2. Рекламные каналы 37, 38 и 39

Во время рекламы устройство BLE передает один и тот же пакет по всем трем каналам рекламы, один за другим. Центральное устройство, ищущее устройства или маяки, будет прослушивать эти каналы на предмет рекламных пакетов, что помогает ему обнаруживать близлежащие устройства.

Когда устройство BLE находится в режиме рекламы, рекламные пакеты регулярно отправляются на каждый рекламный канал. Временной интервал между набором пакетов является фиксированным со случайной задержкой. Интервал указывается между набором из 3 пакетов. Чем больше интервал между рекламными тегами, тем менее точным будет определение местоположение движущейся цели.

Принцип работы Bluetooth-маяков

Переданные данные от устройства Bluetooth с низким энергопотреблением форматируются в соответствии со спецификацией ядра Bluetooth и состоят из составляющих, показанных на рис. 3 [6].

Preambule 1 байт	Access Address 4 байта	PDU 2-39 байт	CRC 3 байта

Рис. 3. Пакет данных с низким энергопотреблением Bluetooth

Преамбула (1 байт) используется для синхронизации передатчика и приёмника. Далее следует *адрес доступа* (Access Address – 4 байта). На всех рекламных каналах он одинаков. Далее *пакет данных* (PDU) (от 2 до 39 байт). В версии 5.0 длина пакета данных увеличена до 257 байт. В конце каждого рекламного пакета следуют три байта *контрольной суммы* (CRC).

Хотя Bluetooth 5.0 известен своей большей дальностью действия и более высокой скоростью передачи данных, рекламные расширения Bluetooth v5 позволяют расширить возможности технологии. Вместо того, чтобы просто отправлять рекламные данные по всем 3 рекламным каналам (как показано на рис. 2), BLE позволяет объединять рекламные пакеты вместе и использовать остальные 37 каналов, которые ранее не передавали рекламные данные. Это используется для получения рекламных данных даже в условиях больших помех.

Bluetooth 5 также позволяет рекламному пакету содержать до 257 байт данных, что намного больше, чем 39 пакетов, которые были возможны в Bluetooth 4.0, 4.1 и 4.2 [7].

В Интернете вещей (IoT- Internet of Things) одной из задач является оценка стоимости передачи с точки зрения мощности. В зависимости от мощности передатчика устройства Bluetooth делятся на три класса:

- устройства класса 1 имеют максимальную выходную мощность 100 мВт (20 dBm) и обеспечивают дальность связи до 100 метров;
- устройства класса 2 имеют мощность до 2,5 мВт (4 dBm) и обеспечивают дальность связи до 10 метров;
- устройства класса 3 имеют мощность до 1 мВт (0 dBm) и дальность связи до 1 метра.

Устройство IoT обычно имеет ограниченное количество PDU, которые оно может отправить, прежде чем батарея достигнет точки, где он не может подключиться, пока электричество не будет восстановлено или пополнено. Предположим, что протокол iBeacon объявляется в интервале 600 мс, длина пакета составляет 34 байта, а устройство (IoT) использует аккумуляторную батарею CR2025 с номинальной емкостью 240 мА при 3 В. Электроника маяка потребляет 50 мкА при 3 В. Теперь мы можем прогнозировать срок службы маяка и эффективность передачи:

- потребляемая мощность одного маяка равна 50 мкА × 3В = 0,150 мВт;
- объём информации в байтах в секунду равен 34 × (1 с / 600 мс) × 3 канала = 170 байт / с;
- объём информации в битах в секунду равен 170 байт / с × 8 = 1360 бит / с;
- энергия на бит равна 0,150 мВт / (1360 бит / с) = 0,110 мкДж / бит;
- затраты энергии на одну рекламу равны 0,110 мкДж / бит × 34 байта × 8 бит / байт = = 29,92 мкДж / реклама;
- запасенная в батарее энергия: 240 мАч × 3 В × 3,6 с = 2592 Дж;
- срок службы батареи равен (2592 Дж × (1000000 мкДж / Дж)) / ((29,92 мкДж / ad) × (1 реклама / 0,6 с)) × 0,7 = 36385027 = 421 дней = 1,15 года.

Когда устройство Android или iOS находится в пределах досягаемости маяка Bluetooth, оно распознает сигнал, отправленный маяком, и может выполнять контекстные задачи в зависимости от того, что оно получает. Сам маяк не делает ничего, кроме передачи сигнала. Он не принимает данные с мобильного устройства. Потому что он работает в одном направлении благодаря новой спецификации Bluetooth 4.0, представленной в 2010 году [8].

Маяки Bluetooth на самом деле не являются стандартом Bluetooth SIG. Вместо этого они представляют собой то, что можно было бы назвать «псевдостандартами» или формализованными форматами для приложений радиобуев, возглавляемых крупным провайдером или группой компаний. Существует три основных рыночных стандарта для маяков: iBeacon от Apple, Eddystone от Google и AltBeacon компании Radius Networks. Все три псевдостандарта используют методологию широковещательной передачи BLE для размещения рекламных пакетов на каналах 37, 38 и 39 BLE, чтобы избежать конфликта трафика с Wi-Fi в нелицензируемом диапазоне 2,4 ГГц для промышленных, научных и медицинских (ISM) приложений. Кратко рассмотрим главные различия между ними [9].

Стандарт iBeacon. Корпорация Apple была одним из первых приверженцев технологии iBeacon в 2013 году. iBeacon определяет 30-байтовый пакет, который должен транслироваться с интервалами 100 мс. Протокол, разработанный Apple, который позволяет приложениям на смартфонах сканировать радиомаяки в определенном диапазоне и отображать контент при обнаружении. Рекомендуется, когда компании хотят проводить маркетинговые кампании Bluetooth через свои собственные приложения. Beaconstac SDK - это простой способ включить маркетинг и анализ местоположения через сеть BLE, совместимую с iBeacon.

Стандарт Eddystone разработан транснациональной корпорацией Google в 2015 году. Он способен поддерживать четыре типа пакетов, Eddystone-URL, Eddystone-UID, Eddystone-EID и Eddystone-TLM, пока iBeacon не поддерживает эти пакеты. Пакет Eddystone-UID очень похож на iBeacon от Apple, поддерживает дополнительные данные телеметрии с Eddystone-TLM.

Eddystone-URL – это единое расположение ресурсов. Этот кадр позволяет приемному устройству отображать веб-контент на основе местоположения маякового радиосигнала. Чтобы

активировать контент, приложение не нужно устанавливать. Содержимое имеет переменную длину и применяет уникальные схемы сжатия, чтобы уменьшить размер URL-адреса до предела в 17 байт**.**

Eddystone-UID – уникальный 16-байтовый идентификатор маяка с 10-байтовым пространством имен и шестибайтовым экземпляром. Использует реестр маяка Google для возврата вложений.

Eddystone-EID – короткоживущий идентификатор для маяков, требующих более высокого уровня безопасности. Нет фиксированного пространства имен и идентификатора, идентификаторы постоянно вращаются и требуют разрешенного приложения для декодирования. Использует реестр маяка Google для возврата вложений.

Eddystone-TLM – транслирует телеметрические данные о самом маяке (уровень заряда батареи, время с момента включения, количество рекламы). Широковещательные передачи наряду с URI или URL-пакетами.

Стандарт AltBeacon**.** Компания Network Radius запустила свой маяк в 2014 году. Это – маяк с открытым исходным кодом, имеющий широкий спектр открытых устройств с различными типами приложений маяков.

Все три стандарта используют механизм широковещательной передачи BLE для передачи рекламных пакетов по каналу BLE. Они используют каналы 37, 38 и 39, чтобы избежать конфликта трафика Wi-Fi.

Сферы применения Bluetooth-маяков

Для обнаружения и просмотра BLE-устройств можно использовать любой мобильный телефон с функцией Bluetooth. Одна из самых полезных служб маячков заключается в том, что их можно использовать для рекламы везде, где есть люди: в торговых центрах, магазинах, парках и даже на мероприятиях. Для его использования должно быть устройство, совместимое с маячками [5].

Маяки Bluetooth окажут преобразующее влияние на взаимодействие с физическим миром. Они обеспечивают контекстную осведомленность на основе близости, используя технологию, которая есть у большинства населения мира - смартфон с приложениями. Использование беспроводной технологии для обнаружения приближения не новость, но с появлением в 2010 году функций Bluetooth с низким энергопотреблением, маяки теперь развертываются в широком масштабе. Это – важная и значимая технология для IoT [10].

Передаваемая Bluetooth информация может быть данными об окружающей среде (температура, атмосферное давление, влажность и т. д.), данными микролокации (отслеживание активов, розничная торговля и т. д.) Или данными ориентации (ускорение, вращение и т. д.). Эти устройства используются для передачи данных с помощью сигналов Bluetooth Low Energy.

Благодаря возможности Bluetooth маяки могут определять местоположение клиентов и отправлять соответствующие сообщения на их смартфоны. Маяки безопасны в том смысле, что они разрешают доступ только к приложениям и веб-сайтам, авторизованным пользователем. Это означает, что теги передают только информацию и предоставляют помощь, которая была аутентифицирована пользователем, обеспечивая удобство работы с пользователем [11, 12].

Заключение

Внедрение Интернета вещей способствует появлению новых технологий и услуг. Одной из таких технологий является Bluetooth с низким энергопотреблением (BLE-Bluetooth Low Energy), позволяющая с использование последних достижений в области оконечных устройств сотовой мобильной связи применять BLE-маяки.

Литература

1. *Townsend, K.* Introduction to Bluetooth Low Energy [Электронный ресурс]. URL: https://learn.adafruit.com/introduction-to-bluetooth-low-energy (дата обращения: 18.11.2020).

2. *Woolley, M.* Bluetooth Core Specification Version 5.2. [Электронный ресурс]. URL: https://3pl46c46ctx02p7rzdsvsg21-wpengine.netdna-ssl.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf (дата обращения: 10.11.2020)

3. Silicon Labs BG22 Secure Bluetooth 5.2 SoC обещает 10-летний срок службы батареи [Электронный ресурс]. URL: https://cnx-software.ru/2020/01/20/silicon-labs-bg22-secure-bluetooth-5-2-soc-obeshhaet-10-letnij-srok-sluzhby-batarei/ (дата обращения: 05.11.2020).

4. BLE ADVERTISING PRIMER [Электронный ресурс]. URL: https://www.argenox.com/library/bluetooth-low-energy/ble-advertising-primer/ (дата обращения 17.11.2020).

5. Почему Bluetooth-маяк так привлекателен для маркетологов?? [Электронный ресурс]. URL: https://www.mokosmart.com/ru/bluetooth-beacon/ (дата обращения: 18.11.2020)

6. *Lindh, J.* Bluetooth low energy Beacons. [Электронный ресурс]. URL: http://file.elecfans.com/web1/M00/00/05/pIYBAFnLi6KABs7RABvYrQep_v4502.pdf (дата обращения: 20.11.2020)

7. *Ли, П.* Архитектура интернета вещей / пер. с анг. М.А. Райтмана. М.: ДМК Пресс, 2020. 454 с.

8. Что такое Bluetooth-маяки? Все, что вы должны знать [Электронный ресурс]. URL: https://ru.gadget-info.com/19060-what-are-bluetooth-beacons-everything-you-should-know (год обращения: 16.11.2020).

9. *Lance, L.* Bluetooth BLE Beacon Standards from iBeacon, Eddystone, and AltBeacon [Электронный ресурс]. URL: https://www.silabs.com/community/blog.entry.html/2016/04/25/bluetooth_ble_beacon-IGMb (дата обращения: 13.11.2020).

10. Developing Beacons with Bluetooth low energy (BLE) Technology [Электронный ресурс]. URL: http://pages.silabs.com/rs/634-SLU-379/images/Whitepaper-Developing-Beacons-with-Bluetooth-Low-Energy-Technology.pdf (дата обращения 11.11.2020).

11. What is a Bluetooth beacon? [Электронный ресурс]. URL: https://www.beaconstac.com/what-is-a-bluetooth-beacon (дата обращения 10.11. 2020).

12. Beacon Technology – What is, How does it Work and it's Uses [Электронный ресурс]. URL: https://blog.sagipl.com/beacon-technology/ (дата обращения 12.11.2020).

IMPLEMENTATION OF RADIO BEACON FUNCTIONS IN BLUETOOTH TECHNOLOGY

Kassa Alexandra Guylaine Anne,
Graduate MTUCI, Moscow, Russia
kassaalexandra@gmail.com
Pshenichnikov A.P.
Professor of the Department of CNaSS, MTUCI, PhD, Professor, Moscow, Russia
pshenichnikov@mtuci.ru

Keywords: *Bluetooth, Bluetooth low energy (ble), Bluetooth beacon, ble advertising primer, radio beacon functions, ibeacon, eddystone, altbeacon.*

The article presents the implementation of the functions of a radio beacon in Bluetooth technology. The architecture of Bluetooth Low Energy technology is considered. The stages of development of Bluetooth technology from version 4.0 to version 5.2 are given. Shown are the advertising channels used by the beacon in the frequency range 2402-2480 MHz. The functions and spheres of application of Bluetooth Low Energy radio beacons for obtaining data on the environment, micro-location and orientation are described.

ХАРАКТЕРИЗУЕТ ЛИ СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ КАЧЕСТВО УСЛУГИ ДОСТУПА В ИНТЕРНЕТ?

Магафуров Марс Рафикович,
аспирант МТУСИ, Москва, Россия
marsmag1997@yandex.ru
Ерёменко Владимир Александрович,
доцент кафедры ТЭОД МТУСИ, к.т.н., Москва, Россия
erva-2018@mail.ru

Ключевые слова: качество услуги связи, сеть Интернет, скорость передачи данных, услуги доступа в Интернет, модель четырех рынков, NGN, модель контроля качества.

Одним из объектов отраслевого нормативно-правового регулирования является «Информационно-телекоммуникационная сеть Интернет», но в законодательстве Российской Федерации отсутствует определение этого термина. Рассмотрены тенденции изменения архитектуры сервисов в современных мультисервисных сетях связи, показано место услуг связи в современной архитектуре построения информационных сервисов. На основе базовой модели контроля производительности пакетных сетей связи, использующих протокол IP, показаны возможные точки разграничения ответственности между оператором сети доступа и остальными ISP. Рассмотрены факторы, влияющие на скорость передачи данных при доступе в Интернет. Показано, что ответственность оператора сети доступа за качество услуг доступа в Интернет должна быть ограничена и устанавливаться в пределах сети связи, находящейся под управлением этого оператора.

Введение

Федеральный проект «Информационная инфраструктура», реализуемый в рамках Национальной программы «Цифровая экономика Российской Федерации», направлен на создание на основе отечественных разработок глобальной конкурентоспособной инфраструктуры передачи, инфраструктуры обработки и хранения данных, инфраструктуры функционирования цифровых платформ и экосистемы «Умный город». Реализация проекта позволит обеспечить современными услугами связи, в том числе фиксированным широкополосным доступом к сети «Интернет» (далее – ШПД), беспроводным ШПД, телефонией, IP-телевидением жителей городов, сельских малых и труднодоступных населенных пунктов. Одним из важнейших направлений проекта является подключение к сети Интернет социально значимых объектов, в том числе медицинских организаций, фельдшерско-акушерских пунктов, образовательных организаций на скорости до 100 Мбит/с в городах и до 50 Мбит/с – в сельской местности.

Скорость передачи данных при доступе в Интернет является одним из самых чувствительных для абонентов параметров услуги. Этот вопрос широко обсуждается в профессиональной среде, абонентами в социальных сетях. При этом высказываются порой прямо противоположные позиции: от «оператор связи обязан гарантировать скорость передачи данных при доступе в Интернет» до «оператор связи предоставляет услугу по принципу best effort, т.е. наилучшую из возможных при текущей загрузке сети».

Целью настоящей статьи является проведение анализа особенностей отраслевого регулирования, факторов, влияющих на скорость передачи данных в современной инфокоммуникационной среде, и определение границ ответственности оператора связи при предоставлении услуг доступа в Интернет в части скорости передачи данных.

Особенности отраслевого регулирования

Услуги доступа к информационно-телекоммуникационной сети Интернет относятся к телематическим услугам связи. Основным содержанием телематических услуг связи, как и любой другой услуги связи, является предоставление абоненту соединения для передачи информации в форме сообщений электросвязи. Сетевое соединение характеризуется двумя точками (сетевыми портами), между которыми обеспечивается передача сообщений электросвязи. При доступе в Интернет одной из таких точек является интерфейс между сетью и оборудованием пользователя, второй интерфейс очевидно должен соответствовать пограничному маршрутизатору между сетью оператора, который предоставляет услугу связи, и сетью Интернет. Для того, чтобы определить, в чем состоит ответственность оператора сети доступа перед абонентом при предоставлении данного вида услуг необходимо предельно четко понимать, что такое информационно-коммуникационная сеть Интернет и в какой точке к ней присоединена сеть оператора связи, предоставляющего абонентам услугу доступа.

Отраслевая терминология в области связи и информационных технологий установлена следующими специальными законами:

- Федеральным законом РФ «О связи» № 126-ФЗ [1], который регулирует отношения в сфере телекоммуникаций, почтовой связи и предоставления услуг связи;
- Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ [2]. Закон регулирует отношения в области информационных технологий и обеспечении информационной безопасности.

Понятие информации может иметь разные определения в зависимости от области, где оно применяется. Общим в этих определениях является то, что информация – это знания о чем-либо, сведения, воспринимаемые человеком. Для того, чтобы информацию можно было сохранить или обмениваться, она должна быть представлена в какой-то форме, доступной для непосредственного восприятия: в виде голоса, письменного текста, знака, изображения и т.п). Информация инвариантна относительно формы, в которой она представлена. Это отмечает законодатель, давая определения данного термина в Федеральном законе РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ. В целях, на которые направлен данный закон, законодатель связывает информацию с формой ее представления (сообщение, данные) как едином объекте защиты.

Согласно Федеральному закону РФ «О связи» № 126-ФЗ услугой связи является «деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений». Вместе с тем, в законе нет прямо установленного определения термина сообщение электросвязи. Косвенно содержание данного понятия можно вывести из установленного в данном законе определения «электросвязь». Под электросвязью законодатель понимает «любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам». Заметим, что по электромагнитной системе сообщения могут быть переданы только в электромагнитной форме вне зависимости от того, в какой форме была представлена информация (текст, изображение, звук и т.д). Другой важной особенностью сообщения электросвязи является наличие в электромагнитной системе дополнительной служебной информации об его адресате и отправителе. В сетях связи с коммутацией пакетов эта служебная информация включена непосредственно в сообщение электросвязи, в сетях с коммутацией каналов эта информация используется в процессе коммутации, который обеспечивает соответствие между сообщением электросвязи и используемым для его обслуживания каналом связи, а может определяться технологией, необходимой для приема сообщения электросвязи неопределенным кругом получателей – как это реализовано в системах радио и телевизионного вещания.

В качестве примера приведем определение понятия «пакет информации», установленное в Правилах оказания услуг по передаче данных: «"пакет информации" - сообщение электросвязи, которое передается по сети передачи данных и в составе которого присутствуют данные, необходимые для его коммутации узлом связи» [4]

Очевидно, что сообщение электросвязи – это специальная форма, в которую преобразуются сообщения или данные, содержащие сведения (информацию), дополненную служебными сведениями об адресате и отправителе сообщения, без которых невозможно установить взаимодействие между его отправителем и получателем. Таким образом, сообщение электросвязи – это специальная форма, необходимая для передачи информация (сведений) по электромагнитной системе. Отметим, что сообщение электросвязи всегда содержит подлежащую передаче информацию, а также служебную адресную информацию. В этой связи даже при передаче «пустого» сообщения, сам факт его передачи или факт установления соединения может быть использован для получения сведений.

Заметим, что в отраслевом регулировании широко используется понятие «информационно-телекоммуникационная сеть Интернет», однако отсутствует его определение. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» содержит лишь определение понятия «информационно-телекоммуникационная сеть», под которой законодатель понимает технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Из этого определения следует, что в такой системе передаваемым объектом является именно информация как сведения, а для доступа к информации используются средства вычислительной техники. В этом состоит ключевое отличие информационно-телекоммуникационной сети от сети связи, в которой сообщения электросвязи передаются не только как форма данных, содержащая передаваемые между пользователями сведения, но также включающую адресную информацию, необходимую для их доставки по назначению. При этом никакого использования средств вычислительной техники для доступа к передаваемой между пользователями информации не предполагается.

Изменение архитектуры сервисов в современных телекоммуникациях

Приведенные выше определения являются общими и не дают ответа на вопрос о том, что же является отличительной особенностью информационно-телекоммуникационной сети Интернет, выделяющую ее в множестве информационно-телекоммуникационных систем. Если вспомнить историю создания сети Интернет, то можно утверждать, что краеугольными научно-техническими разработками, на которых основана эта сеть явились разработанная в конце 50-х годов прошлого века концепция создания глобальных вычислительных сетей и изобретение пакетной коммутации, как способа организации доставки пакета данных между вычислительными системами, а также доменная организации сети и система доменных имен.

Коммутация пакетов лежит в основе всех протоколов, используемых в сети Интернет. Важнейшим из них является протокол IP (*IP – Internet Protocol*) для организации доставки между вычислительными системами пакетов данных сетевого уровня модели открытых систем. Особенностью процесса передачи по сети IP пакетов является отсутствие необходимости организации физического канала связи между взаимодействующими вычислительными системами. Соединение организуется на логическом уровне, а пакеты данных передаются независимо, по стохастическим маршрутам, зависящим от правил маршрутизации, текущей нагрузки и производительности узлов сети связи.

Использование сетей передачи данных с коммутацией пакетов оказало существенное влияние на архитектуру абонентских сервисов. Традиционно в сети связи общего пользования (ССОП) каждому виду абонентского сервиса соответствовала вертикально организованная сетевая служба: служба телефонии, служба передачи данных, телематические службы и т.д. На смену традиционному построению сетевых служб пришла концепция NGN (Next Generation Networks), которая предусматривала два горизонтальных уровня. На коммуникационном уровне обеспечивалось взаимодействие узлов второго, сервисного уровня. Узлами второго уровня являются вычислительные средства и информационные системы, прикладное программное обеспечение которых обеспечивает реализацию пользовательских сервисов. При этом сами информационные системы и вычислительные ресурсы могут быть реализованы как в виде физического, так и в виде виртуального решения.

На рисунке 1 показаны современные тенденции изменения архитектуры построения абонентских сервисов в современных сетях связи.

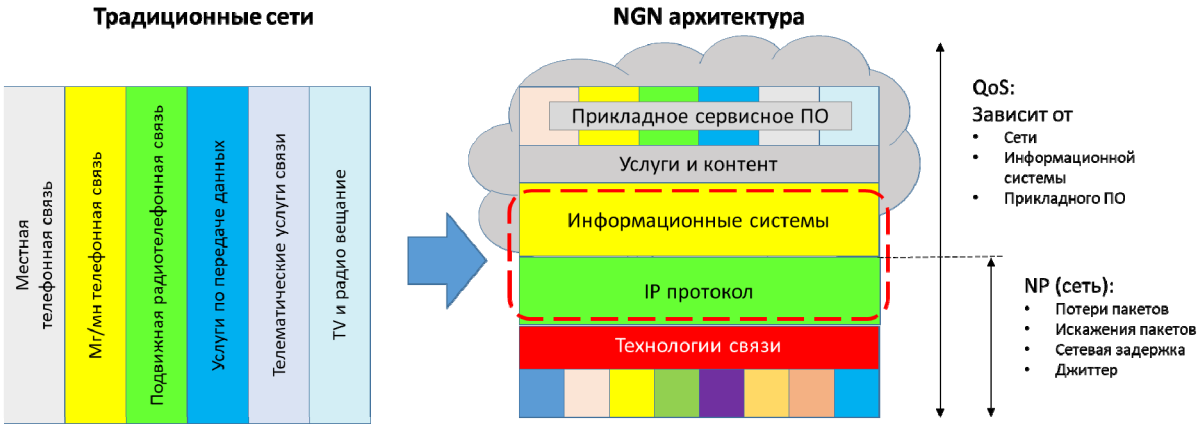


Рис. 1. Изменение архитектуры сервисов в современных сетях связи

Заметим, что взаимодействие между коммуникационным и сервисным уровнем в сетях NGN должно обеспечиваться с использованием универсального протокола, которым фактически является протокол IP, являющийся протоколом сетевого уровня. На канальном уровне могут использоваться совершенно разные протоколы, однако использование протокола IP на сетевом уровне обеспечивает телекоммуникационную среду, необходимую для обеспечения взаимодействия узлов сервисного уровня. Качество обслуживания IP сетью передаваемых пакетов информации характеризуется показателями производительности сети (Network Performance - NP), важнейшие из которых показаны на рисунке 1. Важно отметить, что и в отечественном, и в международном отраслевом техническом регулировании установлены требования к качеству обслуживания сетью передачи данных IP пакетов, и разработчики решений сервисного уровня при реализации сервисов могут учитывать потери, возникающие на коммуникационном уровне.

Пользовательские сервисы, услуги, которые потребляет пользователь создаются на информационном уровне. Это становится характерным для реализации совершенно традиционных сервисов, например – телефонии. В качества примера можно привести услугу VoLTE (Voice over LTE). Коммуникационный уровень реализован сетью передачи данных, которой является сеть LTE, а организацию соединений (сеансов связи) для передачи поверх IP пакетов голосовой информации обеспечивает платформа IMS (IP Multimedia Subsystem), которая может быть реализована в виртуальной вычислительной среде. По аналогичному принципу построены многочисленные OTT (Over The Top) сервисы. Некоторые из этих сервисов предоставляют аналогичные по потребительским свойствам услуги, телефонию, однако в Российской Федерации почему-то не отнесены к услугам связи, а деятельность операторов таких сервисов не лицензируется.

Потребительские свойства сервисов в такой архитектуре формируются логикой работы прикладного программного обеспечения, абонент непосредственно воспринимает результат обслуживания на пользовательском интерфейсе используемого им вычислительного устройства, а о качестве коммуникационного уровня может судить лишь косвенно. Если отвлечься от истории создания сети Интернет, то можно говорить, что пользователи ассоциируют Интернет скорее с работой вычислительных сетей. При доступе в Интернет пользователю совершенно недостаточно решения коммуникационной задачи, которая состоит в передаче и получении сообщений электросвязи. Ему необходим обмен информацией, а эта задача решается в вычислительной среде, на коммуникационном уровне. А за работу сервисов, реализуемых на этом уровне, отвечает оператор информационной системы, который в большинстве случаев не является оператором сети доступа, к которой подключён пользователь. С точки зрения абонента Интернет – это глобальная информационная инфраструктура, состоящая из информационных систем и информационных ресурсов, взаимодействие которых и

доступ к которым обеспечивается с использованием средств вычислительной техники по сети связи общего пользования с использованием протокола IP.

Технология передачи данных в сети не связана с тем, какая услуга будет предоставлена пользователю. Сама услуга формируется на информационном уровне, а соответствующая информационная система может быть реализована не только в виде физической архитектуры, но и в «в облаке». А средой, которая обеспечивает взаимодействие информационных систем и доступ к ним абонентом, является сеть пакетная сеть передачи данных, использующая протокол IP. Эта среда по своей сути является транспортом, обслуживающим IP пакеты, которые содержат как информацию пользователя, так и служебную информацию, в том числе адресную. IP сеть является универсальным медиатором, который не зависит от физической среды и протоколов канального уровня. Например, при предоставлении услуги VoLTE речевое сообщение передается последовательностью IP пакетов в сети с коммутацией пакетов, которой по своей сути является сеть LTE, а организация взаимодействия между абонентами и управление сеансом связи обеспечивается с помощью специальной мультисервисной информационной системы - IMS платформы.

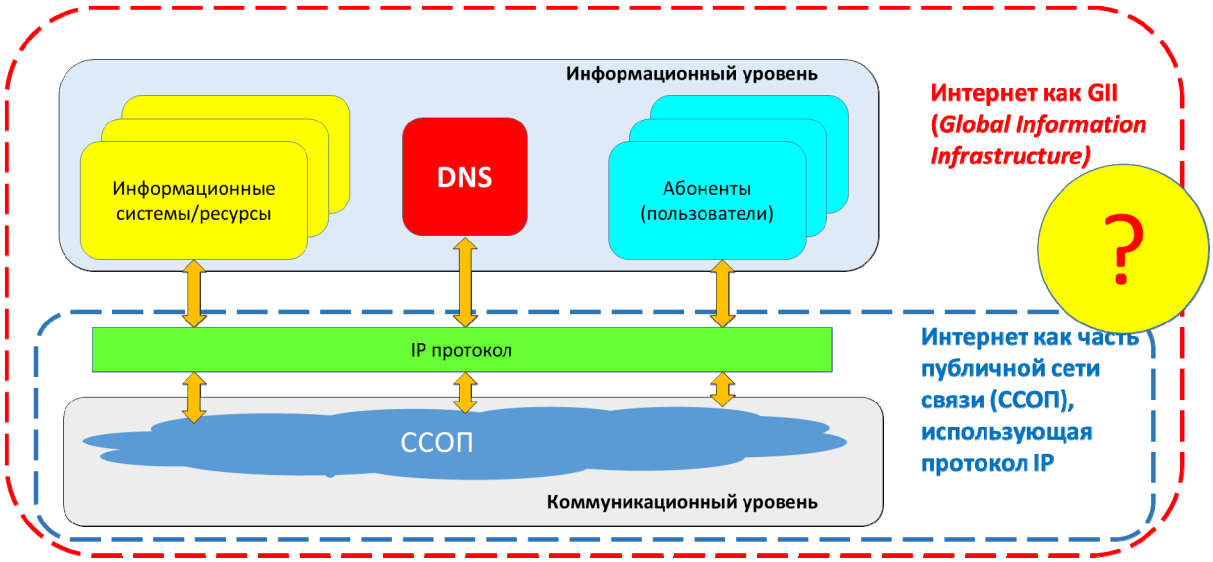


Рис. 2. Интернет и ССОП

В отсутствие четко определенного в отраслевом законодательстве определения понятия «Информационно-коммуникационная сеть Интернет» возникают совершенно разные его трактовки крайними из которых являются следующие крайние точки(рис.2):

- Интернет как часть публичной сети (ССОП), показано синим цветом; первоначально, IP-протокол для этого и разрабатывался, чтобы связать разные информационные системы.
- С другой стороны, сейчас для пользователя Интернет – это средство получения информации, то есть совокупность глобальных систем и ресурсов и справочная служба DNS, которая позволяет перевести доменные имена в IP-адреса.

В практической плоскости, при предоставлении абоненту услуги доступа в Интернет, отсутствие четкого определения данного понятия есть отсутствие установленного регулятором описания объекта, доступ к которому производиться при предоставлении данной услуги связи.

Особенности организации взаимодействия в инфокоммуникационных сетях

Для того, чтобы разобраться с тем, что же является данным объектом, рассмотрим взаимодействие информационных устройств, которые используются для доступа абонента к источнику информации, с использованием рисунка 3. Рисунок разработан на основе модели 4-х рынков, описанной в Рекомендации МСЭ-Т Е.802 [5]. В качестве информационных устройств могут быть

использованы компьютеры, вычислительные средства, смартфоны, информационные системы и ресурсы).

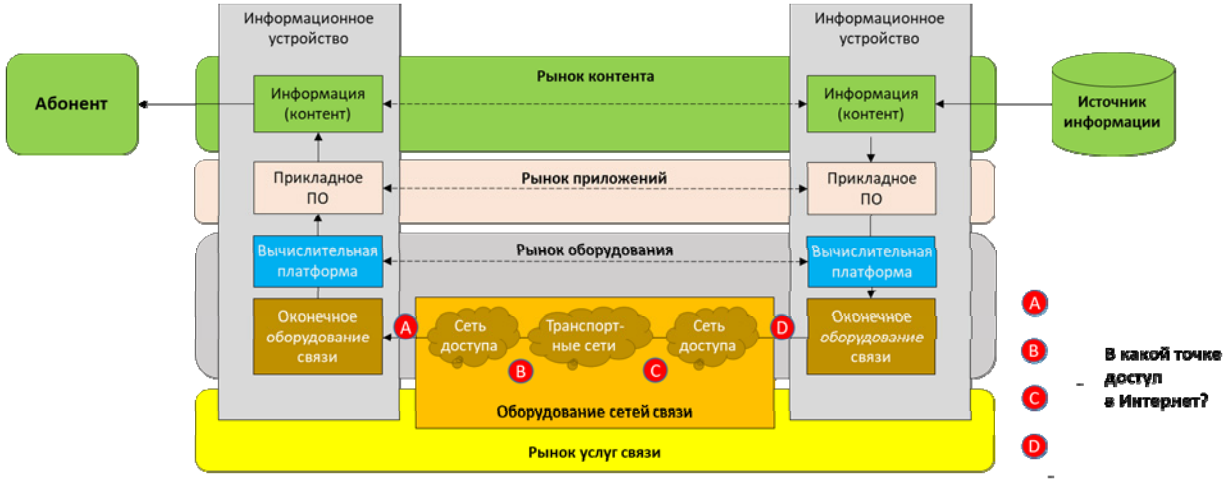


Рис. 3. Модель 4-х рынков и доступ в Интернет

Абоненту требуется информация как сведения, которая создается на рынке контента и размещается в электронной форме в виде файлов, либо формируется и преобразуется в электромагнитное сообщение непосредственно в течение сеанса связи.

Например, нам нужно получить сведения, содержащиеся в изображении, которое хранится в виде файла того или иного формата на удаленном от абонента хосте. Логическое взаимодействие информационного устройства абонента и удаленного хоста обеспечивает прикладное программное обеспечение (ПО), которое создается и распространяется на соответствующем рынке.

Прикладное ПО обеспечивает взаимодействие на уровне приложений, преобразует информации в ту или иную форму, которую удобно хранить или передавать с использованием средств электросвязи, либо, после получения, представляется в форме доступной для обработке вычислительными средствами или в форме доступной для восприятия пользователем. Прикладное Программное обеспечение, которое работает с использованием протоколов верхних уровней модели открытых систем, создается и распространяется на рынке программного обеспечения. Среда для работы прикладного ПО обеспечивается рынком оборудования, на котором создаются и распространяются вычислительные средства и соответствующие операционные среды. Оконечное оборудование связи (модем, сетевая плата и т.п) обеспечивает логическое и физическое взаимодействие информационных систем с сетью связи общего пользования (ССОП) на 1-3 уровнях модели открытых систем, а сама сеть связи обеспечивает передачу сообщений электросвязи между информационными устройствами.

Факторы, влияющие на фактическую скорость передачи данных

ССОП состоит из присоединенных и взаимодействующих друг с другом сетей связи, принадлежащим разным операторам связи. На рисунке 3 показаны точки A, B, C, D и нужно определить в какой точке обеспечивается доступ в Интернет при предоставлении соответствующей услуги связи. Абоненту должно быть предоставлено соединение от точки A, в которой предоставляется услуга доступа в интернет и в которой подключено оборудование пользователя до точки, которая находится на оборудовании информационно-телекоммуникационной сети Интернет. Здесь возможны разные варианты, которым соответствуют показанные на рисунке точки B, C и D.

Более детально рассмотрим вопрос с использование базовой модели качества (Рекомендация МСЭ-Т Y.1543[6]), показанной на рисунке 4.

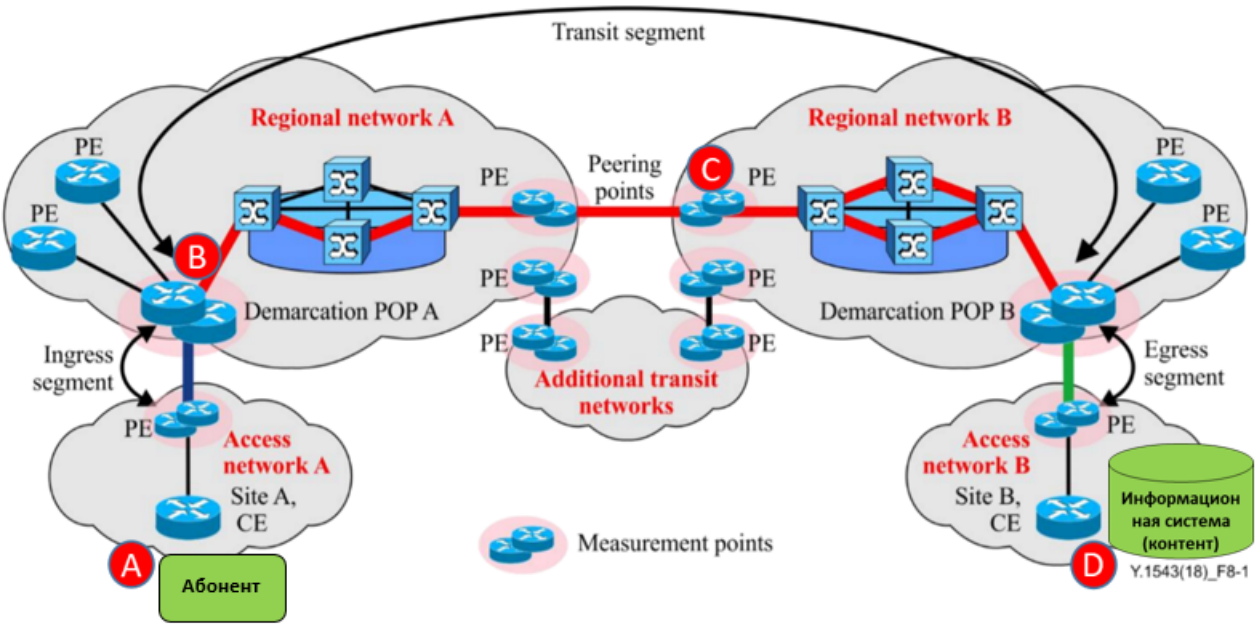


Рис. 4. Базовая модель контроля качества в IP сети

По нашему мнению, при предоставлении услуги доступа в Интернет ответственность оператора связи за качество услуги должна быть ограничена участком сквозного соединения, находящимся под его контролем. Таким участком наиболее часто является участок A-B, но для крупных операторов связи, владеющими региональными транзитными сетями – участок A-C. Если рассматривать соединение в целом (участок A-D), то здесь уместно говорить не о доступе в Интернет, а о совершенно другой услуге, о доступе к конкретной информационной системе.

В соответствии с правилами оказания телематических услуг связи[3] и Правилами оказания услуг связи по передаче данных[4] одним из показателей качества является полоса пропускания соединения, предоставляемого оператором связи. Фактическая скорость передачи данных в сквозном соединении может оказаться существенно ниже. На рисунке 5 показано влияние участков соединения между абонентом и информационной системой на полосу пропускания каждого сегмента.

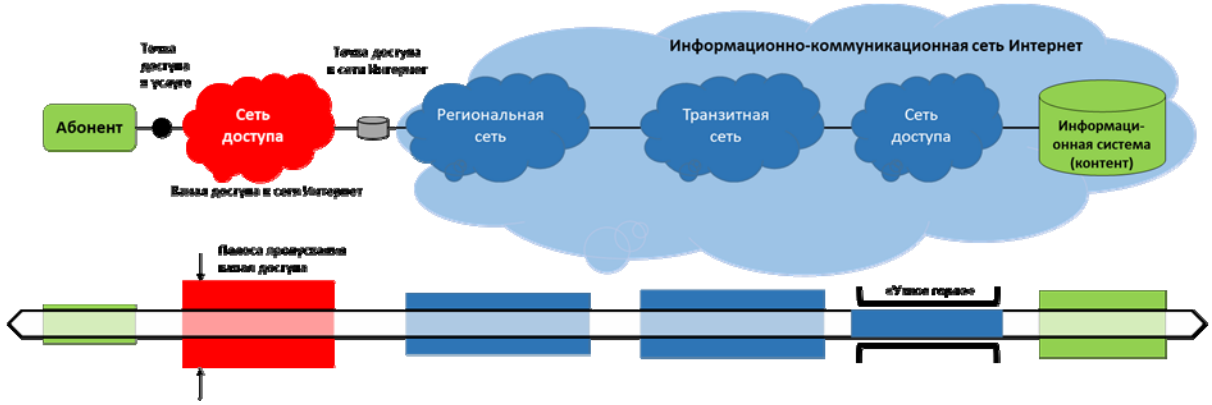


Рис. 5. Ограничение скорости передачи данных при доступе в Интернет

Скорость передачи данных в показанном на рисунке соединении будет ограничена участком сети, который имеет наименьшую пропускную способность. Полоса пропускания этого участка может быть ограничена по разным причинам, которые мы не будем рассматривать. Важно, что «узкое горло», ограничивающее полосу соединения из конца в конец может быть вне разумного контроля со стороны оператора сети доступа, а максимальная скорость передачи данных не может быть выше полосы пропускания этого «узкого горла» в соединении.

Узкое горло может создаваться оборудованием информационной системы, абонентским оборудованием или используемыми протоколами передачи данных. Также скорость передачи данных не может быть выше, чем скорость их отправки источником данных. Причины могут быть разные, в данной статье мы их более подробно не рассматриваем. Важно, что скорость передачи данных не может характеризовать качество услуги доступа в Интернет, а корректным показателем качества является полоса пропускания участка соединения из конца в конец, находящимся под контролем оператора связи, предоставляющего услугу доступа.

Заключение

- В отечественном регулировании нет явного определения информационно-телекоммуникационной сети Интернет и ее соотношения с ССОП. Точка, в которую должен быть обеспечен доступ при предоставлении услуги доступа в Интернет – не определена.
- Скорость передачи данных в E2E соединении ограничена полосой пропускания сегмента сети, имеющего наименьшую полосу.
- Скорость передачи данных при доступе в Интернет может быть ограничена быстродействием источника данных, производительностью оборудования хостов, используемых приложений и свойствами протоколов.
- Ответственность оператора, предоставляющего доступ в сеть Интернет, должна быть ограничена полосой пропускания соединения в пределах сети связи, находящейся под управлением этого оператора.

Литература

1. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 15.10.2020) "О связи".
2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) "Об информации, информационных технологиях и о защите информации".
3. Постановление Правительства РФ от 10.09.2007 N 575 (ред. от 25.10.2017) "Об утверждении Правил оказания телематических услуг связи".
4. Постановление Правительства РФ от 23.01.2006 N 32 (ред. от 25.10.2017) "Об утверждении Правил оказания услуг связи по передаче данных".
5. Рекомендация МСЭ-Т E.802 Принципы и методики определения и применения параметров QoS.
6. Рекомендация МСЭ-Т Y.1543. Измерения в сетях интернет-протокола для оценки эффективности внутри домена.

DOES THE SPEED OF DATA TRANSMISSION CHARACTERIZE THE QUALITY OF THE DATA INTERNET ACCESS SERVICES?

Mars R. Magafurov,
Post-graduate MTUCI, Moscow, Russia
marsmag1997@yandex.ru
Vladimir A. Eremenko,
Associate professor of ToEDE Department MTUCI, PhD., Moscow, Russia
erva-2018@mail.ru

Keywords: *quality of communication service, Internet, speed of data transmission, Internet access services, four market model, NGN, quality control model.*

One of the objects of the sectoral regulatory framework is the «Internet Information and Telecommunications Network», but there is no definition of this term in the legislation of the Russian Federation. The trends of changing service architecture in modern multi-service communication networks are discussed, the place of communication services in modern architecture of information services construction is shown. Based on the basic performance control model of packet networks using the IP protocol, possible points of liability delimitation between the network operator and the rest of the ISP are shown. Factors influencing the speed of data transmission during access to the Internet are considered. It has been shown that the responsibility of the access network operator for the quality of Internet access services should be limited and set within the network managed by that operator.

КОРРЕЛЯЦИЯ АТРИБУТОВ СОГЛАШЕНИЯ ОБ УРОВНЕ ОБСЛУЖИВАНИЯ С ОСНОВНЫМИ ПАРАМЕТРАМИ QoS В КОРПОРАТИВНЫХ СЕТЯХ

Назаров Мирзохусейн Джамшедович,
магистрант МТУСИ, Москва, Россия
mirzohuseyn@mail.ru
Шведов Андрей Вячеславович,
старший преподаватель кафедры СИТиС МТУСИ Москва, Россия
a.v.shvedov@mtuci.ru

Ключевые слова: *качество обслуживания, соглашение об уровне обслуживания, корпоративная сеть, мультисервисная сеть, телекоммуникационная услуга,* QoS*, Quality of Service, SLA, Service Level Agreement.*

Представлены критерии качества обслуживания (Quality of Service – QoS), рассматриваемые с точки зрения конечного пользователя и сети в целом. Рассматриваются соглашение об уровне обслуживания (Service Level Agreement – SLA) как инструмент для управления параметрами качества обслуживания, который документирует его фиксированные критерии, пороговые значения, обязательства и компенсации, а также корреляция атрибутов соглашения об уровне обслуживания с основными параметрами качества обслуживания, в частности, определяются основные вопросы и проблемы определения и управления SLA. В работе представлен краткий обзор качества обслуживания с особым акцентом на выявление соответствующих параметров QoS, а также представлены стандартизированные определения и цели соглашения об уровне обслуживания в качестве инструмента управления QoS.

Введение

Сегодня, формирование новых технологических концепций информационно-коммуникационных технологий приводит к постоянному возрастанию количества подключаемых устройств и, как следствие, к постоянному возрастанию объемов передаваемой информации по всем типам сетей связи. К числу подобных концепций относится IoT [1]. Согласно определению Международного Союза Электросвязи (МСЭ) IoT – это глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом объектов (физических и виртуальных) на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий. В концепции IoT ИКТ, которые уже обеспечивают возможность организации связи "в любое время" и «в любом месте», получают новый аспект – "связь с любой вещью" [2]. Сюда же можно отнести технологии облачных вычислений (Cloud Computing) и граничных вычислений (Edge Computing), концепции программно-конфигурируемых сетей (SDN) и виртуализации сетевых функций (NFV). Планирование сети и управление трафиком при этом проходит путем программирования [3]. Таким образом, введение новых услуг на сети упрощается и ускоряется [3].

Качество обслуживания (Quality of Service – QoS) может интерпретироваться как способность пользователя конкретного приложения получать услугу с предсказуемой производительностью в течение некоторого разумного периода времени, который позволяет приложению работать приемлемым образом. В корпоративных мультисервисных сетях управление ресурсами осуществляется на основе так называемых соглашений об уровне обслуживания (SLA). SLA - это документально подтвержденный результат согласования между заказчиком и поставщиком услуг или между самими поставщиками услуг, который определяет уровни доступности, удобства обслуживания, производительности, работы или других атрибутов услуги. Соглашения об уровне обслуживания могут

помочь клиентам использовать новые технологии и сервисы, поскольку они предоставляют поставщику услуг обязательство гарантировать определенный уровень производительности.

Механизмы QoS позволяют улучшить производительность и эффективность сетей связи, снизить нагрузку на узлы во время прохождения через них большого количества пакетов и минимизировать задержки трафика. В целом можно сказать, что для выполнения поставленных перед ними задач корпоративным сетям связи, в том числе построенным на базе или с использованием новых технологических концепций, использование механизмов и инструментов QoS является одним из самых главных условий [4,5].

Структура качества обслуживания

На основании рекомендации МСЭ Е.800 качество обслуживания (QoS) определяется как совокупный эффект производительности обслуживания, который определяет степень удовлетворенности пользователя услуги [6].

Критерии качества обслуживания можно рассматривать с разных точек зрения:

- требования QoS клиента;
- предложения QoS для провайдера услуг (запланированное/целевое QoS);
- Степень достижимости QoS;
- опросы клиентов по рейтингам качества обслуживания.

Комбинация взаимосвязей между этими четырьмя точками зрения формирует основы практического и эффективного управления качеством обслуживания. Параметры качества обслуживания характеризуют уровень качества определенного аспекта предлагаемой услуги и, в конечном итоге, удовлетворенность потребителя этой услуги. Параметры QoS представляют субъективное и абстрактное воспринимаемое пользователем «качество» в виде числовых (количественных) значений. Первоначально термин QoS использовался главным образом для определения набора характеристик производительности сети, таких как задержка, джиттер, частота ошибок по битам или потеря пакетов. С внедрением и развитием мультимедийных услуг, предоставляемых через сеть Интернет, концепция QoS стала охватывать уже не только саму сеть, но и конечные системы. На рис. 1 показан обобщенный вид общих элементов архитектуры для поддержки сквозного качества обслуживания, состоящего из уровней пользователя, приложения и системы [7].

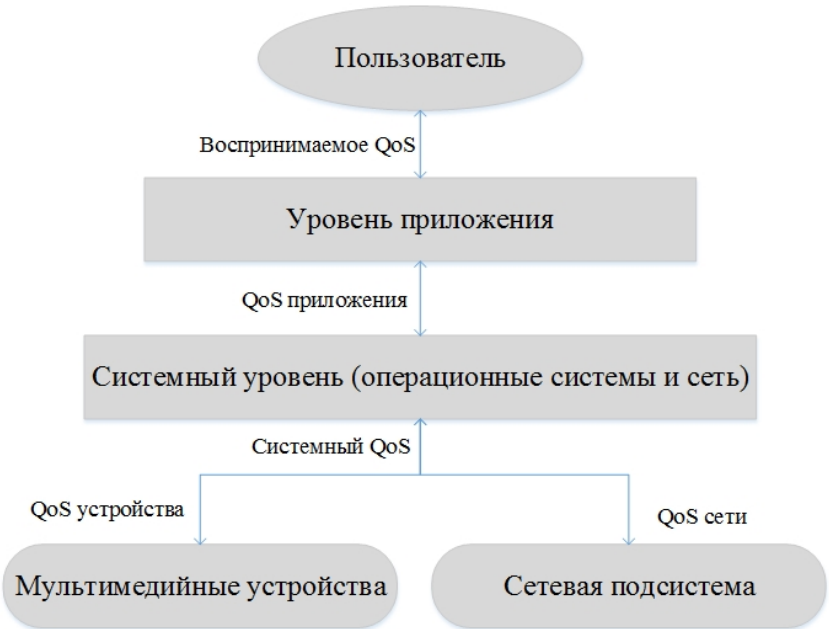


Рис. 1. Структура сквозного QoS

На каждом из уровней вышеуказанной архитектуры необходимо указать параметры QoS для уровня, располагающегося ниже. Указанные пользователем параметры QoS должны быть переведены в параметры, специфичные для этого уровня, и затем нижележащие уровни должны обеспечить соответствие ожиданиям QoS.

Пользователи мультимедийных приложений принимают окончательное решение о качестве услуги, основываясь на своем субъективном восприятии. Параметры восприятия пользователя должны быть сопоставлены с технологическими параметрами более низкого уровня.

Параметры QoS приложения, описывающие требования к прикладным услугам, как правило, включают в себя качество мультимедийного контента, требования к задержке, межпотоковую и внутрипотоковую синхронизацию и прочее. Параметры QoS приложения должны отображаться в параметры QoS системного уровня.

Параметры QoS системного уровня описывают требования к системе связи и операционной системе, формирующиеся из QoS приложения. Уровень QoS устройства определяет, в частности, параметры синхронизации и пропускной способности.

Некоторые примеры параметров QoS сетевого уровня приведены ниже:

- сквозная задержка;
- джиттер;
- скорость передачи данных (необходимая или доступная пропускная способность);
- среднее время до отказа;
- среднее время восстановления;
- среднее время между отказами;
- доступность;
- коэффициент потери пакетов (доля от общего числа пакетов, которые не были доставлены из-за перегрузки сети);
- коэффициент ошибок по пакетам.

Параметры QoS могут использоваться поставщиками услуг для управления и улучшения качества предоставляемых ими услуг, а также клиентами (конечными пользователями или поставщиками-партнерами), чтобы гарантировать, что они получают уровень качества, за который они платят. Эти параметры используются для поддержки разработки и проверки соглашений об уровне обслуживания (SLA).

Методы контроля качества обслуживания

Качество обслуживания зависит от и оценивается на основе статистических характеристик трафика. Чтобы максимизировать использование сетевых ресурсов (например, полосы пропускания и буфера) и в то же время удовлетворить требованиям QoS отдельного пользователя, необходима разработка специальных механизмов управления параметрами качества обслуживания для приоритезации доступа к ресурсам на узлах сети. Например, системы массового обслуживания в реальном времени являются ядром любой реализации метода контролируемого QoS для сетевых служб. Предоставление единого класса услуг контролируемого QoS требует скоординированного управления доступом к сети, планирования потоков трафика, а также управления буфером. Другие методы включают управление потоком трафика и перегрузкой в сети. Контроль доступа ограничивает нагрузку на систему очередей, определяя, может ли входящий запрос на новую услугу приниматься без нарушения гарантий обслуживания для уже действующих потоков трафика. Процесс допуска основан на спецификации QoS, а пороговые значения включают такие параметры, как минимальная полоса пропускания и объем буфера.

Соглашение об уровне обслуживания (SLA)

Соглашение об уровне обслуживания (Service Level Agreement – SLA) — это официальное соглашение между двумя или более субъектами, которое достигается после согласования их действий

с целью оценки характеристик обслуживания, обязанностей и приоритетов каждой из сторон [8]. SLA может включать данные о производительности, условиях тарификации и выставления счетов, предоставлении услуг и компенсации. Соглашение об уровне обслуживания может включать в себя правила согласования трафика, которые составляют соглашение о регулировании трафика.

Как правило, SLA заключается между пользователем и поставщиком услуг. Такое соглашение называется SLA пользователя (или SLA внутри домена). Чтобы гарантировать сквозную производительность в нескольких доменах, также должны существовать соглашения ISP-SLA, заключенные между поставщиками услуг (рис. 2). SLA может быть статическим или динамическим. Статические SLA согласовываются на регулярной (например, еженедельной или ежемесячной) основе. При использовании динамического SLA услуги должны запрашиваться по требованию с использованием протокола сигнализации. Часть SLA, которая относится к QoS, называется соглашением QoS, основанным на рекомендации МСЭ E.860, и включает в себя программу, согласованную двумя организациями, в отношении мониторинга, измерения и определения параметров QoS.

Определение параметров QoS является важным этапом в разработке SLA и, в частности, соглашения QoS. Очевидно, что гарантированный уровень обслуживания зависит от многих факторов и может быть различным у разных пользователей. Некоторые традиционно типичные объекты соглашения – это доступность сети, средняя задержка сети, эффективная пропускная способность, время восстановления услуг и методы выставления счетов.

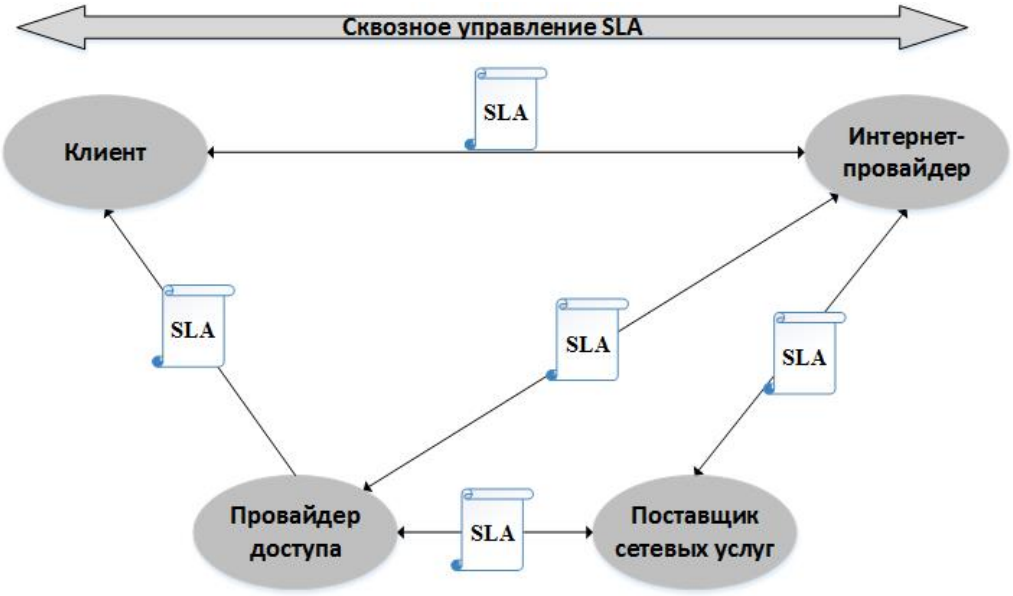


Рис. 2. Сквозное управление SLA

Стоит обратить внимание, что соответствующие параметры SLA зависят от различных транспортных технологий. Точно определенное соглашение QoS дает следующие преимущества:

- Гарантия QoS: пользователь точно знает, какую гарантию QoS он получит;
- Мониторинг качества: пользователь и сеть могут контролировать качество услуги на основе набора заранее определенных параметров QoS;
- Биллинг: дифференциальный сбор информации об использовании телекоммуникационных услуг, их тарификация, выставление счетов абонентам, обработка платежей может быть реализована на основе значений параметров QoS, указанных в соглашении QoS. Например, сумма за контракт с более строгими пределами задержки может взиматься выше, чем в случае, когда допускаются менее строгие пределы.

Структура SLA

Общая структура SLA на основе рекомендации МСЭ Е.860 приведена на рис. 3, иллюстрирующим, что SLA относится ко всем сервисам, которыми обмениваются два объекта (мультисервисный SLA), и состоит из одной общей части и специфических частей, относящихся к другим услугам. Краткое описание каждого поля этой структуры приведено ниже.

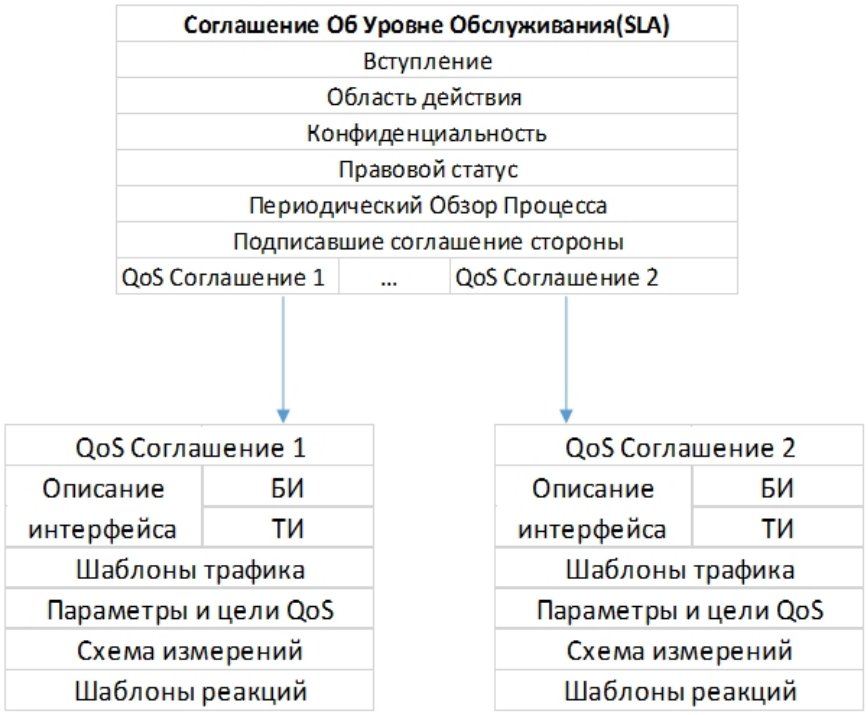


Рис. 3. Общая структура SLA

Поле вступление описывает цель SLA. Оно может включать определение уровней обслуживания, которые необходимо гарантировать, помощь двух объектов (пользователя, поставщика услуг, сетевого поставщика) в обмене информацией с подходящими параметрами QoS и производительностью сети или предоставление базовых понятий, измерений и параметров для реализации соглашения. Область действия описывает услуги и их целевую производительность. Конфиденциальность определяет режим соглашения и обмен информацией между вовлеченными сторонами. Периодический обзор процесса проверки определяет частоту (например, ежедневную, ежемесячную, полугодовую) и формат (бумажный, электронный) для обмена информацией, относящейся к QoS. Подпись сторон подтверждает взятые ими обязательства.

Соглашение о качестве обслуживания (QoS)

Соглашение о качестве обслуживания является логической границей между двумя объектами и состоит из группы точек взаимодействия – интерфейсов. В зависимости от типа обмениваемой информации, описание интерфейса классифицируется как бизнес-интерфейс (БИ) или технический интерфейс (ТИ). Бизнес-интерфейс состоит из точек взаимодействия, расположенных между пользователем и поставщиком услуг, которые используются для конкретных параметров соглашения QoS, а также формирования отчетов о производительности и шаблонов реагирования, которые используются, когда не обеспечивается согласованный уровень QoS. Точки взаимодействия с техническим интерфейсом служат для обмена информацией, специфичной для службы, и позволяют проводить измерения, исходя из которых определяются параметры QoS.

Для правильного управления ресурсами каждый объект должен знать характеристики трафика, который он получает от других объектов, а также условия (пороги), которые позволяют активировать шаблоны реакции от принимающего объекта.

Для определения индивидуальных параметров QoS, применяемых при взаимодействии двух объектов можно обратиться к рекомендации МСЭ E.801, где учитываются как потребительские, так и сетевые параметры [9]. Классификация параметров на сервис-зависимые и сервис-независимые позволяет получить общее определение независимых параметров для всех сервисов, как показано на рис. 4.

Рис. 4. Классификация параметров QoS

Вопросы управления SLA

Управление SLA должно обеспечивать средства и инструменты для надежного предоставления услуг, мониторинга выполнения SLA во время использования услуг, а также прогнозирования и реагирования в случае деградации производительности [10]. Первая трудность для поставщиков услуг заключается в том, что они в основном имеют дело с различными сетевыми технологиями и элементами, которые часто предоставляются разными поставщиками услуг. Кроме того, поставщик услуг должен обеспечить сквозную систему управления уровнем обслуживания, которая может точно и детализировано измерять производительность сети.

Основные части управленческой цепочки SLA включают определение содержания соглашения QoS и переговорного процесса, а также часть выполнения и гарантии SLA.

Заключение

Таким образом, SLA — это документально подтвержденный результат переговоров между клиентом и поставщиком услуг, который определяет характеристики, обязанности и приоритеты каждой стороны. Соглашение об уровне обслуживания может включать условия тарификации и выставления счетов, предоставления услуг и компенсации. А структура и содержание SLA — это вопросы, которые в настоящее время стандартизированы различными органами стандартизации, в то время как другие аспекты, включая правовой статус или выставление счетов / тарификацию, все еще остаются открытыми. В настоящее время некоторые аспекты SLA, такие как определение конкретных параметров, область применения или процедуры управления все еще обсуждаются профессиональным сообществом или находятся в процессе стандартизации. Надлежащий контроль доступа к ресурсам и управление распределением ресурсов являются основными проблемами для выполнения SLA. Чтобы гарантировать, что воспринимаемое качество соответствует ожидаемому, показатели QoS должны контролироваться и измеряться.

Литература

1. *Докучаев В.А., Ермалович А.В., Шведов А.В.* Концепция «Интернет Вещей» как основа развития информационно-коммуникационных технологий (ИКТ) // Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XV международная научно-практической конференции. Симферополь-Гурзуф, 17-19 ноября 2016 год. Саки: ИП Бровко А.А., 2016. С. 298.
2. *Гадасин Д.В., Шведов А.В., Ермалович А.В.* Концепция "туманные вычисления" – эволюционный этап развития инфокоммуникационных технологий // Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции «Технологии информационного общества». (14-15 марта 2018 г. Москва, МТУСИ). М.: ИД Медиа Паблишер, 2018. С. 96-99.
3. *Докучаев В.А., Кальфа А.А., Мытенков С.С., Шведов А.В.* Анализ технических решений по организации современных центров обработки данных // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №6. С. 16-24.
4. *Шведов А.В*., *Назаров М.Д.* Зависимость показателей эффективности функционирования корпоративных сетей связи от показателей качества обслуживания (Qos) // Технологии информационного общества. Сборник трудов XIV Международной отраслевой научно-технической конференции «Технологии информационного общества». (18-19 марта 2020 г. Москва, МТУСИ). М.: ИД Медиа Паблишер, 2020. С. 302-304.
5. *Григорьев И.Д., Орлов В.Г.* Методы контроля качества обслуживания в мобильных самоорганизующихся сетях // Фундаментальные проблемы радиоэлектронного приборостроения.- 2015. Т. 15. № 5. С. 292-296.
6. ITU-T Recommendation E.800, Definitions of terms related to quality of service, 1994.
7. *Nahrstedt K., Steinmetz R.* Resource management in networked multimedia systems. IEEE Comp. 28 (5), 1995. P. 52-63.
8. ITU-T Recommendation E.860, Framework of a service level agreement, 2002.
9. ITU-T Recommendation E.801, Framework for Service Quality Agreement, 1996.
10. *Marilly E., Martinot O., Betge-Brezetez S., Delegue G.* Requirements for service level agreement management. In: Proc. of IEEE Workshop on IP-Operations and Management (IPQM 2002). Dallas, Texas, pp. 57-62. 2002.

CORRELATION OF SERVICE LEVEL AGREEMENT (SLA) ATTRIBUTES WITH KEY QOS PARAMETERS IN CORPORATE NETWORKS

Mirzohuseyn J. Nazarov,
Graduate MTUCI, Moscow, Russia
mirzohuseyn@mail.ru
Andrey V. Shvedov,
Senior lecturer of NITaS Department MTUCI, Moscow, Russia
a.v.shvedov@mtuci.ru

Keywords: *quality of Service, QoS, Service Level Agreement, SLA, corporate network, multiservice network, telecommunication service.*

This paper presents the quality of service (QoS) criteria considered from the point of view of the end user and the network as a whole. The service level agreement is considered as a tool for managing QoS parameters, which documents fixed QoS criteria, thresholds, obligations and compensation, and some aspects of service quality, as well as the correlation of service level agreement (SLA) attributes with the main QoS parameters.in particular, the main issues and problems of defining and managing SLA are identified. This paper provides a brief overview of the quality of service with a particular focus on identifying relevant QoS parameters, and provides standardized definitions and goals of the service level agreement as a QoS management tool.

АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРОЦЕССОРА 1892ВМ14Я С ЦЕЛЬЮ ПРИМЕНЕНИЯ В ИНФОКОММУНИКАЦИОННЫХ ПРИЛОЖЕНИЯХ

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

Ключевые слова: сигнальный процессор, микропроцессор, система на кристалле, защита информации, импортозамещение, инфокоммуникационые приложения, инфокоммуникации, прерывания, архитектура, 1892ВМ14Я, Мультиком-02, MCStudio 4, ЭЛВИС.

Анализируется возможность импортозамещения в инфокоммуникационных приложениях на примере системы на кристалле 1892ВМ14Я — «Мультиком-02» (*MCom*-02) производства АО НПЦ «ЭЛВИС». Выделены факторы, оказывающие существенное влияние на применение сигнальных процессоров в инфокоммуникациях. Проведен анализ функциональных и архитектурных особенностей системы на кристалле 1892ВМ14Я. На примере базовой криптографической операции разработано программное обеспечение для сигнального процессора *ADSP*-2181 и системы на кристалле 1892ВМ14Я. Сравнительный анализ технических характеристик и разработанного программного обеспечения позволил выявить предпосылки для внедрения микропроцессорных решений на базе 1892ВМ14Я в различные сферы инфокоммуникаций и замены зарубежной элементной базы на отечественные аналоги при обучении специалистов по профессиональным образовательным программам.

Постановка задачи

На современном этапе, с учетом экономических ограничений и требований к защищенности средств связи от несанкционированного доступа, разработчики микропроцессорных устройств для инфокоммуникационных приложений должны ориентироваться на применение отечественных микропроцессоров.

В рамках профессиональных образовательных программ по направлению «Инфокоммуникационные технологии и системы связи» в ФГБОУ ВО «Московский технический университет связи и информатики» (МТУСИ) на кафедре «Многоканальные телекоммуникационные системы» (МТС) студенты приобретают навыки разработки микропроцессорных устройств. Курсовые и выпускные проектные решения микропроцессорных средств связи реализованы на базе сигнального микропроцессора семейства *ADSP*-21*xx* американской фирмы *Analog Devices*. Однако в современных условиях основной стратегией стало проведение импортозамещения – замены зарубежной элементной базы на отечественные аналоги.

Для реализации инфокоммуникационных приложений необходима обработка сигналов в реальном времени. К областям применения сигнальных процессоров в инфокоммуникациях относятся криптографическая обработка информации, цифровая адаптивная фильтрация, эхокомпенсация, генерация ключевых последовательностей, обнаружение и обработка навигационных сигналов и пр. Типовыми задачами по цифровой обработке сигналов являются цифровая фильтрация, преобразования Фурье и криптографические операции в полях Галуа.

Обзор микропроцессорных устройств позволил определить факторы, оказывающие существенное влияние на применение сигнальных процессоров в инфокоммуникационных приложениях [1,6]:

- обработка сигналов в реальном времени;

- неограниченность в выборе решаемых задач;

- возможность модернизации программного обеспечения микропроцессорных устройств.

Специализированные микропроцессоры и программируемые логические интегральные схемы (ПЛИС) ограничены строгими рамками выполнения определенного типа задач, поэтому при разработке телекоммуникационных решений приоритет отдается сигнальным процессорам. Это существенно расширяет спектр научных исследований, разработки и внедрения перспективных телекоммуникационных приложений. [2]

Основными методическими предпосылками при выборе сигнального процессора для профессионального образования по направлению подготовки «Инфокоммуникационные технологии и системы связи» являются [3]:

- архитектура, специально ориентированная на цифровую фильтрацию;

- интуитивно понятный язык и система команд, не требующая изучения и запоминания большого количества аббревиатур команд процессора и позволяющая студентам сосредоточить усилия на процессе обработки информации;

- удобный набор отладочных средств, включая отладочную плату, на базе которого могут быть реализованы макеты и опытные образцы микропроцессорных устройств;

- простота дальнейшей реализации готовых изделий вплоть до серийного выпуска за счет отсутствия специальных требований к трассировке печатных плат, поскольку все скоростные цепи сосредоточены внутри процессора.

К важным условиям обеспечения защиты информации в телекоммуникационных приложениях относится система прерываний сигнального процессора, свободная от незадокументированных функций, т. е. действий, не отраженных в техническом описании процессора. Следует учитывать тот факт, что иностранные компании-изготовители обычно включают в работу процессора особые прерывания для нужд технического обслуживания и проведения различных тестирований, так называемые «закладки». При этом злоумышленники, воспользовавшись такой возможностью, могут получить несанкционированный доступ к информации, в том числе имеющей гриф секретности. Поэтому наличие полного контроля над всеми прерываниями – одно из важных условий реализации телекоммуникационных приложений.

Основными задачами исследования являются:

1) анализ архитектурных и функциональных возможностей системы на кристалле (*SoC – System-on-a-Chip*) 1892ВМ14Я;

2) проведение сравнения технических характеристик системы на кристалле 1892ВМ14Я с характеристиками сигнального процессора *ADSP*-2181;

3) реализация базовой операции криптографии на системе на кристалле 1892ВМ14Я и на сигнальном процессоре *ADSP*-2181, сравнение результатов;

4) оценка эффективности применения системы на кристалле 1892ВМ14Я в инфокоммуникационных приложениях.

Система на кристалле 1892ВМ14Я – «Мультиком-02»

В качестве одного из возможных решений, в статье рассмотрена отечественная система на кристалле 1892ВМ14Я – «Мультиком-02» (*MCom*-02) производства АО НПЦ «ЭЛВИС».

Следует учитывать, что помимо АО НПЦ «ЭЛВИС», в разработке микропроцессоров по своей, либо зарубежной топологии с модификациями, принимает участие множество компаний, такие как «Байкал Электроникс» с изделием «Байкал-Т1», или широко известный «Эльбрус-1С+» и не столь широко – «КВАРК» [1]. Выбранный в докладе микропроцессор 1892ВМ14Я – лишь один из вариантов отечественной микроэлектроники.

Система на кристалле «Мультиком-02» использует сдвоенное 32-битное *CPU*-ядро (от англ. *Central Processing Unit* – центральное обрабатывающее устройство) *ARMCortex-A*9 *MPCore* [4]. Схема системы на кристалле 1892ВМ14Я приведена на рисунке 1. В области инфокоммуникаций это ядро

представляет интерес с точки зрения контроля и управления процессами в ядрах *DSP* (от англ. *Digital Signal Processor* – цифровой процессор обработки сигналов) *Elcore*-30*M*. Процессорное ядро *Cortex-A*9 отличается высокой производительностью в условиях ограниченной мощности. Может использоваться не только как традиционный одноядерный процессор, но и в качестве наращиваемого многоядерного процессора *Cortex-A*9 *MPCore* [4].

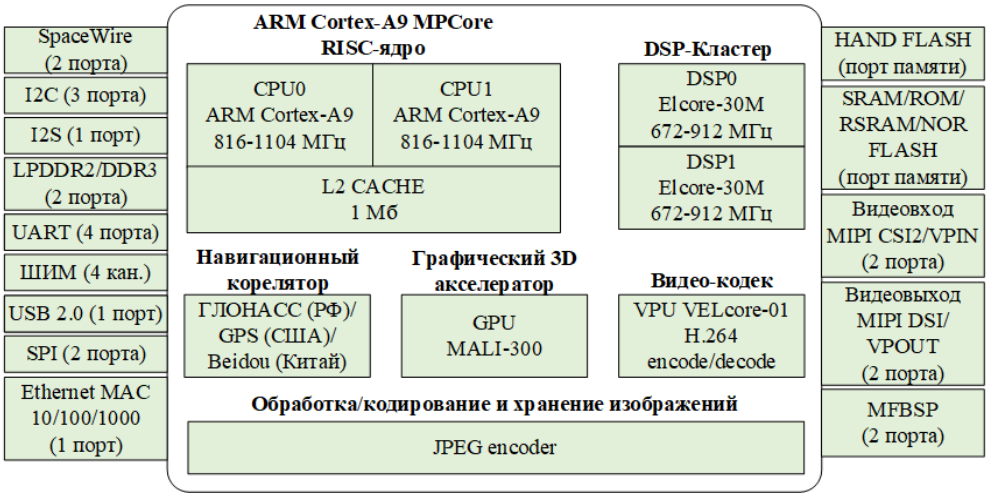


Рис. 1. Схема системы на кристалле 1892ВМ14Я

DSP-ядра *Elcore*-30*M* – одна из составных частей *DSP*-кластера *Elcore*-30*M*, которая является основным элементом сопроцессора-акселератора сигнальной обработки. *DSP*-кластер выполняет 8, 16, 32 и 64-битные операции с плавающей и фиксированной точкой, а наличие двух *DSP*-ядер дает возможность производить параллельные вычисления, данные результатов которых передаются в *CPU*, где впоследствии обрабатываются.

Архитектурные возможности системы на кристалле 1892ВМ14Я позволяют реализовать параллельную и независимую обработку данных, при этом *DSP*-ядра так же могут обмениваться информацией не только с *RISC*-ядром (от англ. *Reduced Instruction Set Computer* – компьютер с набором простых команд), но и между собой. Таким образом, наибольший интерес в телекоммуникациях представляют именно *DSP*-ядра для реализации базовых вычислительных операций. *RISC*-ядро использует результаты работы *DSP*-ядер в основных вычислениях.

Система на кристалле 1892ВМ14Я имеет различные режимы работы. Под такими режимами понимаются условия окружающей среды и значение напряжения питания ядер. Процессор может работать и в критических условиях эксплуатации, однако при этом скорость обработки информации существенно падает. В нормальных условиях эксплуатации 1892ВМ14Я, на ядра можно подать напряжение 1,2 В и добиться повышения производительности. Наличие подобных режимов работы и низкое энергопотребление позволяют реализовать решение поставленных задач в разных условиях эксплуатации микропроцессора как на земле, так и в космосе.

Наличие достаточного количества портов для ввода/вывода информации, в том числе аудио- и видеоинформации, расширяет спектр для активного внедрения микропроцессорных решений на базе 1892ВМ14Я в различные сферы инфокоммуникаций.

Функциональные возможности системы на кристалле 1892ВМ14Я позволяют реализовать:

- аудио- и видеообработку данных;
- приложения для связи и навигации;
- средства защиты информации.

Результаты сравнения сигнальных процессоров

Для разработки и отладки программного обеспечения телекоммуникационных приложений на базе системы на кристалле 1892ВМ14Я была использована среда разработки *MCStudio* 4,

демонстрационная версия которой в свободном доступе представлена на официальном сайте АО НПЦ «ЭЛВИС» [4].

Реализация базовой криптографической операции вычисления остатка от деления в расширенных полях Галуа на примере сигнальных процессоров *ADSP*-2181 и 1892ВМ14Я приведена в таблице 1. Проведение различных вычислительных операций в расширенных полях Галуа является немаловажным процессом для криптографии. Главным образом за счет того, что такие операции не приводят к расширению разрядной сетки и являются обратимыми. В *RISC*-ядре происходит инициализация основных параметров, которые будут использоваться в ядре *DSP*0, и запуск этого ядра. В *DSP*0 происходит сама операция вычисления в расширенных полях Галуа с автоматическим сдвигом.

Таблица 1

Базовая криптографическая операция вычисления остатка от деления

***ADSP*-2181**	**1892ВМ14Я**	
	***RISC*-ядро**	***DSP*0**

NGDivision:
mr0 = 0x8000;
dis ar_sat;
af = tstbit 0xf of mr1;
if ne jump NGMark1;
ar = mr0 and ay1;
if ne jump NGOutDiv;
af = ay1 - mr1;
if eq jump NGOutZero;
if lt jump NGOutDiv;
se = exp mr1 (hi);
ar = se;
ar = ar - 1;
se = ar;
sr = norm mr1 (hi);
mr1 = sr1;
af = pass ay1;
none = mr0 and af;
if ne af = mr1 xor af;
ar = abs ar;
cntr = ar;
se = -1;
sr = lshift mr0 (lo);
do NGCircle until ce;
sr = lshift mr1 (lo), mr0 = sr0;
ar = mr0 and af, mr1 = sr0;
if ne af = mr1 xor af;
NGCircle: sr = lshift mr0 (lo);
ar = pass af;
rts;
NGMark1:
af = mr0 and ay1;
if eq jump NGOutDiv;
ar = mr1 xor ay1;
rts;
NGOutDiv:
ar = ay1;
rts;
NGOutZero:
ar = 0;
rts;
	#include "multicore/nvcom02t.h"
	
	extern unsigned int DSP0_GF_In_A;
	extern unsigned int DSP0_GF_In_B;
	extern unsigned int DSP0_GF_Out_C;
	extern unsigned int DSP0_GFDivision;
	
	unsigned int DSP0_GF_Output;
	
	int main() {
	
	unsigned short DSP0_InputA = 314;
	unsigned short DSP0_InputB = 67;
	
	DSP0_GF_In_A = DSP0_InputA;
	DSP0_GF_In_B = DSP0_InputB;
	
	DSP0_PCU.DCSR.data = 0;
	DSP0_PCU.SR.data = 0;
	
	DSP0_PCU.PC.data = ((unsigned int)
	&DSP0_GFDivision - 0xb8440000) >> 2;
	
	DSP0_PCU.DCSR.data = 0x4000;
	
	while (!DSP0_CSR.QSTR_DSP.bits.STP0);
	
	DSP0_GF_Output =DSP0_GF_Out_C;
	
	while (1);
	
	return 0;
	}
		.global DSP0_GFDivision
		.global DSP0_GF_In_A
		.global DSP0_GF_In_B
		.global DSP0_GF_Out_C
		
		.text
		DSP0_GFDivision:
		MOVE DSP0_GF_In_A,A0.S
		MOVE DSP0_GF_In_B,A1.S
		MOVE DSP0_GF_Out_C,A2.S
		MOVE (A0),R0.L
		MOVE (A1),R2.L
		
		MOVE 1, R1.L
		DO 31, Mark1
		ANDL R1.L, R0.L, R4.L
		MOVE.NE R4.L, R6.L
		ANDL R1.L, R2.L, R4.L
		MOVE.NE R4.L, R8.L
		LSLL 1, R1.L
		Mark1: nop
		
		MOVE R8.L,R1.L
		MOVE 1, R10.L
		DO 31, Mark2
		ANDL R1.L, R6.L, R4.L
		ADDL.NE 1, R10.L
		LSLL 1, R1.L
		Mark2: nop
		LSLL R10, R2
		EORL R0.L, R2.L
		MOVE R2.L, (A2)
		
		STOP
		nop
		nop
		
		.data
		DSP0_GF_In_A: .word 0
		DSP0_GF_In_B: .word 0
		DSP0_GF_Out_C: .word 0

Как можно видеть в таблице 1, реализация для системы на кристалле 1892ВМ14Я, хотя и выглядит более громоздко, однако количество задействованных команд меньше, по сравнению с

ADSP-2181. Вся операция в ядре *DSP*0 основывается на использовании команд переноса данных в другие ячейки, логического «И», «исключающее ИЛИ» и логического сдвига. Для реализации такой же операции в *ADSP*-2181 требуется куда более широкий синтаксис с множеством условий.

Также одним из примеров успешной разработки инфокоммуникационных приложений в *MCStudio* 4 можно назвать курсовое проектирование цифровых КИХ-фильтров и БИХ-фильтров [5].

Результаты сравнения технических характеристик процессора семейства *ADSP*-21*xx* фирмы *Analog Devices* и системы на кристалле 1892ВМ14Я фирмы АО НПЦ «ЭЛВИС» представлены в таблице 2. Система на кристалле 1892ВМ14Я существенно выигрывает за счет поддерживаемой разрядности, количества ядер, совмещении разных архитектур, режимов работы, высокой производительности, количества портов на периферии. Таким образом, это увеличивает количество различных решений в инфокоммуникационных приложениях, которые могут использоваться разработчиками программного обеспечения для реализации своих задач.

Таблица 2

Сравнение сигнальных процессоров

Характеристики	***ADSP*-2181**	**1892ВМ14Я**
Архитектура	модифицированная гарвардская	*ARM* (*CPU ARM Cortex-A*9), гарвардская (*DSP*-ядра)
Разрядность, бит	8 / 16	8 / 16 / 32 / 64
Количество ядер	1	2 (*Cortex-A*9 *MPCore*) 2 (*DSP*-ядро)
Напряжение питания ядер	5 В	1,1–1,2 В 1,8 В / 2,5 В / 3,3 В (для периферии)
Параллелизм и независимость вычислительных процессов	отсутствует	поддерживается
Производительность	33,3 МГц	Нормальные условия: 912 МГц — *CPU*, 720 МГц — *DSP* Нормальные условия и напряжение питания 1,2 В: 1104 МГц — *CPU*, 912 МГц — *DSP* Критические условия: 816 МГц — *CPU*, 672 МГц — *DSP*
Количество портов и режимы	2 – последовательные порты приема/передачи *SPORT*0 и *SPORT*1; 1 – порт интерфейса	2 – оперативная память (*LPDDR*2/*DDR*3); 2 – память (*NORMPORT* и *NANDMPORT*); 2 – портативная флеш-память (*SD*/*MMC*); 2 – сетевая связь с космическими аппаратами (*Space Wire*); 4 – организация связи с другими устройствами (*UART*); 2 – многофункциональные порты *MFBSP*; 2 – ввод видеоданных (*MIPI CSI*, *DMA*, *IP*); 1 – вывод видеоданных (*MIPIDSI*, *DMA*); 3 – аудио выходы; 1 – USB2.0
Скорость обмена данными по портам	40 *MIPS*	порты *LPDDR*2/*DDR*3 – 1008 МТ/с на частоте 504 МГц; разрядность — 16/32; порты *Space Wire* – от 2 до 696 Мбит/с; дуплексный режим работы; *USB*2.0 – 480 Мбит/с

Заключение

На основе проведенного исследования можно сделать вывод, что система на кристалле 1892ВМ14Я удовлетворяет основным требованиям по защите информации, главным образом за счет отсутствия незадокументированных прерываний. Архитектурные и функциональные возможности

процессора 1892ВМ14Я, его технические характеристики значительно превышают аналогичные показатели у сигнального процессора *ADSP*-2181, что делает его эффективным вариантом для использования в инфокоммуникационных приложениях и замены зарубежной элементной базы на отечественные аналоги в рамках стратегии импортозамещения.

Литература

1. *Осколков И.* Отечественные микропроцессоры Были! Есть. Будут? // 3*DNews Daily Digital Digest*. 09 августа 2018. *URL*: https://3dnews.ru/973284/page-1.html (дата обращения: 20.10.2020).
2. *Шаврин С.С., Зуйкова Т.Н., Мусатова О.Ю.* Техника микропроцессорных систем в инфокоммуникационных приложениях. Часть 1. Цифровые фильтры: Учебное пособие. М.: МТУСИ, 2019. 57 с.
3. *Шаврин С.С., Мельник С.В.* Цифровые системы передачи и методы их защиты: Учебное пособие. М.: МТУСИ, 2020. 91 с.
4. Официальный сайт акционерного общества «Научно-производственный центр «Электронные вычислительно-информационные системы». *URL*: https://multicore.ru/index.php?id=4 (дата обращения: 20.10.2020).
5. *Талантова А.Т.* Проектирование цифровых фильтров: Курсовая работа / рук. С.С.Шаврин. МТУСИ, 2020.
6. *Орлов В.Г., Терехов А.Н.* Характеристики речевых накопителей с однокристальными микроэлектронными устройствами // Фундаментальные проблемы радиоэлектронного приборостроения. 2009. Т. 9, № 4. С. 59-63.

FUNCTIONAL CAPABILITIES ANALYSIS OF THE 1892VM14YA SIGNAL PROCESSOR FOR THE PURPOSE OF USAGE IN INFOCOMMUNICATION APPLICATIONS

Robert A. Shchegolev,
Student MTUCI, Moscow, Russia
Vannetis@yandex.ru
Tatyana N. Zuikova,
Senior Lecturer of the Department of MTS MTUSI, Moscow, Russia
t.n.zuikova@mtuci.ru

Key words: *signal processor, microprocessor, SoC, information protection, import substitution, infocommunication applications, infocommunications, interruptions, architecture, 1892VM14YA, Multicom-02, MCStudio 4, ELVIS*

The article analyzes import substitution possibility in infocommunication applications and consider as an example the system based on 1892VM14YA chip «Multicom-02» (MCom-02), manufactured by JSC SPC «ELVIS». The factors that have a significant impact on the use of signal processors in infocommunications are highlighted. Analysis of the functional and architectural features of the system on 1892VM14YA chip. Based on the example of a basic cryptographic operation, software has been developed for the ADSP-2181 signal processor and for the system based on 1892VM14YA chip. A comparative analysis of technical characteristics and our developed software made it possible to identify a premise for implementation of microprocessor solutions based on 1892VM14YA chip in various fields of infocommunications and replacement of foreign element base with domestic counterparts when training specialists in professional educational programs.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Гончаров Владислав Сергеевич,
ведущий инженер АО "НПО РусБИТех, Москва, Россия
goncharovvslive@gmail.com
Верба Вера Алексеевна,
доцент кафедры ИСУиА МТУСИ, к.т.н., Москва, Россия
verba@list.ru

Ключевые слова: система обнаружения вторжений, Snort, Suricata, IDS, IPS, HIDS, NIDS.

В данной статье предметом исследования являются системы обнаружения вторжений (*IDS*). Выполнен анализ систем обнаружения вторжений (*IDS*) *Snort* и *Suricata*. Для решения данной задачи в статье использованы такие методы, как анализ, сравнение, описание, обобщение. Рассмотрены основные понятия *IDS*, *IPS*. Представлены типовая архитектура *IDS*, а также структурные схемы расположения сетевых (*NIDS*) и хостовых (*HIDS*) в сети. Описаны основные типы определения вредоносной активности, достоинства и недостатки данных типов систем. Приведены результаты сравнения. Внедрение систем обнаружения вторжений в комплексную систему средств защиты информации (СЗИ) позволяет существенно расширить спектр возможностей данных комплексов (СЗИ).

На сегодняшний день стремительное развитие информационных технологий и сети интернет является неотъемлемой частью современного общества. Однако, с развитием технологий, растёт количество проблем, связанных с информационной безопасностью (ИБ) и её обеспечением, а также со способами реализации ИБ [1].

Интегрируя веб-службы в бизнес-модель, организация может повысить доступность к своей бизнес-информации. Однако в то же время это делает эту организацию уязвимой для кибератак, которые могут нанести огромный финансовый ущерб.

Наличие правильно настроенного межсетевого экрана и часто обновляемых антивирусных программ по-прежнему не гарантирует защиты компьютера или сети компьютеров, и для этой цели важно фактически отслеживать трафик и обнаруживать потенциальные случаи подозрительного поведения.

Рассматриваемые далее программные решения могут предложить широкий спектр преимуществ как для отдельных пользователей, так и для крупных предприятий, где основное различие заключается в фактическом объеме финансовых ресурсов.

Вследствие этого на первый план выходят системы обнаружения вторжений (*IDS*) и системы предотвращения вторжений (*IPS*). Коммерческие продукты *IDS/IPS* дорогостоящие, и не всегда по своей эффективности превосходят свободно распространяемые системы.

IDS помогают в обнаружении потенциальных атак и предупреждать о них, анализируя сетевой трафик и определяя, соответствует ли наблюдаемое поведение допустимым условиям. *IDS* может быть основана на предопределенном наборе сигнатур известных угроз, или текущее поведение может быть сравнено с базовым уровнем, который был измерен ранее в течение определенного периода времени, в попытке обнаружить возможные аномалии. Конечно, существуют определенные ограничения данных решений, в которых используются эти два метода обнаружений, такие как ложноположительное и ложноотрицательное обнаружения. Таким образом, при обнаружении на основе аномалий базовый уровень должен быть точно измерен с учетом контекстных аспектов, которые будут определять нормальное поведение в сети, избегая ложных срабатываний. В то время как в случае обнаружения на

основе сигнатур база данных сигнатур должна часто обновляться, чтобы система могла распознавать атаки. Существуют также *IDS* на гибридной основе, использующие два вышеупомянутых метода обнаружений. Независимо от типа *IDS*, безопасность должна быть структурирована таким образом, чтобы это не мешало производительности организации.

IPS можно рассматривать как усовершенствование *IDS*, потому что, помимо регулярных действий по мониторингу, они также способны блокировать потенциально нежелательные действия.

В связи с этим вопросы, которые касаются изучения и анализа систем обнаружения вторжения, являются достаточно актуальными.

В этой статье основное внимание уделялось системным механизмам обнаружения и предотвращения сетевых вторжений *Snort* и *Suricata*.

Понятие и структура системы обнаружения вторжений

Системы обнаружения вторжений представляют собой специализированные программные комплексы, предназначенные для выявления информационных атак в автоматизированных системах (АС). Типовая архитектура IDS включает в себя следующие компоненты (рис. 1):

- модули-датчики, предназначенные для сбора необходимой информации о функционировании, АС;
- модуль выявления атак (МВА), выполняющий обработку данных, собранных датчиками, с целью обнаружения информационных атак нарушителя;
- модуль реагирования на обнаруженные атаки;
- модуль хранения данных, в котором хранится вся конфигурационная информация, а также результаты работы СОВ;
- модуль управления компонентами СОВ [2].

Рис. 1. Типовая архитектура систем обнаружения вторжений

IDS типы и методы

Реализация *IDS* зависит от среды. Система обнаружения вторжений на основе хоста (HIDS) предназначена для реализации в одной системе и защиты этой системы от вторжений или вредоносных атак, которые могут нанести ущерб ее операционной системе или имеющимся данным.

HIDS обычно зависит от метрик в среде хоста, таких как файлы журналов в компьютерной системе. Эти метрики или функции используются в качестве входных данных для механизма принятия решений *HIDS*. Таким образом, извлечение признаков из среды хоста служит основой для любых *HIDS*. Операционная структура *HIDS* и ее расположение в сети (рисунок 2).

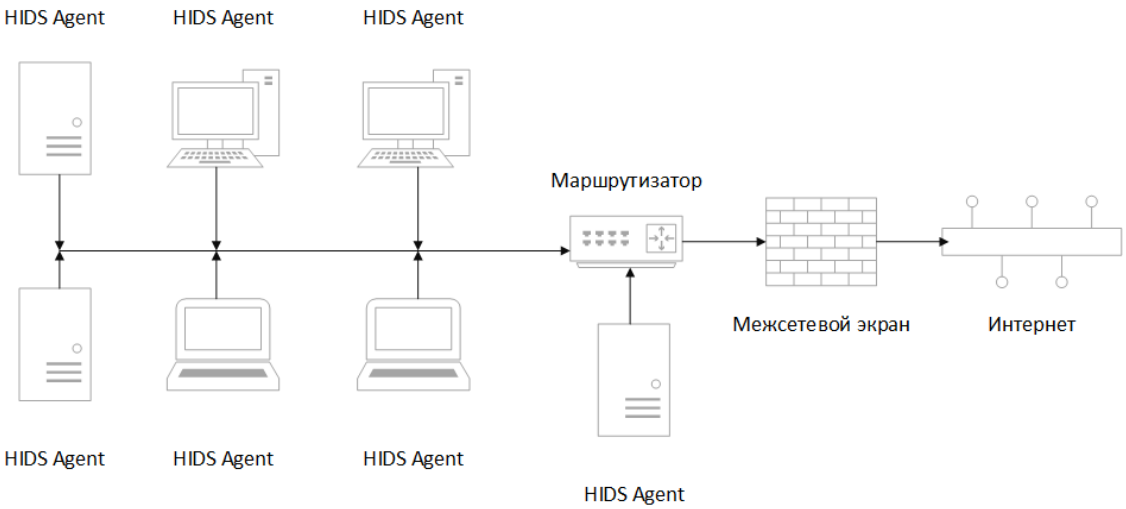


Рис. 2. Операционная структура *HIDS* и ее расположение в сети

Сетевая система обнаружения вторжений (*NIDS*) отслеживает пакеты сетевого трафика для обнаружения вторжений и вредоносных атак. *NIDS* может быть представлена в виде программного решения, а также программно-аппаратного. Например, *Snort* – это *NIDS* программный. Оперативная структура *NIDS* и ее расположение в сети продемонстрированы на рисунке 3.

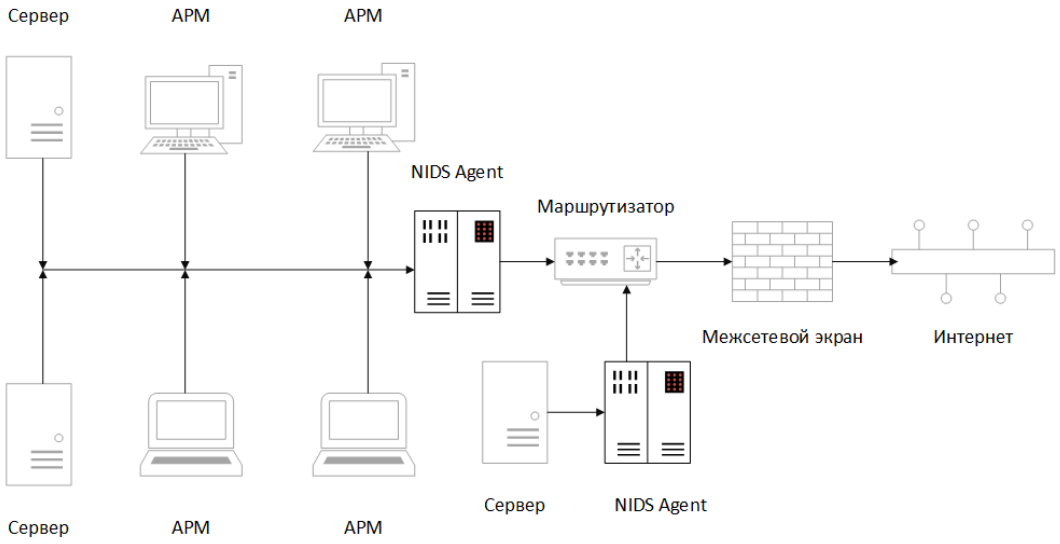


Рис. 3. Операционная структура *HIDS* и ее расположение в сети

Способы обнаружения вредоносной активности

1. Метод обнаружения вторжений на основе неправильного использования использует базу данных известных сигнатур и паттернов вредоносных кодов и вторжений для обнаружения хорошо известных атак. Перегрузка сетевых пакетов, высокая стоимость согласования сигнатур и большое количество ложных тревог являются тремя недостатками данных IDS, основанных на неправильном использовании [3]. Кроме того, серьезные ограничения памяти в некоторых типах сетей, приводят к низкой производительности *IDS* на основе неправильного использования из-за их необходимости хранить большую базу данных сигнатур.

Кроме того, базы данных сигнатур и шаблонов в *IDS* на основе сигнатур и *IDS* с сопоставлением шаблонов должны постоянно обновляться. Такие *IDS*, основанные на неправильном использовании, предназначены для обнаружения вредоносных атак и вторжений на основе предыдущих знаний.

2. В *IDS* на основе аномалий обычный шаблон данных создается на основе данных обычных пользователей, а затем сравнивается с текущими шаблонами данных в режиме онлайн для обнаружения аномалий. Такие аномалии возникают из-за шума или других явлений, которые имеют некоторую вероятность быть созданными хакерскими инструментами [4].

Таким образом, аномалии — это необычное поведение, вызванное злоумышленниками, которые оставляют следы в вычислительной среде. Эти следы обнаруживаются для идентификации атак, особенно неизвестных атак. Аномально-ориентированный *IDS* работает путем создания модели нормального поведения в вычислительной среде, которая постоянно обновляется, основываясь на данных от обычных пользователей и используя эту модель для обнаружения любых отклонений от нормального поведения.

3. Сигнатурные *IDS*, уже ранее упомянутые, работают с трафиком подобно антивирусному программному обеспечению на основе определенных шаблонов [5]. К недостаткам данных *IDS* стоит отнести отсутствие возможности противостоять атакам, отсутствующим в базах данных сигнатур.

SNORT

Snort- это однопоточная система обнаружения и/или предотвращения вторжений (*IDPS*), основанная на сигнатурах - это один из наиболее часто используемых механизмов *IDS*. Он работает, анализируя весь сетевой трафик в попытках обнаружить вторжение. *Snort* захватывает и анализирует пакеты и на основе сигнатуры известных атак определяет, является ли трафик легитимным или злонамеренным, причем в последнем случае превентивные меры будут приняты в соответствии с заранее определенным набором правил. Обработка трафика осуществляется путем пропуска пакетов через несколько модулей инфраструктуры *IDPS* (см. рис. 2).

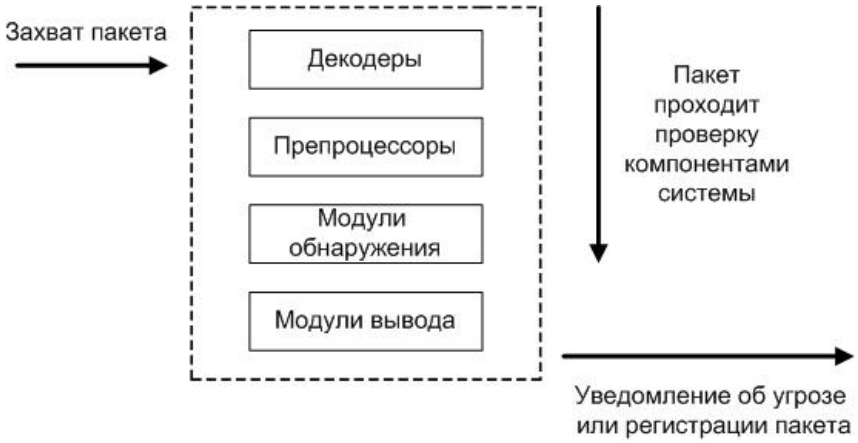


Рис. 4. Схема обработки пакетов *Snort*

Сначала пакеты обрабатываются модулем захвата пакетов, а затем в декодере структура каждого пакета анализируется на наличие отклонений, которые в случае обнаружения вызывают предупреждения. Однако этот декодер может время от времени запускать ложные срабатывания, поэтому в некоторых случаях может потребоваться изменить конфигурацию настроек предупреждений декодера. На следующем уровне препроцессоры подготавливают данные трафика для применения правил. Необходимо правильно настроить препроцессоры, чтобы предотвратить попадание нежелательных данных в механизм обнаружения. Таким образом, можно улучшить общую производительность системы. Затем в механизме обнаружения пакеты анализируются на наличие признаков вторжения путем применения к ним предопределенных правил. В состав каждого правила входит описание трафика, искомая сигнатура и описание угрозы, а также описание реакции на обнаружение угрозы. На заключительном этапе подключаемые модули вывода определяют, как поступать с предупреждениями, а именно спецификацию типа предупреждений, которые должны регистрироваться, и то, в каком каталоге необходимо уточнить.

Для мер безопасности также важно хранить правила *IDPS* на удаленном хосте и установить план восстановления, в котором будут указаны меры, необходимые предпринять, если система, в которой работает *Snort*, выйдет из строя и станет неспособной выполнять защитные обязанности.

Из-за ограничений обработки одного процессора, масштабируемость *Snort* может быть достигнута путем создания нескольких экземпляров *Snort* для каждого процессора (в случае многоядерных систем). Таким образом, в случае, если *IDPS* должна работать в многопоточной среде, возможно, потребуется реализовать многопоточное решение *IDPS*.

SURICATA

Как и *Snort, Suricata* – это *IDPS*, основанный на предопределенном наборе правил, точность которых будет определять частоту ложноотрицательного и ложноположительного распознавания угроз. [6]

Suricata была создана на основе инфраструктуры *Snort*, но в ней использовался многопоточный подход к обнаружению, который позволил более эффективно использовать многоядерные системы и выполнять параллельный анализ сетевого трафика, что позволило достичь большей масштабируемости, чем *Snort*. Кроме того, при использовании на одноядерных машинах Suricata может работать в однопоточном режиме.

Процесс обработки трафика в *Snort* использует концепцию многопоточности, что в основном означает, что несколько ядер центрального процессора (ЦП) используются для одновременной обработки сетевого трафика. Чтобы быть более конкретным, механизм обнаружения в *Suricata* содержит несколько потоков, что позволяет ему точно распределять вычислительную мощность и разделять операции обнаружения сигнатур между несколькими потоками.

Сравнение систем обнаружения вторжений

В ходе проведения анализа данной работы были проанализированы такие системы обнаружения вторжений, как *Snort, Suricata*.

Таблица 1

Результаты исследований

Скорость, Мбит/с	Система обнаружения вторжений	
	Snort	*Suricata*
10	38865 (30% загрузка ЦП)	43913 (30% загрузка ЦП)
100	28233 (100% загрузка ЦП)	43472 (100% загрузка ЦП

Таблица 2

Инструменты для анализа сетевого трафика и предотвращения атак

Инструментарий	*Snort*	*Suricata*
Анализ трафика	+	+
Выявление *Shell code*	+	+
Сканирование системы	+	+
Выявление атак на такие службы как *Telnet, FTP, DNS* и т.д	+	+
Выявление атак *DoS/DDoS*;	+	+
Выявление атак, связанных с *Web* серверами (*cgi, php, frontpage, iss* и т.д.)	+	+
Выявление атак на базы данных *SQL, Oracle* и т.д	+	+
Выявление атак по протоколам *SNMP, Net Bios, ICMP*	+	+
Выявление атак на *SMTP, imap, pop2, pop3*	+	+
Обнаружение *«Back doors»*	+	+
Web-фильтры	+	+
Извлечение и проверка переданных по *HTTP* файлов	-	+
Возможность идентификации по *URL*	-	+
Интеграция в системы мониторинга и виртуализации логов за счет модуля *Eve log* (*JSON* предупреждения)	-	+

Заключение

Оба рассматриваемых *IDPS* являются решениями с открытым исходным кодом, что может сделать их очень гибкими, когда дело доходит до конфигурации в соответствии с очень специфическими контекстами. Этот конкретный факт также может позволить интегрировать такой механизм *IDPS* в качестве одного из элементов в более крупную систему безопасности.

Таким образом, в результате сравнения пропускной способности и инструментов для анализа сетевого трафика IDPS Snort и Suricata, можно сделать вывод, что данные программные решения очень схожи. Выбор IDS/IPS будет обусловлен топологией сети и требуемыми функциями защиты.

Стоит отметить, что применение систем обнаружения вторжений позволяет:

- обеспечить близкий к максимальному уровень защищенности информационной системы;
- минимизировать время реакции системы на угрозы, следовательно, и наносимый системе вред, или же принять превентивные меры защиты, полностью блокирующие атаку;
- увеличить объемы анализируемого трафика;
- вести противодействие большому количеству атак одновременно.

Литература

1. *Белова А.Л., Бородавкин Д.А*. Сравнительный анализ систем обнаружения вторжений // Компьютерные и информационные науки. Актуальные проблемы авиации и космонавтики. 2016. С. 742-744.
2. *Лось А.Б., Даниелян Ю.Ю.* Сравнительный анализ систем обнаружения вторжений, представленных на отечественном рынке // Вестник МФЮА. 2014. № 3. С. 181-187.
3. *Creech G, Hu J* (2014) A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Trans Comput 63(4), pp. 807-819.
4. *Kumar S, Gautam, Om H* (2016) Computational neural network regression model for host-based intrusion detection system. Perspect Sci 8, pp. 93-95.
5. *Bul'ajoul W, James A, Pannu M* (2015) Improving network intrusion detection system performance through quality of service configuration and parallel technology // J Comput Syst Sci 81(6), pp. 981-999.
6. *Duque S, bin Omar MN* (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Comput Sci 61, pp. 46-51.

COMPARATIVE ANALYSIS OF INTRUSION DETECTION SYSTEMS

Vladislav S. Goncharov,
Leading engineer of JSC "NPO RusBITech", Moscow, Russia
goncharovvslive@gmail.com
Vera A. Verba,
Associate Professor of ICaAS Department MTUCI, Ph. D., Moscow, Russia
verba@list.ru

Keywords: *intrusion detection system, Snort, Suricata, IDS, IPS, HIDS, NIDS.*

In this article, the subject of research is intrusion detection systems (IDS). The analysis of intrusion detection systems (IDS) Snort and Suricata was performed. To solve this problem, the article uses such methods as analysis, comparison, description, and generalization. The basic concepts of IDS and IPS are considered. A typical IDS architecture is presented, as well as structural diagrams of network (NIDS) and host (HIDS) locations in the network. The main types of malicious activity detection, advantages and disadvantages of these types of systems are described. The results of comparison are given. The introduction of intrusion detection systems in the integrated system of information security tools (IST) allows you to significantly expand the range of capabilities of these complexes (IST).

НАВЫКИ ЯНДЕКС.АЛИСА: ОТ ИДЕИ ДО РЕАЛИЗАЦИИ

Дубельщиков Александр Александрович,
студент МТУСИ, Москва, Россия
mr.thunnus@gmail.com
Тутова Наталья Владимировна,
доцент кафедры ИСУиА МТУСИ, к.т.н., Москва, Россия
e-natasha@mail.ru

Ключевые слова: голосовой помощник, Яндекс.Алиса, голосовой интерфейс, Яндекс.Навыки, Яндекс.Диалоги, базы данных.

Рассмотрен процесс разработки навыков для голосового помощника Алисы от компании Яндекс. Рассмотрены виды навыков. Приведены этапы разработки навыка: формулировка идеи, создание сценария, написание программного кода, разработка баз данных и регистрация навыка. Проанализированы основные трудности при создании программ, использующих голосовые интерфейсы. Приведен анализ перспектив развития навыков для Алисы для пользователей и разработчиков «умных» устройств и приложений. Сделан вывод о том, что затраты на разработку навыка не окупаются и имеет смысл заниматься разработкой навыков в качестве рекламного и имиджевого хода.

На фоне стремительно развивающейся технологии Интернета вещей, находящей свое отражение в устройстве «умного» дома, все большую распространенность получают различные голосовые интерфейсы, призванные упростить процесс управления «умными» устройствами для получения информации и выполнения повседневных задач, например, прослушивания музыки, установки будильника и совершения покупок через Интернет.

Крупные IT-компании, такие как *Google*, *Amazon* и *Apple* инвестируют в разработку технологий голосовых интерфейсов и Интернета вещей значительные суммы, считая данные направления перспективными и прибыльными в ближайшем будущем. Они объединяются для разработки единых стандартов работы устройств умного дома и их интеграции с голосовыми помощниками [1]. Большой интерес представляют предлагаемые этими компаниями средства разработки специальных программ для расширения функциональности голосовых помощников силами сторонних разработчиков. Примерами таких программ являются *AmazonSkills* для голосового помощника *Alexa* или Яндекс.Навыки для Яндекс.Алиса.

В данной работе представлен обзор процесса разработки подобного навыка, а также приведен анализ перспектив развития навыков для Алисы для пользователей и разработчиков «умных» устройств. В нашей стране для русскоговорящих пользователей ключевым фактором выбора голосового помощника является полноценная поддержка родного языка, поэтому описание процесса разработки приведем на примере Яндекс.Алиса, предлагаемого компанией Яндекс.

Навык для Яндекс.Алиса

Компания Яндекс дала следующее определение «навыку» [2]:

- с точки зрения пользователя, навык – это специализированный режим Алисы, который вызывается определенным разработчиком активационным именем. В этом режиме Алиса транслирует реплики пользователя на сервер, и отвечает переданным сервером текстом, ссылками и подсказками.
- с технической точки зрения, навык – это веб-сервис, который ожидает реплик пользователя от Яндекс.Диалогов (платформы для создания чат-ботов и навыков). Веб-сервис можно

писать на любом удобном языке программирования или веб-фреймворке – он должен только корректно отвечать на запросы Диалогов.

Всего Яндекс предоставляет три категории навыков, разработкой которых могут заняться сторонние разработчики:

1. навыки общего типа, в которые входят все навыки, связанные с выполнением повседневных задач, таких как проверка банковского счета, уточнения состояния на дорогах и покупки в интернет-магазинах;
2. навыки умного дома, которые создают разработчики умных устройств для интеграции и работы их продукта с Яндекс.Алисой;
3. навыки «Синтезатор», которые представляют собой игру наспецифичном музыкальный инструмент реализованном с помощью «Яндекс.Станция Мини», в которой доступна регулировка громкости с помощью жестов.

Процесс разработки для каждого типа навыков имеет свои особенности. Поэтому в данной работе основное внимание сосредоточим на разработке навыка общего типа.

Шаг I: Идея и ее ограничения

Любая разработка начинается с идеи. В случае с разработкой навыка для голосового помощника Алисы следует изначально принимать во внимание, что любая идея должна быть помещена в рамки текущих технических возможностей платформы и специфики восприятия информации на слух.

В случае работы с голосовыми интерфейсами нельзя выдавать пользователю большое количество информации, к окончанию зачитывания которой часть информации пользователем будет уже забыта. Это не визуальный интерфейс, где пользователь сможет повторно прочитать забытое, потратив на это минимальное количество времени. Решаемые задачи должны быть максимально просты, а путь к ним должен быть выстроен в форме последовательного диалога с подсказками, имитирующим живое человеческое общение.

В качестве примера приведем ситуацию, описанную в одном из официальных уроков для разработчиков от компании Яндекс [3]. Некоторая авиакомпания делает независимому разработчику заказ на разработку навыка для голосового помощника Алиса, который должен осуществлять продажу билетов через соответствующий голосовой интерфейс, а также предоставлять актуальную информацию о рейсах, новостях авиакомпании, акциях, скидках, специальных предложениях и многом другом. Разработчик выполнил поставленное техническое задание, однако на выходе получился совершенно не пригодный к использованию навык. Во-первых, на предоставление одного лишь списка возможных действий у Алисы уходило слишком много времени, а во-вторых, навык был перегружен информацией, предоставляемой пользователю. Во время зачитывания информации о доступных к покупке билетах на самолет из Москвы в Санкт-Петербург пользователь, к последней позиции, успевал забыть первую. Невозможность корректного предоставления большого объема информации является главным ограничивающим фактором при разработке навыка.

Компания Яндекс утверждает, что правильным в этом случае было бы решение не пытаться сразу разработать полноценную систему для продажи и всеобъемлющей информационной поддержки клиентов, а начать с малого, например, с навыка, предоставляющего актуальную информацию о конкретном рейсе при произнесении его номера в форме диалога, который был бы прост и действительно полезен. Затем, уже после его интеграции и доработки, начать разработку таких же небольших, но полезных навыков, постепенно интегрируя их в единую, четко структурированную, выстроенную на основе диалогов систему.

На рис. 1 проиллюстрирован приведенный выше пример. На рис. 1 (а) приведен результат неправильной разработки навыка, предоставляющего большое количество сплошной текстовой информации, которую очень тяжело воспринимать на слух. На рис. 1 (б) приведен пример правильной разработки, имитирующий живой диалог, с конкретными вопросами и ответами, где пользователь знает, что он хочет услышать от голосового интерфейса, и получает нужную ему информацию.

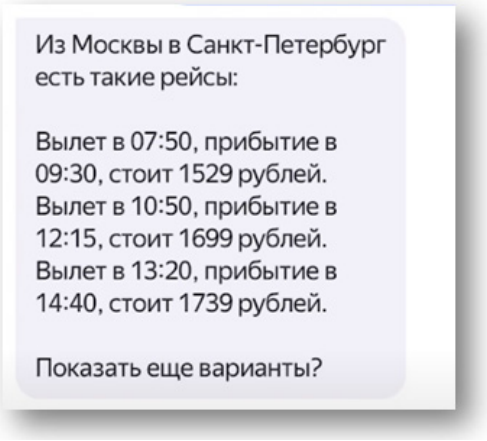


Рис. 1(а) Правильное построение навыка

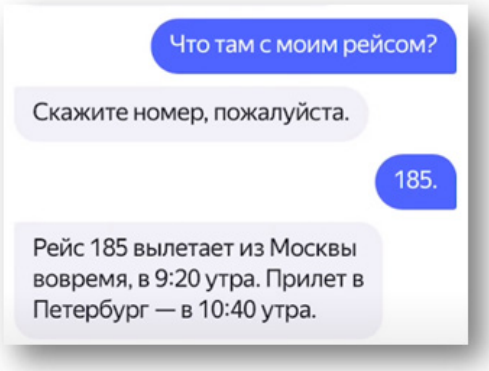


Рис. 1(б) Неправильное построение навыка

Шаг II: Создание сценария

Таким образом, навык – это четко выстроенный диалог между пользователем и голосовым интерфейсом. Для решения данной задачи в процессе написания навыка прописываются все возможные варианты обращения, в ответ на которые будут приходить заранее заданные ответы, т.е. формируется сценарий работы голосового помощника.

Сценарий в виде схемы может быть нарисован от руки, либо составлен с помощью специализированного программного обеспечения по созданию блок-схем, таким, например, как *Visio*. Сценарий должен содержать все события, все диалоги, с полным содержанием всех вариантов ответов, обращений и подсказок, в структурированной, последовательной форме.

Сценарий – это план, по которому будет выстраиваться разработка всего последующего навыка и игнорирование этого шага может привести к потере структурности, связанности и осмысленности в работе навыка в будущем. На рис. 2 представлен простейший, абстрактный пример схемы сценария.

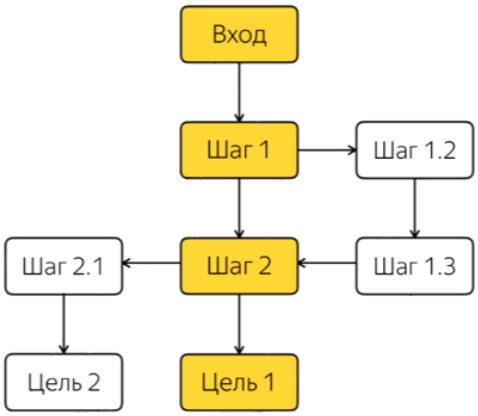


Рис 2. Пример сценария

Шаг III: Написание программного кода

Следующим шагом является написание программного кода вебхука [4]. Код может быть написан практически на любом распространенном языке программирования, например, на *Java* или *Python*, и представляет собой реализацию созданного ранее сценария с подключением к базе данных для записи обращений пользователей и хранения информации, которая может понадобиться для предоставление корректного ответа.

Для навыков, не требующих сложного ветвления диалога и активной работы с базами данных, существует возможность использования специальных конструкторов, призванных помочь в написании навыка без знания программирования. К таким сервисам относятся *Aimylogic*, *Verter*, *Alfabot*, *DialogFlower*, *Pipe.Bot*, *animytellme* и *Alicebot.pro* [5].

На рисунке 4 представлен пример функции обработки диалога для Яндекс.Алисы, написанный на *Python*.

```
# Функция для непосредственной обработки диалога.
def handle_dialog(req, res):
    user_id = req['session']['user_id']

    if req['session']['new']:
        # Это новый пользователь.
        # Инициализируем сессию и поприветствуем его.

        sessionStorage[user_id] = {
            'suggests': [
                "Не хочу.",
                "Не буду.",
                "Отстань!",
            ]
        }
```

Рис 3. Пример кода

Шаг IV: Разработка баз данных и регистрация навыка

После написания программного кода сценария следует разработать несколько баз данных. В первой базе данных будет хранится вся информация, которую в ответ на запросы пользователей будет предоставляться навыком через интерфейс Яндекс.Алиса. Сложность ее разработки зависит от предъявляемых требований. Так, например, если все ответы статичны, их частое изменение и обновление в режиме реального времени не предусматривается, в качестве базы данных можно использовать обычную *Excel*-таблицу, загруженную на Яндекс.Диск. Далее, сложность и используемые технические средства меняются и возрастают соответственно поставленному техническому заданию заказчика.

Во второй разработанной базе данных будут храниться все запросы пользователей, все обращения, которые они адресуют голосовому интерфейсу с целью получения корректного ответа на заданный вопрос, и именно с этим связана самая сложная часть разработки навыка, которая значительно повышает затраты на разработку и поддержание навыка в работоспособном состоянии.

Во время создания сценария разработчик прописывает для Алисы конкретные текстовые запросы, в ответ на которые она будет давать заранее заготовленные ответы, однако пользователи зачастую могут по-разному трактовать задаваемый вопрос, тем самым нарушая работу системы. Таким образом, ожидая ответ «да», Алиса вполне может получить следующие ответы: «Конечно», «Естественно», «Да-да», «Надоело», и даже совсем не связанные с предметом обсуждения запросы, наподобие: «Алиса… да, я сейчас вынесу мусор… да», «Какая погода в Москве?».

Вторая база данных предназначена для хранения всех запросов пользователей, чтобы впоследствии вычислить наиболее частые, не предусмотренные программой, запросы, которые в ходе естественного диалога применяют пользователи. Далее эти запросы добавляются в сценарий и программный код для того, чтобы Алиса впредь могла корректно на них реагировать.

Чем сложнее навык, чем больше у него функций, тем больше времени, сил и средств предстоит потратить на его поддержку и совершенствование. Лишенный поддержки и не доделанный для удобного общения навык не будет принят и востребован в силу неудобств использования.

После разработки баз данных, программного кода, основанного на заранее созданном сценарии, остается только загрузить все это на платформу Яндекс.Диалоги, заполнив всю требуемую информацию, и дождаться одобрения со стороны администрации портала. Если после проверки навыка модераторами Яндекса он будет признан отвечающим политики сообщества и работоспособным, он будет добавлен в общую библиотеку навыков и доступен для общего пользования.

Перспективы разработки навыков

С точки зрения разработчиков, навыки — это возможность получить дополнительный заработок. На данный момент, на сервисах услуг, таких как Яндекс.Услуги, можно найти большое количество предложений по разработке навыков различной сложности и стоимости. Кроме этого, Яндексом была учреждена премия в размере 150000 рублей, которая выплачивается раз в месяц разработчику самого перспективного и интересного с точки зрения Яндекса навыка.

Индивидуальные пользователи могут заказать разработку навыка, не предусмотренный Алисой изначально, для личного пользования. Такие обращения очень удобны разработчикам: они предоставляют возможность быстрого заработка и не требуют длительной поддержки и доработки сценария.

Для крупных компаний разработка голосовых помощников на сегодняшний момент является экономически неэффективной по нескольким причинам. Во-первых, сдерживающим фактором являются большие затраты на поддержание работоспособности навыка. Во-вторых, несмотря на то, что по статистике Яндекса Алиса установлена на трети всех используемых в России интернет-устройствах (смартфонах, компьютерах, ноутбуках), ее охват, несмотря на постоянный и активный рост, все еще недостаточно высок. Продукция Яндекса является предустановленной на многих устройствах и только часть пользователей используют Алису, в основном для управления навигатором и поиска в Интернет. То же касается и умных колонок Яндекс.Станция, призванных стать основной для умного дома. Несмотря на активное развитие этой технологии и все более широкое распространение, ее охват все еще недостаточно широк, чтобы можно было говорить об активной интеграции голосовых интерфейсов в повседневную жизнь обычных граждан.

Заключение

Голосовые помощники являются перспективным направлением, поддерживаемым крупными компаниями-разработчиками программного обеспечения. Они предоставляют средства разработки специальных программ, называемых навыками, предназначенных для расширения функциональности голосовых помощников. Этапы разработки навыка общего вида для голосового помощника Яндекс.Алиса включают формулировку идеи, создание сценария, написание программного кода, разработку баз данных и регистрацию навыка. Основные трудности при создании программ, использующих голосовые интерфейсы, связаны с тем, что некоторые разработчики пытаются создать систему с всеобъемлющей информационной поддержкой, в результате чего навык становится перегруженным и сложным для восприятия пользователями. Чем сложнее навык, чем больше у него функций, тем больше времени, сил и средств предстоит потратить на его поддержку и совершенствование. Лишенный поддержки и не доделанный для удобного общения навык не будет принят и востребован в силу неудобств использования.

Для крупных компаний разработка голосовых помощников пока что является экономически неэффективной. Это связано с большими затратами на поддержание работоспособности навыка, а также недостаточной востребованностью голосовых помощников населением. Но это вопрос времени. Поэтому не означает, что стоит отказаться от идеи голосовых помощников в принципе. Имеет смысл использовать их для повышения имиджа разработчиков и в качестве рекламного хода, что несколько уменьшает потребность в постоянной поддержке разработанного для этих целей продукта.

Литература

1. Cathy Pearl. Designing Voice User Interfaces: Principles of Conversational Experiences 1st Edition. M: Издательство O'Reilly Media, 2017. 150 с.
2. Официальный сайт компании Apple [Электронный ресурс] – Режим доступа: https://www.apple.com/ru/newsroom/2019/12/amazon-apple-google-and-the-zigbee-alliance-to-develop-connectivity-standard/, - свободный – (03.12.2020).
3. Яндекс.Диалоги. Разработка навыков для Алисы [Электронный ресурс] – Режим доступа: https://yandex.ru/dev/dialogs/alice/doc/about.html/, - свободный – (03.12.2020).
4. Вебхуки: как получать данные без промедления и опросов API [Электронный ресурс] – Режим доступа: https://proglib.io/p/vebhuki-kak-poluchat-dannye-bez-promedleniya-i-oprosov-api-2019-11-09 - свободный – (03.12.2020).
5. Youtube канал компании Яндекс. Школа Алисы [Электроный ресурс] – Режим доступа: https://www.youtube.com/channel/UCzQZwJjg0_1RyYPWB9sc4Wg, - свободный – (03.12.2020).

YANDEX.ALICE SKILLS: FROM IDEA TO IMPLEMENTATION

Alexander A. Dubelschikov,
Student MTUCI, Moscow, Russia
mr.thunnus@gmail.com
Natalia V. Toutova
Associate Professor of ISUA Department MTUCI, Ph.D., Moscow, Russia
e-natasha@mail.ru

Keywords: *voice assistant, Yandex.Alice, voice interface, Yandex.Skills, Yandex. Dialogs, databases.*

This paper describes the process of developing skills for Alice's voice assistant from Yandex. Types of skills are considered. The stages of skill development are given: idea formulation, scenario creation, program code writing, database development, and skill registration. The main difficulties in creating programs that use voice interfaces are analyzed. The analysis of Alice's skills development prospects for users and developers of smart devices and applications is presented. It is concluded that the cost of developing a skill does not pay off and it makes sense to develop skills as an advertising and image move.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ И РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ АВТОМАТИЧЕСКОГО ДЕТЕКТИРОВАНИЯ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ

Московская Елизавета Дмитриевна,
студент МТУСИ, Москва, Россия
moscovskayaliza@gmail.com
Звягина Ольга Владимировна,
студент МТУСИ, Москва, Россия
olga.v.zvyagina@gmail.com
Полянцева Ксения Андреевна,
ассистент кафедры МКиИТ МТУСИ, Москва, Россия
k.a.poliantseva@mtuci.ru
Мосева Марина Сергеевна,
старший преподаватель кафедры МКиИТ МТУСИ, Москва, Россия
m.s.moseva@mtuci.ru

Ключевые слова: ДТП, системы автоматического детектирования, методы машинного обучения, ручной подбор, столкновение.

Рассматривается реализация двух подходов автоматического детектирования дорожно-транспортных происшествий на модельном образце: ручной настройки порогов и классификации ситуации с использованием методов машинного обучения. В качестве модельного образца использовалась радиоуправляемая машинка с установленными на нее необходимыми датчиками: акселерометром и датчиком шума. Сбор и обработка данных осуществляется на базе платформы Arduino. Анализ каждого из методов, их последующее сравнение, а также выявление преимуществ и недостатков каждого из подходов.

Введение

В статье [1] рассмотрена проблема смертности в дорожных авариях из-за временного интервала между инцидентом и появлением врачей первой медицинской помощи. Возможным подходом к сокращению задержки между инцидентом и приездом скорой помощи может быть использование в автомобилях автоматических систем по определению дорожно-транспортного происшествия и немедленному вызову соответствующих служб. [2]

Авторами статьи решено было воспользоваться методом ручного подбора порогов. Однако мы посчитали, что это не единственный и не самый оптимизированный метод, поэтому основной задачей стал поиск более эффективного метода детектирования.

Данная работа также посвящена исследованию методов детектирования ДТП. Однако реализацию решено было провести в модельной версии.

Таким образом, целью работы является: создать систему для распознавания дорожно-транспортных происшествий на модельной версии.

Для достижения цели были поставлены следующие задачи:

1. Собрать модельный образец.
2. Изучить методы, позволяющие определить аварийные ситуации.
3. Реализовать изученные подходы детектирования аварий.
4. Провести эксперименты с реализованными методами.
5. Провести сравнительный анализ предложенных методов.

Аппаратная часть

Для создания модели было решено оснастить радиоуправляемую машинку датчиками, идентичными тем, что описаны в статье, а именно акселерометром и датчиком шума. Получать и обрабатывать данные с датчиков было решено при помощи платформы Arduino, которая широко распространена среди новичков в микроэлектронике.

Были использованы следующе аппаратные средства:

1. Акселерометр (Troyka - модуль)
2. Датчик шума (Troyka - модуль)
3. Микроконтроллер Arduino Nano
4. Машинка на радиоуправлении
5. Светодиод
6. Кнопки
7. Контактный датчик
8. Пьезо-элемент

Необходимо прочно закрепить все датчики на машинке во избежание погрешностей в измерениях. Для этого была спроектирована планка для крепления датчиков и контроллера на крышу машинки. Крепежная планка была вырезана из 4мм акрила на лазерном гравере.

При помощи планки все элементы были закреплены на крыше машинки. Схема подключения элементов к контроллеру изображена на рис. 1.

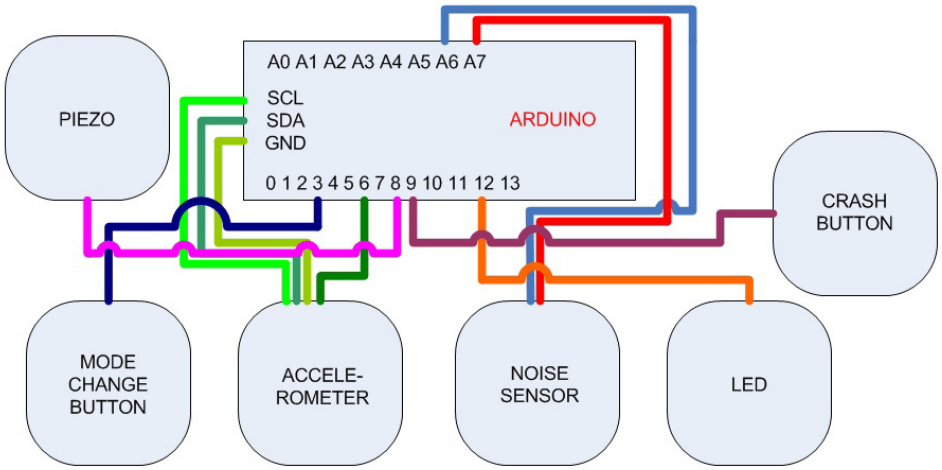


Рис. 1. Схема подключения элементов к контроллеру

Итак, конструкция представляет собой контроллер, к которому подсоединены датчик шума и акселерометр, а также светодиод, две кнопки, контактный датчик и пьезо-элемент (пищалка).

Одна из кнопок (на рис. 2 черная) служит для переключения между разными режимами программы, определяющий столкновения. Вторая кнопка (на рис. 3 белая) контролирует подачу питания на Arduino, что дает возможность детектировать столкновения не подключая контроллер к компьютеру.

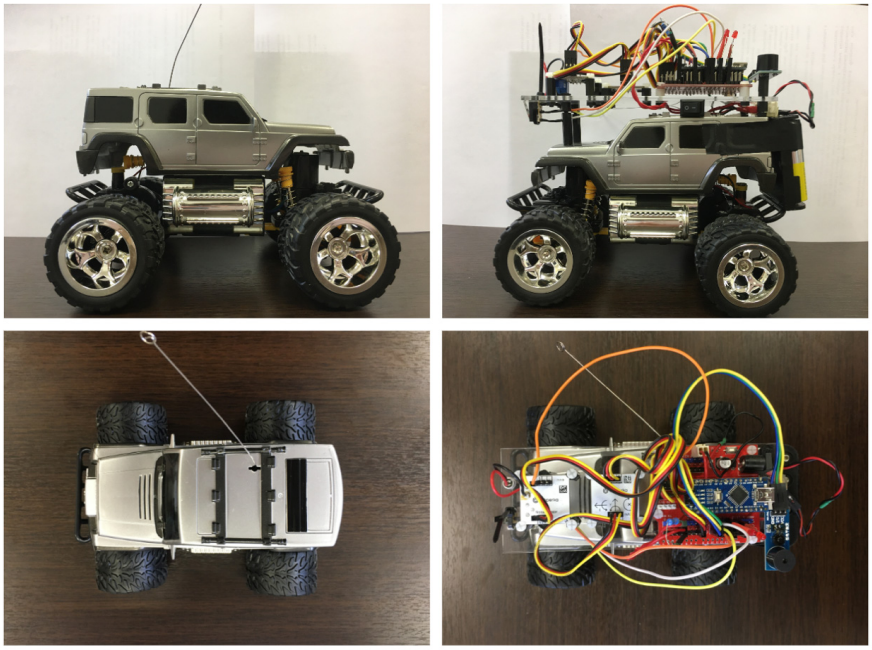


Рис. 2. Фотография крепежа на машинке с реализованной системой

Детектирование аварии при помощи порогов

Подобно авторам изучаемой статьи, первым методом детектирования аварии была ручная настройка порогов срабатывания датчиков. Пороги высчитываются визуально, сравнивая показания при безопасном вождении, резком торможении и столкновении. [3] Как видно столкновение характеризуется низким отрицательным ускорением и высоким уровнем шума рис.3.

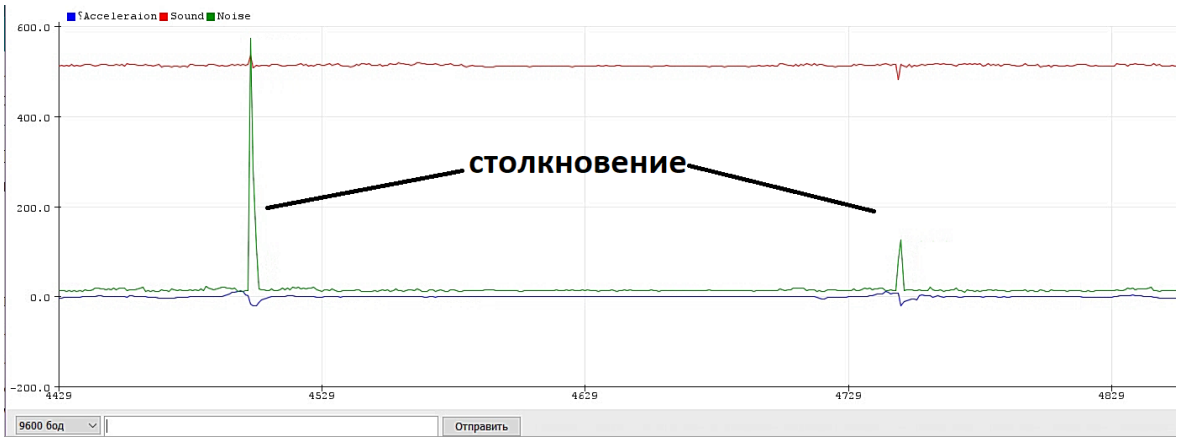


Рис. 3. График значений текущих показаний

Изначально измерялись текущие показания шума и звука, но потом мы пришли к выводу, что это не совсем корректно, так как высокий уровень может быть из-за громко работающего радио, спорящих или смеющихся людей вблизи динамиков, или же из-за громкой стройки на дороге, которую проезжает машина. [4] Из чего сделали вывод, что столкновение будет характеризоваться именно резким скачком этих показаний, а не текущим уровнем.

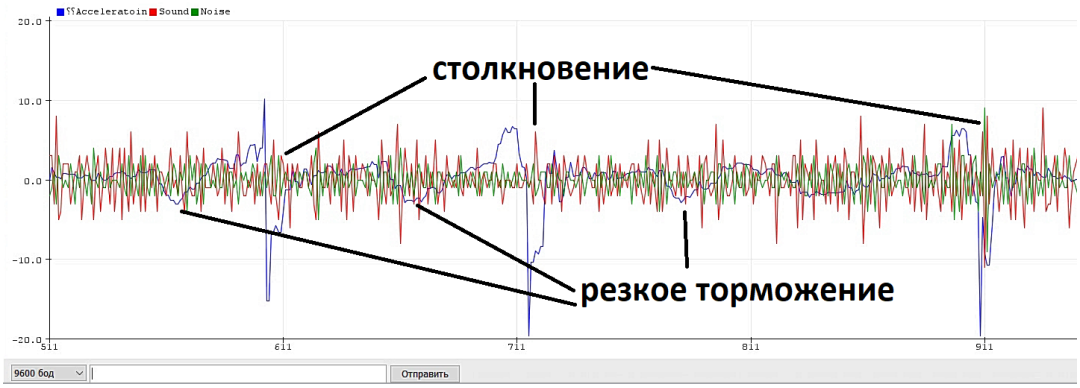


Рис. 4. График разницы последующих измерений

Детектирование аварии методами машинного обучения

Однако существует другой подход к данной задаче, который не требует ручной настройки и подборки порогов срабатывания. Данный подход основан на методах машинного обучения, задача которых автоматически построить модель предсказания на основе данных, предоставленных «учителем». Для этого машинка была также оснащена контактным датчиком, нажатие которого происходит в момент столкновения.

В настоящее время особую популярность в методах машинного обучения получили глубокие нейронные сети (*deep learning*), которые позволяют автоматически решать сложные задачи по распознаванию образов на изображениях, переводу текстов на другие языки, предсказанию экономической ситуации и многие другие. [5] В данной работе решено было обойтись одним нейроном в силу простоты и компактности решения.

Одному нейрону все ещё под силу решить задачу классификации ситуации для модельного случая. То, что делает один нейрон также иногда называют логистической регрессией.

Логистическая регрессия применяется для прогнозирования вероятности возникновения некоторого события (y) по значениям множества признаков ($x_1, x_2, x_3, \ldots, x_n$). Переменная y принимает значение в диапазоне от 0 до 1: число 0 (событие не произошло) и 1 (событие произошло).

В данном случае значение y будет меняться в зависимости от того, произошла авария или нет. А признаками являются значение ускорения по оси OX, скачок шума и звука Рис.5.

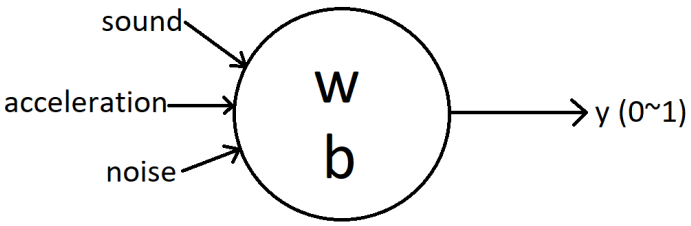


Рис. 5. Схема переменных нейрона

Таким образом нейрон ищет решение по формуле:

(1)

Где

– проекция ускорения на ось OX,

s – уровень звука,

n – уровень шума,

w_1, w_2, w_3, b – гипер-параметры нейрона,

σ – сигмоид, функция вида

$$\sigma(x) = \frac{1}{1 + e^{-x}} \quad (2)$$

Нормирующая значения на интервал (0; 1), график которой представлена рис. 6.

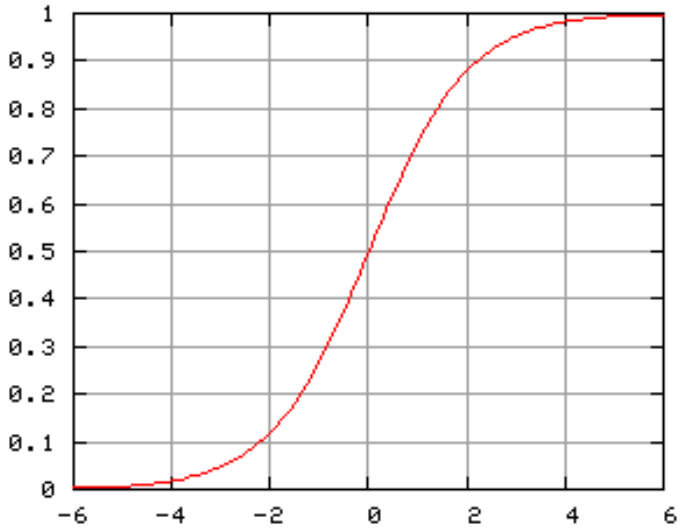


Рис. 6. График функции (с сайта Википедия: Wikipedia.org/wiki/Сигмоида)

Далее нейрон обучается с помощью обучающей выборки, состоящей из множества независимых признаков и соответствующих значений y. Таким образом, высчитываются параметры нейрона (w_1, w_2, w_3, b).

Затем коэффициенты функции σ обновляются для улучшения предсказывающей способности (где y – показатель реальной аварии, $\overline{y}$ – показатель предсказанной аварии, α – параметр обучения (в данном случае равный 0,01)).

$$dz_i = \overline{y_i} - y_i; \quad (3)$$

$$dw_i = x_i \times dz_i; \quad (4)$$

$$w_i = w_i - \alpha \times dw_i; \quad (5)$$

$$db = dz; \quad (6)$$

$$b = b - \alpha \times db; \quad (7)$$

Среда разработки

Программа написана на языке *C++* в среде *Arduino IDE*, работает в нескольких режимах, а именно в режиме обучения и предсказывании нейрона. Кроме того, программа позволяет записывать параметры нейрона в память *Eeprom*, что избавляет от необходимости сначала обучать нейрон при каждом запуске, а также позволяет обнулять память в случае неудачной подборки.

Программа, определяющая столкновения методом подбора ручных порогов так же написана на языке *C++*, в среде *Arduino IDE*. Пороги высчитаны вручную путем визуальной оценки графиков и составляют: -10 м/с2 для ускорения, 4 дБ для разницы шума и 6 дБ для разницы звука.

Обучение нейрона

Изначально программа работает в режиме обучения нейрона. [6] На графике Рис. 7 красным цветом изображена предсказанный нейроном класс ситуации (0 – нет столкновения, 1 – есть столкновение), а синим цветом показание контактного датчика, т.е. реальная ситуация (на графике

совпадает с осью OX, т.к. не происходило столкновения). Синий график совершает скачок, когда срабатывает контактный датчик спереди машинки.

Сразу после запуска этого режима, плавно катаем машинку или оставляем в режиме покоя, и мы видим, как с течением времени графики начинают все больше совпадать, т.е. нейрон обучается правильно распознавать безаварийную ситуацию.

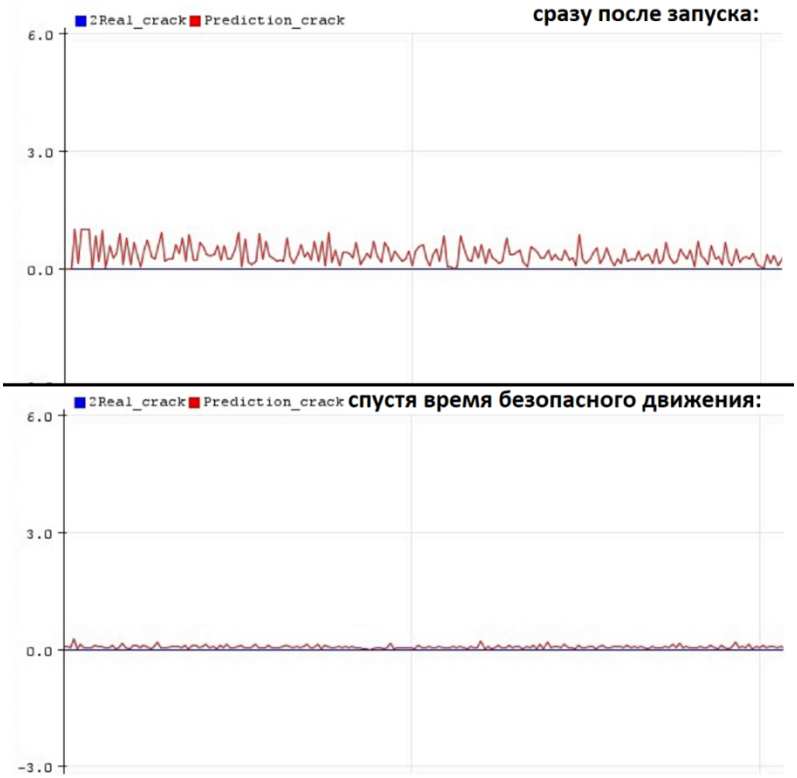


Рис. 7. График изменения предсказывающей аварии при безопасном движении

Теперь добавляем столкновения, а также резкое торможение, но без врезания. Как видно по графику Рис.8, резкие торможения нейрон воспринимает крайне близко к значению аварии.

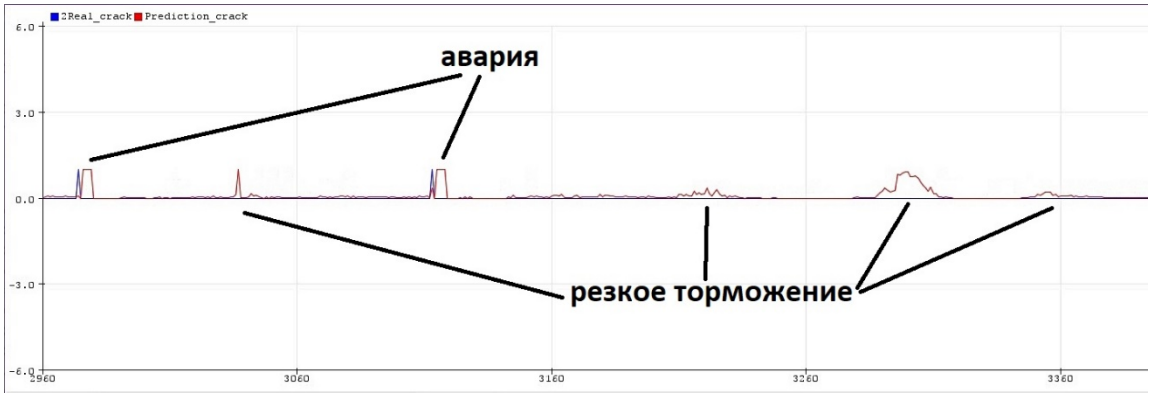


Рис. 8. График изменения предсказывающей аварии при столкновениях и резких торможениях

Это происходит из-за достаточно близких показаний акселерометра в обоих случаях, однако у нас еще есть датчик шума и пищалка, которая заменяет звук раскрывающихся подушек безопасности в реальной жизни. Таким образом, в скором времени в процессе обучения скачки резких торможений станут куда ниже по своему значению рис. 9.

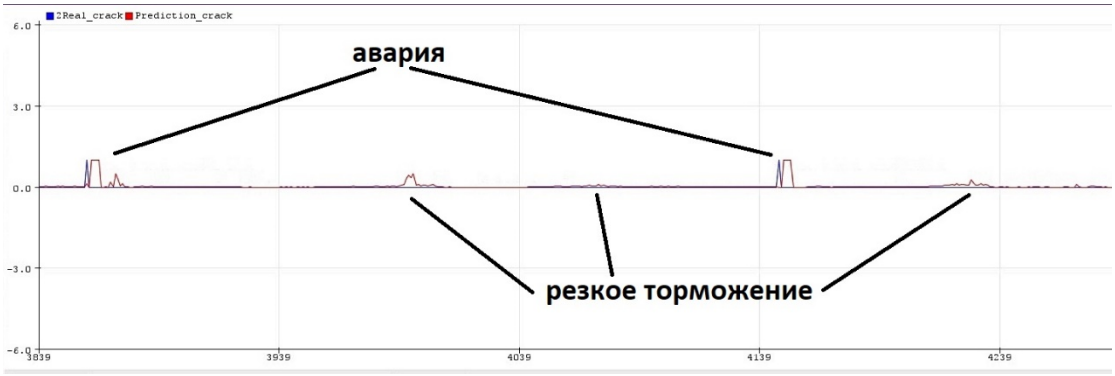


Рис. 9. График изменения предсказывающей аварии при столкновениях и резких торможениях после обучения

Такие случаи можно отсеять, установив порог. Пусть если предсказание аварии составляет 0.75 или выше – авария считается реальной и загорается лампочка, символизируя отправку сигнала в экстренные службы. Все что ниже – будет засчитываться как ложный сигнал. Обучение закончено.

Предсказание аварий

Сравнивая метод детектирования порогами и метод с использованием машинного обучения, стоит отметить, что в данном случае метод машинного обучение оказался более эффективным. На Рис.11 (синий цвет графика, построенного с помощью анализа порогов, зеленый – предсказанный нейроном, красный – реальное столкновение) видно, что нейрон предсказал аварию в 4 из 4 столкновений, в то время как метод порогов только один раз. Однако, не стоит делать глобальный вывод из этого графика, т.к. это зависит от качества подбора порогов. Кроме того, можно увидеть, что нейрон несколько раз предсказал фантомную аварию, является минусом. Несмотря на это, первичной задачей является обнаружение ДТП, а потом уже предотвращение ложных вызовов. Исходя из этого детектирование аварий с помощью методов машинного обучения оказался более эффективном в данном исследовании.

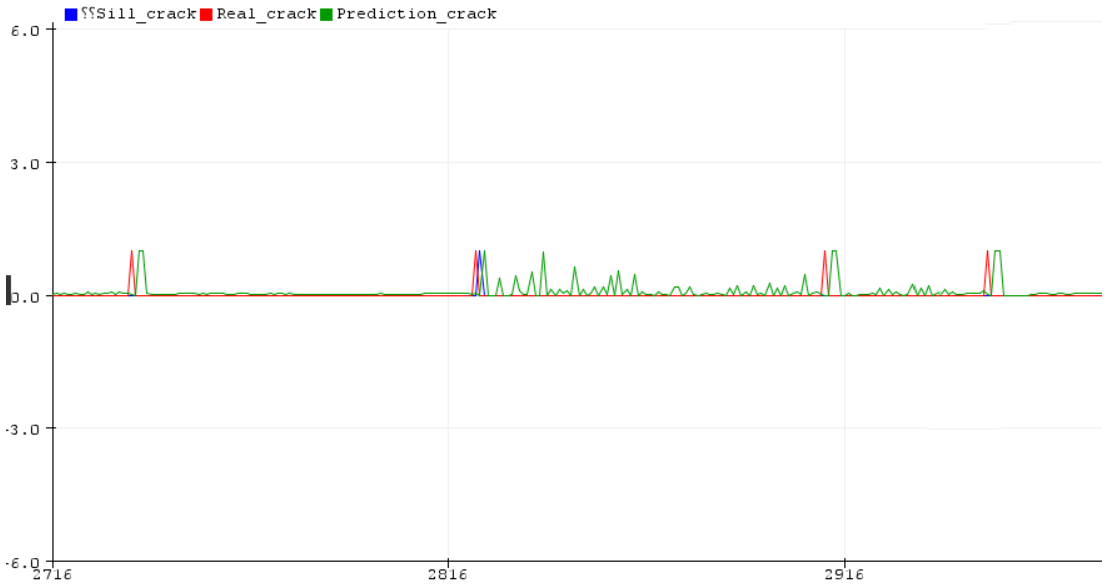


Рис. 10. Сравнение методов детектирования

Заключение

На сегодняшний день большую популярность имеют системы автоматического детектирования. Работа таких систем, основанная на методах машинного обучения, способна заменить работу человека во многих областях: мониторинг заводов, охраняемых территорий, пропускных пунктов и т.п. Однако помимо облегчения рабочего процесса в различных сферах индустрии, системы автоматического детектирования можно использовать для определения аварий в ДТП, ради сохранения человеческих жизней, а также ликвидации пожизненных увечий, принесенных из-за большого временного интервала между получением травмы в автокатастрофе и приездом врачей скорой помощи.

Несмотря на то, что в нашем исследовании была рассмотрена данная проблема всего лишь в модельной версии, все равно можно сделать вывод, что системы, основанные на методах машинного обучения, эффективно справляются со своей работой, и их применение в реальной жизни, поможет спасти сотни жизней.

Литература

1. «WreckWatch: Automatic Traffic Accident Detection and Notification with Smartphones». *Jules White, Chris Thompson, Hamilton Turner, Brian Dougherty, and Douglas C. Schmidt*

2. *K. A. Polyantseva, M. G. Gorodnichev, M. S. Moseva and T. D. Potapchenko,* "On the Applicability of Neural Networks in the Tasks of Detecting Dangerous Movement," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2019, pp. 1-4, doi: 10.1109/WECONF.2019.8840654.

3. *M. G. Gorodnichev, K. A. Polyantseva and M. V. Yashina,* "Informational Aspects of Automated Monitoring of Dangerous Driving," 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1-5, doi: 10.1109/SOSG.2019.8706721.

4. *Hastie, T., Tibshirani R., Friedman J.* The Elements of Statistical Learning: Data Mining, Inference, and Prediction. - 2nd ed. - Springer-Verlag, 2009.

5. *Городничев М.Г., Полянцева К.А.* Современные методы детектирования опасного движения частиц с мотивированным поведением // Материалы XII Международной отраслевой научно-технической конференции. М.: Медиа паблишер, 2018. С. 314-316.

6. *Sheetal S.* Artificial Neural Network (ANN) in Machine Learning 8 August 2017.

COMPARATIVE ANALYSIS AND DEVELOPMENT OF INTELLIGENT SYSTEMS FOR AUTOMATIC TRAFFIC ACCIDENT DETECTION

Elizaveta D. Moskowskaya,
Student MTUCI, Moskva, Russia
moscovskayaliza@gmail.com
Olga V. Zvyagina,
Student MTUCI, Moskva, Russia
olga.v.zvyagina@gmail.com
Ksenia A. Polyantseva,
Assistant of the Department of MCaIT MTUCI, Moskva, Russia
k.a.poliantseva@mtuci.ru
Marina S. Moseva,
Senior lecturer of the Department of MCaIT MTUCI, Moskva, Russia
m.s.moseva@mtuci.ru

Keywords: *traffic accidents, automatic detection systems, machine learning methods, manual selection, collision.*

The article discusses the implementation of two approaches to automatic detection of road accidents on a model sample: manual threshold setting and situation classification using machine learning methods. A radio-controlled car with the necessary sensors installed on it: an accelerometer and a noise sensor was used as a model sample. Data collection and processing is carried out on the basis of the Arduino platform. Analysis of each of the methods, their subsequent comparison, as well as identification of the advantages and disadvantages of each of the approaches.

ИСПОЛЬЗОВАНИЕ АВТОКОДИРОВЩИКОВ В ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ СИСТЕМАХ И СУПЕРКОМПЬЮТЕРАХ ДЛЯ ОПРЕДЕЛЕНИЯ АНОМАЛИЙ

Симонов Кирилл Вадимович,
магистрант МТУСИ, Москва, Россия
kirillsimonov@yandex.ru
Шевелев Сергей Владимирович,
доцент кафедры СИТиС МТУСИ, к.т.н., Москва, Россия
shevelev-s@yandex.ru

Ключевые слова: *высокопроизводительная система, суперкомпьютер, определение аномалий, методы машинного обучения с учителем, методы машинного обучения без учителя, автокодировщик, классификация.*

Представлено актуальное состояние развития современных суперкомпьютеров и высокопроизводительных систем. Рассмотрен принцип работы протокола MQTT. Проведено сравнение методов машинного обучения «с учителем» и «без учителя» для решения задачи выявления аномалий. Описан принцип работы модели нейронной сети автокодировщик. Приведено описание системы сбора телеметрических данных суперкомпьютера D.A.V.I.D.E. Рассмотрен процесс обучения и внедрения моделей нейронных сетей в узлы суперкомпьютера. Представлены количественные характеристики эффективности работы внедренных автокодировщиков.

Введение

В современном мире количество информации, которую необходимо хранить и обрабатывать растет с каждым годом. Согласно отчетам International Data Corporation, мировой объем данных в 2018 году составлял 33 зеттабайта, в то время как в 2020 данная цифра увеличилась до 59 зеттабайт**.** С этим связан рост популярности высокопроизводительных вычислительных систем и использования услуг дата-центров [1, 8]. Точного определения, как и минимальных количественных и качественных характеристик высокопроизводительных вычислительных систем нет, однако их можно описать как системы, имеющие вычислительную мощность для того, чтобы решать сложные вычислительные задачи за приемлемое время**.** Современные суперкомпьютеры увеличиваются как в размерах, так и в количестве вычислительных компонентов, число которых исчисляется в сотнях и тысячах (таблица 1) [2].

Таблица 1

Количество компонентов современных суперкомпьютеров

Место в топ 500	Название	Число компонентов
1	Фугаку	158976 процессоровFujitsu A64FX
2	Summit	4608 узловпо 2 IBMPower9 CPUи 6 NVIDIA Tesla GPU
10	Piz Daint	1813 узлов по 2 Xeon E5-2695 v4 CPU и 5704 узла по Xeon E5-2690 v3 CPU

Такое наращивание компонентов системы с одной стороны ведет к увеличению ее вычислительной мощности, а с другой – к повышению возможности возникновения в ней аномальных ситуаций и неисправностей. Подобные ситуации имеют гетерогенную природу и могут варьироваться от отказов на физическом уровне до неправильной конфигурации администратором и ошибок в программном обеспечение. На данный момент задача выявления проблем с узлами высокопроизводительных вычислительных систем и суперкомпьютеров лежит на системных

администраторах. Современные системы выявления аномалий основаны на анализе системных логов или сообщений, которые генерируются специализированными приложениями на уровне операционной системы [3]. Отсутствие унифицированных систем определения аномалий заставляет администраторов разворачивать набор различных прикладных решений, которые необходимо правильно настроить и установить. Очевидно, что такой подход нельзя использовать в больших системах, которые к тому же с каждым годом масштабируются, и необходимо разработать методы автоматизированного выявления отказов и аномальных ситуаций.

Данные о состояниях узлов суперкомпьютеров и высокопроизводительных систем можно получить от специальных сенсоров, которыми оборудованы их физические компоненты. Интегрированные системы мониторинга циклически считывают данные с датчиков и собирают их в одном месте. Многие такие инфраструктуры используют протокол MQTT (Message Queuing Telemetry Transport), разработанный для работы с телеметрией и работающий поверх стека TCP/IP [4]. Обмен сообщений по этому протоколу происходит по принципу издатель-подписчик. Очевидно, что программы-агенты, развернутые на blade-серверах, будут использовать вычислительную мощность, которая должна быть предоставлена высокопроизводительным вычислениям или приложениям пользователей. Другим подходом является внедрение внешнего устройства в узел, который позволяет отслеживать состояние узла посредством выделенного интерфейса без использования ресурсов сервера.

Разумно предположить, что обработка собранной от датчиков информации в реальном времени может помочь в поисках аномальных ситуаций. Одним из вариантов такой реализации может служить использование методов машинного обучения для выявления аномалий. Систему, основанную на методах машинного обучения с учителем, можно обучить классифицировать поведение узлов на нормальное и абнормальное. Проблема такого подхода заключается в ограничениях, которые накладывают методы обучения с учителем. Во-первых, для наилучшего результата обучения исходный набор данных должен содержать примерно равное количество данных для каждого из имеющихся классов, что сложно осуществить, так как аномальные ситуации возникают достаточно редко и информации о них заведомо немного. Во-вторых, система будет обучена различать конкретные, заранее определенные ситуации, а новые, невиданные ранее, будут неправильно классифицированы. Методы машинного обучения без учителя позволят избежать данных ограничений: для них не нужна размеченнаяобучающая выборка, а систему можно обучить только нормальным состояниям узлов, что позволит считать остальные состояния за аномальные. Одной из таких архитектур является автокодировщик – нейронная сеть, которая пытается воссоздать входные данные, прошедшие кодировку в скрытых слоях, на выходном слое.

Устройство автокодировщика

Рассмотрим возможности использования автокодировщиков для определения аномальных ситуаций в высокопроизводительных системах и суперкомпьютерах.

Автокодировщик состоит из 3 основных компонентов: слоя кодировщика, слоя закодированных данных и слоя декодера (рис. 1).

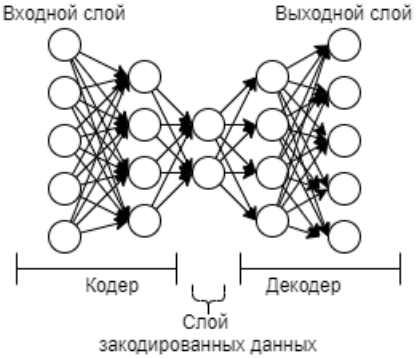


Рис. 1. Архитектура автокодировщика

Данные с входного слоя кодировщика сжимаются - “кодируются” - и поступают в скрытые слои. Это достигается за счет того, что количество нейронов в скрытых слоях уменьшается с каждым слоем, что позволяет снизить размерность данных и выделить только важные зависимости. После того, как размерность данных уменьшилась до необходимого размера, данные поступают в скрытые слои декодера. Размерность слоев в декодере аналогична размерности слоев в кодировщике, а количество нейронов в его выходном слое равно размерности входных данных. Основная задача автокодировщиков – воспроизвести входные данные с допустимой погрешностью, называемой ошибкой восстановления. Если модель такой нейронной сети будет обучена на данных, соответствующих нормальному состоянию системы, то при прохождении через нее метрик, характерных для аналогичного состояния, ошибка восстановления будет низкой. С другой стороны, автокодировщику будет сложно воспроизвести входные данные для аномальных ситуаций – ошибкавосстановления будет высока. На основе нее будет сделан вывод о возникновении в системе неполадок.

Инфраструктура мониторинга

Один из вариантов использования системы на основе автокодировщиков тестировался на суперкомпьютере D.A.V.I.D.E., разработанным компанией E4 Computer Engineering и располагающимся в некоммерческом консорциуме итальянских университетов CINECA в город Болонья [5]. Данный суперкомпьютер состоит из 45 узлов, а его максимальная производительность достигает 990 TFlops. Инфраструктура сбора информации, развернутой в D.A.V.I.D.E., называется Examon [6]. Examon является легковесной, расширяемой программой, собирающей детализированные данные о системе. Эти данные поступают в Examon от плат Beaglebone Black, встроенных в узлы суперкомпьютера и измеряющих набор системных метрик, таких как температура, скорость вращения вентиляторов, нагрузки ядер, потребление энергии и других, описывающих состояние системы. Данные платы основаны на процессоре ARM Cortex-A8 и оснащены 12-битным аналогово-цифровым преобразователем, способным производить 50 тысяч замеров в секунду. В общей сумме для каждого узла таких метрик 166. Платы в узлах снабжены программами-агентами системы Examon, а обмен данными с сервером ведется с помощью протокола MQTT. Архитектура сбора телеметрической информации представлена на рисунке 2.

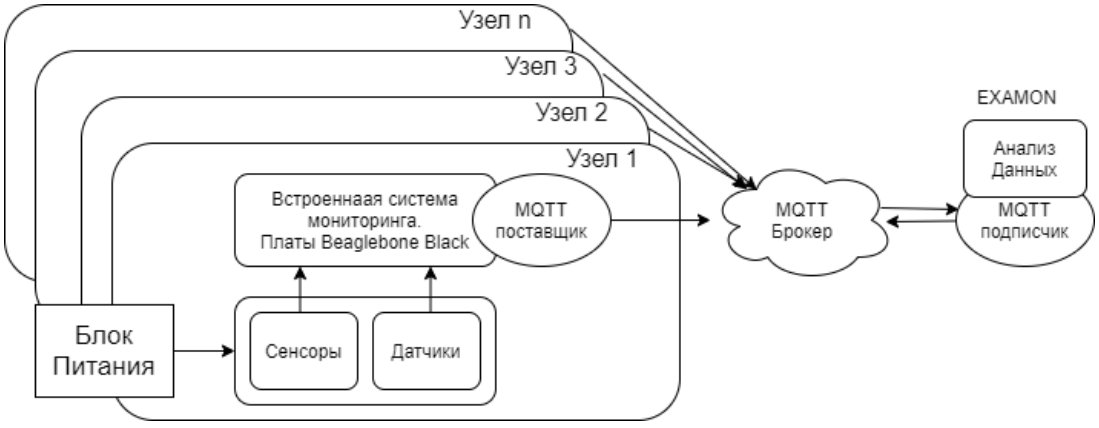


Рис. 2. Архитектура сбора телеметрической и формации суперкомпьютера D.A.V.I.D.E

Одна из проблем, которая возникает при работе с точными метриками системы – необходимость большого объема дискового пространства для хранения необработанных данных. Учеными из CINECA было принято решение хранить точные данные только в течении недели, а обобщенные данные – 7 месяцев.

Обучение и внедрение моделей

Для того, чтобы развернуть систему выявления аномалий на основе автокодировщиков, необходимо обучить и внедрить данные модели в уже существующую систему сбора телеметрических данных. Процесс внедрения моделей автокодировщиков в систему показан на рисунке 3.

Рис.3. Процесс внедрения модели нейронной сети в систему

Каждая плата, внедренная в узел суперкомпьютера, передает данные на сервер, на котором развернут основной компонент системы мониторинга Examon. Информация о состояниях узлов хранится в распределенной базе данных временных рядов KairosDB [7], построенной на основе базы данных NoSQL. Для каждой платы необходимо обучить свою модель нейронной сети на соответствующих ей данных из базы. При формировании набора данных для обучения важно провести их первичную обработку, например, удалить данные, которые относятся к периодам неправильного функционирования системы мониторинга. Во время нормальной работы системы ее метрики связаны определенными отношениями (например, температура процессора зависит от его охлаждения и нагрузки системы), которые прекращают действовать при возникновении аномальных ситуаций. Автокодировщик можно обучить распознаванию отношений между метриками при нормальной работе системы. Соответственно, любые изменения в данных связях будут означать наличие аномалий или отказов в системе.

Для обучения моделей разработчиками данной системы были сформированы 3 дата-сета для каждого узла на основе данных об их состоянии за период в 2 месяца. Первый дата-сет содержал данные о метриках во время нормальной работы системы и являлся тренировочным; второй и третий были использованы для тестирования ибыли собраны во время нормальной работы системы, а также во время внедрения в узлы аномальных явлений соответственно.

Тестирование и основные результаты

Для каждого набора данных были рассчитаны средний модуль отклонения и корень из среднего квадрата отклонения. Однако, чтобы точнее оценить данные метрики, было принято решения использовать их нормализованные значения (1-2):

$$NMAE_{D_{test}} = \frac{MAE_{D_{test}}}{MAE_{D_{train}}}, (1)$$

$$NRMSE_{D_{test}} = \frac{RMSE_{D_{test}}}{RMSE_{D_{train}}}, (2)$$

где D_{test}– один из наборов данных для тестирования,

D_{train}– набор данных для тренировки модели,

MAE – средний модуль отклонения,

RMSE – корень из среднего квадрата отклонения,

По результатам вычислений, средний NMAE по всем узлам для дата-сетов без аномалий - 1.08, для дата-сетов с аномалиями - 14.54; средний NRSME по всем узлам для дата-сетов без аномалий - 1.17, для дата-сетов с аномалиями – 11.18. Данные результаты доказывают, насколько сложно автокодировщику восстановить входные данные с аномалиями. Следующим шагом был выбор уровня

порога допустимой ошибки восстановления, при превышении которого состояние считается аномальным. Для определения порогового значения можно использовать стратегию, при которой в конечное число измерений вносят конечное число ошибок. Сформированный набор пропускают через нейронную сеть и вручную настраивают пороговое значение в зависимости от результатов. Данные эксперименты на суперкомпьютере D.A.V.I.D.E. показали, что для разных узлов пороговые значения, с помощью которых достигается максимальная точность определения ошибок, разные. Этот факт доказывает, что эффективнее обучить свою модель автокодировщика для каждого узла высокопроизводительной системы, чем использовать одну универсальную. Эффективность системы была оценена с помощью показателя F-меры, оценивающего точность классификатора. Результаты оценки работы автокодровщиков для некоторых узлов приведены в таблице 2.

Таблица 2

Значение F-меры для четырех узлов суперкомпьютера

Узел	Нормальное состояние	Аномальное состояние
17	0.97	0.89
19	0.97	0.90
29	0.97	0.92
45	0.97	0.75

Результаты работы системы определения аномалий достаточно высокие – минимальный результат F-меры продемонстрировано в узле 45 при определении аномальных состояний. Причиной для такого результата может служить некорректно выставленное значения порога определения аномалий. Остальные значения колеблются в пределах от 0.89 до 0.92.

Заключение

Использование нейронных сетей для определения аномалий в реальном времени в высокопроизводительных системах и суперкомпьютерах может предоставить администраторам возможность быстрого реагирования на сбои и отказы в их узлах без использования вычислительных ресурсов самих узлов системы. Пример использования автокодировщиков как способ определения аномалий в суперкомпьютере D.A.V.I.D.E. показал, что при правильной настройке параметров модели нейронной сети можно добиться высокой точности результатов данной задачи.

Литература

1. *Докучаев В.А., Кальфа А.А., Маклачкова В.В.* Архитектура центров обработки данных / Под ред. профессора В.А. Докучаева. М.: Горячая линия – Телеком, 2020. 240 с. ISBN 978-5-9912-0849-9
2. Supercomputer [Электронный ресурс] - https://www.ecmwf.int/en/computing/ our-facilities/supercomputer Дата обращения 03.04.2020
3. Nagios [Электронный ресурс] - https://www.nagios.com/solutions/log-monitoring/?__hstc=118811158.36c50c143f5634bd83d7ae62468a1120.1605343974275.1605343974275.1605343974275.1&__hssc=118811158.2.1605343974276&__hsfp=2776261183. Дата обращения 04.04.2020
4. MQTT - Universal protocol for cloud and IoT applications [Электронный ресурс] - http://new.hwg.cz/support/mqtt-universal-protocol-for-cloud-and-iot-applications. Дата обращения 04.04.2020
5. D.A.V.I.D.E. [Электронный ресурс] - https://www.e4company.com/en/2020/06/ d-a-v-i-d-e-a-top-500-project/. Дата обращения 05.04.2020
6. *Beneventi F., Libri A., Bartolini A., Benini L.* ExaMon: Exascale Holistic Monitoring. ANTAREX 2015. https://web.fe.up.pt/~specs/projects/antarex/ book/ExaMon.pdf.
7. KairosDB system properties [Электронный ресурс] https://db-engines.com/en/system/KairosDB. Дата обращение 07.04.2020.
8. *Докучаев В.А., Кальфа А.А., Мытенков С.С., Шведов А.В.* Анализ технических решений по организации современных центров обработки данных // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №6. С. 16-24.

APPLYING AUTOENCODERS FOR ANOMALY DETECTION TASKS IN SUPERCOMPUTERS AND HIGH-PERFORMANCE SYSTEMS

Kirill V. Simonov,
Graduate MTUCI, Moscow, Russia
kirillsimonov@yandex.ru
Sergey V. Shevelev,
Associate Professor Department of NITaS MTUCI, PhD., Moscow Russia
shevelev-s@yandex.ru

Keywords: *high-performancesystem, supercomputer, anomalydetection, supervisedmachine learning methods, unsupervised machine learning methods, autoencoder, classification.*

Current state of development of contemporary supercomputers and high-performance systems is presented. MQTT protocol principals of operation are outlined. Comparison between methods of supervised machine learning and unsupervised machine learning for anomaly detection is made. Principal of operation of autoencoder neural network model is shown. Description of telemetric data gathering system of D.A.V.I.D.E supercomputer is given. Process of learning and embedding neural network models in the nodes of supercomputer is depicted. Quantitative characteristics of performances of embedded autoencodersare presented.

ИСПОЛЬЗОВАНИЕ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ИЗУЧЕНИИ ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ

Туаева Екатерина Гургеновна,
студент МТУСИ, Москва, Россия
ktuaeva13@gmail.com
Фриск Валерий Владимирович,
доцент кафедры ТЭЦ МТУСИ, к.т.н., Москва, Россия
frisk@mail.ru

Ключевые слова: *свободное программное обеспечение, проприетарное программное обеспечение, электрические цепи, интеллектуальная собственность, лицензионное соглашение, LibreOffice, Scilab, QUCS.*

Проведено сравнение свободного и проприетарного программного обеспечения. Обосновывается необходимость использования в учебном процессе пакетов прикладных программ относящихся к свободному программному обеспечению (СПО). Производится выбор пакетов СПО для дисциплин кафедры теории электрических цепей. Даются рекомендации по применению пакетов СПО LibreOffice, Scilab и QUCS для оформления отчетов, выполнения расчетов и моделирования электрических цепей.

Компьютерные программы давно применяются для изучения электрических цепей, а при современной дистанционной форме обучения, это единственный и универсальный инструмент. Студенты используют программы исходя из их функциональности, наличия методического обеспечения, рекомендаций преподавателя и личного опыта. При этом, часто не обращают внимания на требования лицензионных соглашений по использованию этих программных продуктов, что может привести к негативным последствиям для пользователей. Поэтому необходимо проинформировать студентов о типах лицензий на программное обеспечение (ПО), об ответственности за нарушение лицензионных соглашений и предложить доступное для студентов бесплатное лицензионное свободное программное обеспечение, которое можно использовать при изучении электрических цепей (ЭЦ) для моделирования электрических цепей, выполнения расчетов и оформления отчетов по работам.

Нормативные правовые акты об авторском праве на программное обеспечение

В Российской Федерации действуют законы об авторском праве на программное обеспечение. В соответствии с пунктом 1 статьи 1225 Гражданского кодекса РФ (ГК РФ), программное обеспечение признаётся интеллектуальной собственностью, которая подлежит охране, а в соответствии с пунктом 1 статьи 1229 ГК РФ, правообладатель вправе использовать программное обеспечение по своему усмотрению любым не противоречащим закону способом. Другие лица не могут использовать ПО без согласия правообладателя. Правила использования ПО определяются договором – лицензионным соглашением.

Существуют различные виды нарушений лицензионных соглашений, связанные с использованием ПО.

1. Нарушения связаны с использованием нелицензионного ПО. В данном случае у пользователя нет ни одного законно приобретенного экземпляра ПО.

2. Пользователь выходит за пределы условий лицензионного соглашения по использованию ПО. Это может создавать видимость законного использования ПО, дает возможность получать обновления и техническую поддержку.

Ответственность за нарушение авторских прав на программное обеспечение

Не все знают, что за нарушение авторских прав на ПО организации, должностные лица и пользователи, по закону могут быть привлечены к ответственности: гражданско-правовой, административной, уголовной.

Уголовная ответственность наступает по статье 146 Уголовного кодекса РФ при ущербе от нарушения авторских прав на использование ПО более ста тысяч рублей. В соответствии с частью 2 статьи 146 УК РФ, за незаконное использование ПО предусмотрено наказание – штраф в размере до двухсот тысяч рублей, либо исправительные работы на срок до двух лет, либо лишение свободы на срок до двух лет.

Те же действия совершенные группой лиц либо лицом с использованием своего служебного положения, наказываются лишением свободы на срок до шести лет со штрафом в размере до пятисот тысяч рублей. По статье 146 УК РФ за незаконное использование ПО в организации привлекаются лица, которые принимают это решение – руководители организации или подразделений. Другие должностные лица привлекаются за незаконное использование ПО, если они участвуют в принятие решения об использовании ПО.

При ущербе менее ста тысяч рублей, наступает административная ответственность по статье 7.12 Кодекса РФ об административных правонарушениях, в которой предусмотрены штрафы: для граждан - до 2 тыс. руб., для должностных лиц - до 20 тыс. руб., для организаций - до 40 тыс. руб. При этом предусмотрена конфискация ПО и компьютерной техники.

Привлечение правонарушителя к административной или к уголовной ответственности за нарушение авторских прав на ПО не исключает возможности одновременного привлечения к гражданско-правовой ответственности, которая носит имущественный характер, направлена на компенсацию ущерба потерпевшей стороны и применяется по её требованию.

Кроме того необходимо знать, что использование ПО с нарушениями лицензионного соглашения: не гарантирует, надежной и бесперебойной работы; не позволяет рассчитывать на своевременное обновление и техническую поддержку; подвергает риску заражения компьютерными вирусами; приводит к прекращению гарантийных обязательств на компьютерную технику.

Таким образом, совершенно очевидно, что для обучения надо использовать только лицензионное программное обеспечение.

Виды лицензий на программное обеспечение

В настоящее время существуют разные виды лицензий на программное обеспечение.

Программное обеспечение, которое является частной собственностью правообладателей и имеет ряд ограничений по использованию, называется проприетарным. Проприетарное программное обеспечение подразделяется на платное проприетарное программное обеспечение и бесплатное проприетарное программное обеспечение. Компании-разработчики проприетарного программного обеспечения составляют собственные лицензионные соглашения.

Ограничения лицензий проприетарного ПО:

1.Ограничение на коммерческое использование.

ПО которое разрешается использовать бесплатно в некоммерческих целях частными лицами, медицинскими и учебными заведениями, некоммерческими организациями, но может требоваться оплата в случае использования в коммерческих целях.

2.Ограничение на распространение.

Этот вид ограничений сопровождает обычно крупные программные проекты, когда правообладатель требует оплату за каждый экземпляр программы. Обычно с таким ограничением продаются программы для профессионального использования большим числом пользователей.

3.Ограничение на изучение, модификацию.

Этот вид ограничения используется в ПО с закрытыми исходными кодами и может запрещать или ограничивать любое изменение программного кода.

В отличие от проприетарного, свободное ПО не имеет таких лицензионных ограничений и распространяется под стандартной свободной лицензией - GNU General Public License (GPL). Определение свободного программного обеспечения дано в ГОСТ Р 54593-2011 [19].

GPL лицензии на свободное программное обеспечение позволяют пользователям: использовать ПО в любых не противоречащих закону целях; изучать, адаптировать и вносить изменения в ПО; распространять копии ПО.

Выбор программного обеспечения для изучения электрических цепей

В таблице 1 даны результаты сравнения проприетарного программного обеспечения, которое традиционно широко используется при изучении ЭЦ и свободного ПО, которое предлагается внедрять в учебный процесс и рекомендовать для использования студентам.

Таблица 1

Программное обеспечение для изучения электрических цепей

№	Наименование ПО	Тип лицензии	Платное/ бесплатное	Операционная система	Адрес официального сайта разработчика ПО
1.	Программное обеспечение для оформления работ по электрическим цепям				
1.1	Microsoft Office	Проприетарное	платное	Windows	https://www.microsoft.com
1.2	LibreOffice	Свободное ПО	бесплатное	Windows Linux	https://www.libreoffice.org
2.	Программное обеспечение для расчетов электрических цепей				
2.1	MatLab	Проприетарное	платное	Windows Linux	https://www.mathworks.com
2.2	MathCad	Проприетарное	платное	Windows	https://www.mathcad.com
2.3	Scilab	Свободное ПО	бесплатное	Windows Linux	https://www.scilab.org
3.	Программное обеспечение для моделирования электрических цепей				
3.1	Simulink	Проприетарное	платное	Windows Linux	https://www.mathworks.com
3.2	Micro-Cap	Проприетарное	бесплатное	Windows	http://www.spectrum-soft.com
3.3	QUCS	Свободное ПО	бесплатное	Windows Linux	http://qucs.sourceforge.net

Программное обеспечение, представленное в таблице 1, объединено в группы: ПО для оформления работ; ПО для расчетов; ПО для моделирования.

Для сравнения используются следующие характеристики ПО: типы лицензий - проприетарные или свободные; стоимость лицензий - платные или бесплатные; операционные системы, на которых функционирует ПО -Windows или Linux.

Кроме того, надо учитывать фундаментальные преимущества использования СПО:
передача прав и исходных кодов достаточных для обеспечения жизненного цикла; совместимость с открытыми стандартами; возможность создания инфраструктуры разработки отечественного ПО.

В Российской Федерации создан Единый реестр российских программ для электронных вычислительных машин и баз данных [18]. Большинство российских операционных систем (ОС), занесенных в этот реестр, разработаны на основе СПО Linux, поэтому прикладное СПО, приведенное в таблице 1, присутствует и в российских репозиториях и функционирует на российских программных платформах, например в российском репозитории Сизиф [20].

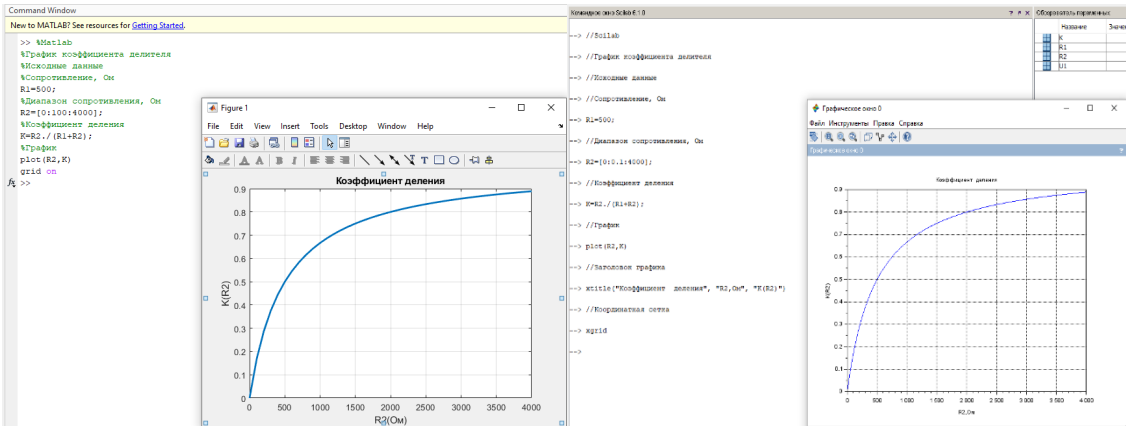
С учетом приведенной выше информации, выбрано ПО из таблицы 1 для использования студентами при изучении ТЭЦ [1, 2, 6, 7]:

- Свободное ПО LibreOffice, Scilab и QUCS, функционирующее под ОС Windows и Linux.
- Проприетарное, бесплатное ПО Micro-Cap, функционирующее под ОС Windows. Так как для этого ПО изданы учебные пособия по всем разделам ЭЦ [3-5,13].

Назначение программного обеспечения для изучения электрических цепей

Для оформления работ по ЭЦ выбрано СПО LibreOffice, которое содержит текстовый и графический редакторы, позволяет работать с электронными таблицами, презентациями, базами данных и редактировать формулы. Основным форматом файлов является открытый международный формат Open Document, поддерживаются другие широко распространенные форматы: doc, docx, txt, ppt, pptx и другие. СПО LibreOffice доступно на официальном сайте разработчика [17].

Для расчетов по ЭЦ выбрано СПО Scilab, которое позволяет выполнять математические операции для инженерных и научных целей. В СПО Scilab доступна возможность конвертации скриптов формата MATLAB в скрипты собственного формата, но использовать это сложно ввиду большого количества различных ограничений. Для выполнения расчетных заданий по ЭЦ на СПО Scilab полезно использовать подробные методические рекомендации по проведению расчетов ЭЦ, которые даны в учебных пособиях ориентированных на MATLAB [8-12, 20-23]. На рисунке 1 приведен пример выполнения расчета делителя напряжения в MATLAB и Scilab. СПО Scilab доступно на официальном сайте разработчика [15].



а) б)

Рис. 1. Пример выполнения расчета делителя напряжения в MATLAB (а) и Scilab (б)

Для моделирования ЭЦ предложено продолжить использовать проприетарное ПО Micro-Cap, которое позволяет производить аналоговое и цифровое моделирование ЭЦ. ПО Micro-Cap доступно на официальном сайте разработчика [14]. Следует подчеркнуть, что ПО Micro-Cap распространяется бесплатно, давно и успешно используется студентами, доступны учебные пособия для выполнения практикума по ЭЦ [3-5,13].

Для моделирования ЭЦ выбрано СПО QUCS, которое по функциональным возможностям аналогично ПО Micro-Cap. СПО QUCS доступно на официальном сайте разработчика [16]. На начальном этапе внедрения СПО QUCS в учебный процесс, можно использовать задания и прядок выполнения практикумов из существующих учебных пособий ориентированных на применение ПО Micro-Cap [3-5,13].

Сформулированные выше предложения по использования СПО, были успешно проверены при выполнении практикумов по ЭЦ. В соответствии с методическими указаниями из учебных пособий по ЭЦ [3-5,13], были выполнены пять практикумов по ЭЦ на СПО QUCS (моделирование ЭЦ) и СПО Scilab (расчеты ЭЦ):

- Компьютерный анализ делителя напряжений.
- Компьютерный анализ характеристик RC - цепи.
- Исследование нелинейных цепей при гармонических воздействиях.
- Исследование характеристик источников напряжения и тока.
- Моделирование переходных процессов в цепях первого порядка.

Заключение

Основные результаты, выводы и рекомендации по использованию свободного программного обеспечения при изучении электрических цепей:

1. Использование только СПО при изучении ЭЦ возможно и не потребует дополнительных затрат на лицензии на программное обеспечение.
2. Для оформления работ по ЭЦ можно использовать СПО LiberOffice, которое поддерживает все основные форматы данных ПО Microsoft Office.
3. Для расчетов ЭЦ надо использовать СПО Scilab, вместо проприетарного и платного ПО MATLAB. Для методической поддержки перехода на СПО, можно использовать существующие учебные пособия по расчетам ЭЦ, ориентированные на ПО MATLAB.
4. Для моделирования ЭЦ надо использовать СПО QUCS. Для ускорения внедрения СПО QUCS в учебный процесс, можно применять разработанные методические указания для практикумов с использованием бесплатного проприетарного ПО Micro-Cap.
5. Возможность использования СПО QUCS и СПО Scilab студентами для изучения ЭЦ, была продемонстрирована на примере выполнения пяти практикумов по основам ЭЦ.
6. Комплект СПО для изучения электрических цепей может работать под управлением операционных систем Windows и Linux. СПО предъявляет минимальные требования к быстродействию процессора, объемам оперативной и дисковой памяти компьютера.
7. СПО LiberOffice, QUCS и Scilab присутствует в репозиториях отечественных операционных систем, созданных на основе СПО Linux и занесенных в реестр российского ПО, поэтому использование данного комплекта СПО для изучения ЭЦ, можно считать импортозамещением и началом внедрения в учебный процесс отечественного свободного программного обеспечения.

Литература

1. *Фриск В.В.* Основы теории цепей. М.: РадиоСофт, 2002. 288 с.
2. *Смирнов Н.И., Фриск В.В*. Теория электрических цепей: конспект лекций. М.: Горячая линия – Телеком, 2016. 270 с.
3. *Фриск В.В., Логвинов В.В.* ОТЦ, ОС, РПрУ. Лабораторный практикум на персональном компьютере. М.: СОЛОН-Пресс, 2008. 608 с.
4. *Фриск В.В., Логвинов* В.В. РПрУСМСВ и РПрУСРС и РД, Лабораторный практикум II на персональном компьютере. М.: СОЛОН-Пресс, 2011. 656 с.
5. *Фриск В.В. Логвинов В.В.* ТЭЦ. СТУ, РПрУСМСВ и РПрУСРС и РД, Лабораторный практикум III на персональном компьютере. М.: СОЛОН-Пресс, 2016. 480 с.
6. *Смирнов Н.И., Фриск В.В.* Теория электрических цепей. Учебник для вузов, М.: Горячая линия - Телеком, 2019. 286 с.
7. *Шакин В.Н., Семенова Т.И., Фриск В.В.Базовые* средства математического пакета Scilab.Учебник для вузов. М.: Горячая линия – Телеком, 2019. 338 с.
8. *Фриск В.В., Ганин В.И., Степанова А.Г.* Компьютерный анализ переходных процессов в электрических цепях с помощью MATLAB. М.: СОЛОН-ПРЕСС, 2019. 41 с.
9. *Фриск В.В., Ганин В.И., Степанова А.Г.* Компьютерный анализ и моделирование электрических цепей постоянного тока в среде MATLAB. М.: СОЛОН-ПРЕСС, 2020. 32 с.
10. Российский разработчик операционных систем Базальт СПО. Официальный сайт. URL https://www.basealt.ru.
11. *Фриск В.В., Ганин В.И., Степанова А.Г.,* Применение пакета MATLAB и SIMULINK для анализа электрических цепей. Том 1. М.: СОЛОН-ПРЕСС, 2020. 400 с.
12. *Фриск В.В., Ганин В.И., Степанова А.Г.,* Применение пакета MATLAB и SIMULINK для анализа электрических цепей. Том 2. М.: СОЛОН-ПРЕСС, 2020. 276 с.

13. *Кузнецов В. В.* Симулятор электронных схем с открытым исходным кодом Qucs: основные возможности и основы моделирования, Компоненты и технологии, 2015. No.3 (164). С. 114-120.

14. Программное обеспечение Micro-Cap. Официальный сайт. URL http://www.spectrum-soft.com.

15. Программное обеспечение Scilab. Официальный сайт. URL https://www.scilab.org.

16. Программное обеспечение QUCS. Официальный сайт. URL http://qucs.sourceforge.net.

17. Программное обеспечение LibreOffice. Официальный сайт. URL https://www.libreoffice.org.

18. Единый реестр российских программ для электронных вычислительных машин и баз данных. URL- https://reestr.minsvyaz.ru.

19. ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.

20. *Фриск В.В.* 3D электрические монстры в электрических цепях // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 8. С. 32-36.

22. *Кухтенко В.Ф., Фриск В.В.* Использование системы компьютерного моделирования matlab и Simulink в лабораторной работе "Исследование пассивных цепей при гармоническом воздействии на постоянной частоте" // Телекоммуникации и информационные технологии. 2016. Т. 3. № 1. С. 64-66.

23. *Фриск В.В*. Исследование беспроводной технологии передачи электричества // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 7. С. 29-32.

24. *Фриск В.В.* Применении к задачам теории электрических цепей расширения понятия действительных чисел // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 3. С. 36-40.

USING FREE SOFTWARE IN THE STUDY OF ELECTRICAL CIRCUITS

Ekaterina G. Tuaeva,
Student MTUCI, Moscow, Russia
ktuaeva13@gmail.com
Valery V. Frisk,
Associate professor of TEC Department MTUCI, PhD., Moscow, Russia
frisk@mail.ru

Keywords: *free software, proprietary software, electrical circuit, intellectual property, license agreement, LibreOffice, Scilab, QUCS.*

The article compares free and proprietary software. The necessity of using free software application packages in the educational process is justified. The choice of GNU GPL packages for the disciplines of the Department of electrical circuit theory is made. Recommendations are given for using the LibreOffice, Scilab and QUCS software packages for creating reports, performing calculations, and modeling electrical circuits.

ВЛИЯНИЕ ФРАКТАЛЬНОЙ РАЗМЕРНОСТИ НА КАЧЕСТВО БИНАРНОЙ КЛАССИФИКАЦИИ СЕТЕВЫХ АНОМАЛИЙ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

Шелухин Олег Иванович,
заведующий кафедрой ИБ МТУСИ, д.т.н., профессор, Москва, Россия
o.i.shelukhin@mtuci.ru
Кажемский Михаил Андреевич,
аспирант кафедры ИБ МТУСИ, Москва, Россия
m.kazhemskiy@gmail.com

Ключевые слова: *классификация, фрактальная размерность; показатель Херста; атрибуты; обучение, тестирование; метрики; алгоритмы; аномалии; атаки*

Проведенный анализ показал, что для решения задач информационной безопасности целесообразно использовать фрактальный анализ, показывающий, что аномальный пакетный трафик за определенный период времени может значительно изменить функции самоподобия в процессе трафика. Для построения эффективной системы сетевой защиты перспективным направлением является совместное использование фрактального и интеллектуального анализа данных. В результате задача обнаружения сетевых аномалий сводится к бинарной классификации с целью отнесения рассматриваемого временного ряда к одному из двух классов {«отсутствие атаки», «присутствие атаки»}. Представлены результаты проведенного фрактального анализа атак набора данных NSL-KDD R/S-методом и нормального трафика показывающие, что фрактальная размерность может использоваться в качестве дополнительно признака классификации. Показано, что добавление в число атрибутов дополнительного параметра, характеризующего фрактальную размерность атак, положительно влияет на эффективность бинарной классификации и справедливо для всех алгоритмов, представленных в исследовании. В наибольшей степени введение дополнительного атрибута оказывает влияние на алгоритмы, основанные на «деревьях» - *Decision Tree Classifier*, *Random Forest и* A*da Boost.* Для этих алгоритмов введение данного параметра значительно улучшает качество классификации.

Введение

Учитывая все возрастающий размер информационных сетей спрос клиентов на сетевой бизнес быстро растет. При этом все больше и больше уязвимостей систем безопасности обнаруживаются и постоянно используются хакерами [1, 2]. Сетевые аномалии могут возникать вследствие перегрузок, ошибок сетевых устройств, DDoS-атак, попыток несанкционированного доступа. Все эти факторы затрудняют управление сетевой безопасностью. Отслеживание сетевого трафика и обнаружение аномалий в реальном времени имеет важное значение для повышения надежности и доступности сети [1,6]. Статистический анализ измерений показывает четкое присутствие фрактальных, или самоподобных свойств сетевого трафика в компьютерной сети.

В работах [3,4] для решения задач информационной безопасности используются фрактальный анализ. В работе [5] приведены результаты исследований обнаружения скачков мультифрактальных размерностей, вызванных аномальными изменениями свойств телекоммуникационного трафика в реальном (текущем) масштабе времени.

Особенностью фрактального анализа является выявление самоподобия, что позволяет отнести временной ряд к заранее определенной модели, вскрыть особенности локальной структуры и выявить различные свойства, невидимые при обычном представлении в режиме реального времени.

Для построения эффективной системы сетевой защиты перспективным направлением является совместное использование фрактального и интеллектуального анализа данных. В результате задача

обнаружения сетевых аномалий сводится к бинарной классификации с целью отнесения рассматриваемого временного ряда к одному из двух классов {«отсутствие атаки», «присутствие атаки»}.

Учитывая, что свойство самоподобия наблюдается в широких временных масштабах, наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика. Для оценки степени самоподобия используются понятия фрактальной размерности множества (по Хаусдорфу) *D* и показатель Херста *H*, характеризующий степень самоподобия процесса, которые связаны между собой соотношением*: D = 2 – H*. В подавляющем большинстве работ в области телекоммуникаций для обнаружения аномалий сетевого трафика используется показатель Херста.

В отличие от известных работ в статье предлагается использовать для обнаружения сетевых атак методы машинного обучения в которых в качестве одного из признаков (атрибутов) бинарной классификации используется фрактальная размерность (показатель Херста) сетевого трафика при наличии и отсутствии аномалий трафика (атак) .

Постановка задачи

Для решения задачи защиты телекоммуникационного трафика информационных систем проводится его анализ с целью определения наличия или отсутствия сетевых атак. В результате задача сводится к задаче бинарной классификации с целью отнесения рассматриваемого временного ряда к одному из двух классов {«отсутствие атаки», «присутствие атаки»}. Рассмотрим классическую постановку задачи бинарной классификации [6].

Дано множество $\boldsymbol{X}$, в котором хранится описание объектов $\boldsymbol{o}$. $\boldsymbol{Y}$ – конечное множество классов. Классификатором $\boldsymbol{F}$ является отображение $\boldsymbol{X}$ в множество $\boldsymbol{Y}$, т.е. $\boldsymbol{F: X \to Y}$. Признак (атрибут) $\boldsymbol{f}$ объекта $\boldsymbol{o}$ – это отображение $\boldsymbol{f: o \to D_f}$, где $\boldsymbol{D_f}$–множество допустимых значений признака $\boldsymbol{f}$. Если задан набор признаков $\boldsymbol{f_1, \dots, f_m}$ для некоторого объекта $\boldsymbol{o}$, то вектор признаков $\boldsymbol{x}$ объекта $\boldsymbol{o \in X}$ может быть определен как $\boldsymbol{x = f_1(o), \dots, f_m(o)}$. Классификатор $\boldsymbol{F}$ должен быть способен классифицировать произвольный объект $\boldsymbol{o \in X}$.

Для обучения классификатора $\boldsymbol{F}$ используется обучающая выборка, заданная множеством $\boldsymbol{D} = \{(x_1, y_1), \dots, (x_v, y_v)\}, y_r \in \boldsymbol{Y} = \{0; 1\}, r = \overline{1, v}$.

Оптимальным считается классификатор, который дает наименьшую вероятность ошибки $\boldsymbol{P(x)}$ при всех допустимых значениях $\boldsymbol{x}$. Тогда критерием оптимальности будет $\boldsymbol{P(x) \to \min_{x \in X}}$.

Следует отметить, что ошибки разделяются на «ошибки 1-го рода» (False Positive — ложно положительные события) и «ошибки 2-го рода» (False Negative — ложно отрицательные события).

Алгоритмы и метрики классификации

Для классификации набора данных были использованы следующие алгоритмы классификации [20]:

- ***Метод k-ближайших соседей*** (k-Nearest Neighbors, neighbors, ***kN***). Использовался *нормализованный* набор данных.
- ***Множественная логистическая регрессия*** (Logictic Regression, ***LR***). Для решения уравнения логистической регрессии использовался алгоритм SAGA. Использовался *нормализованный* набор данных.
- ***Мультиномиальный Наивный Баиес*** (*Multinomial Naive Bayes*, ***NB***). Использовался *нормализованный* набор данных.
- ***Метод опорных векторов*** (Support Vector Machines, SVM, **VM**). Для исследуемого набора данных применялось ядро *радиальной базисной функции* ($k(x, x') = e^{(-\gamma \|x - x'\|^2)}$) с параметром $\gamma = 2$. Использовался *нормализованный* набор данных.
- ***Дерево решений (****Decision Tree Classifier,* ***DTC***). В качестве оценочной функции использовался коэффициент неопределенности Gini. *Нормализация* данных *не требуется*. В ходе эмпирического анализа было выяснено, что лучший результат алгоритма достигаются при *количестве признаков 28* и *глубине дерева 23*.

- ***Случайный лес (****Random Forest* **- *RF)***. Из-за того, что основой алгоритма является дерево решений, *нормализация не требуется.* Наилучший результат для рассматриваемого набора данных был получен при разбивке данных на 100 подвыборок.
- ***Ada Boost (AB)***. Из-за того, что основой алгоритма является дерево решений, *нормализация не требуется.* Наилучший результат для рассматриваемого набора данных был получен при разбивке данных на 1000 подвыборок.

В задачах машинного обучения наиболее часто используются следующие метрики для оценки эффективности построенных моделей: точность (*precision*), полнота (*recall*), F-мера (*F-score*), ROC-кривые (*Receiver Operating Characteristic curve – кривая ошибок*), AUC-ROC и AUC-PR (*Area Under Curve -площадь под кривой ошибок и площадь по кривой pricison-recall*)

После проведения классификации возможно получение четырёх видов результатов: TP (True Positive — истинно положительный), TN (True Negative — истинно отрицательный), FP (False Positive — ложно положительный), FN (False Negative — ложно отрицательный). Эти результаты можно представить в виде матрицы ошибок (*confusion matrix*) .

Набор данных

Системы обнаружения вторжений (СОВ) являются важным компонентом компьютерной безопасности предназначенными для обнаружения атак. Для создания эффективных моделей обнаружения алгоритмы обычно требуют большого количества помеченных данных. Одной из основных трудностей при развертывании СОВ является необходимость маркировки исходных данных на «нормальная» или «атака». Широкое распространение получил набор данных для оценки СОВ под названием DARPA , включающий в себя широкий спектр атак, используется для обучения и тестирования СОВ.

В работе использовался набор данных DARPA 1998, в котором весь сетевой трафик, включая всю полезную нагрузку каждого пакета, был записан в формате tcpdump. Тестовая сеть состояла из смеси реальных и моделируемых машин; фоновый трафик искусственно создавался реальными и имитированными машинами, атаки осуществлялись против реальных машин.

В обучающие данные DARPA 1998 было включено 24 типа атак, и еще 14 новых атак были добавлены к тестовым данным, для сравнения производительности СОВ для «известных» и «неизвестных» атак. Каждый тип атаки, описанных в DARPA 1998 относится к одной из четырех следующих основных категорий, представленных в таблице 1:

Таблица 1

Классы и типы сетевых атак в DARPA

Класс атаки	Тип атаки
Probe	portsweep, ipsweep, queso, satan, msscn, ntinfoscan, lsdomain, illegal-sniffer
DoS	apache2, smurf, neptune, dosnuke, land, pod, back, teardrop, tcpreset, syslogd, crashiis, arppoison, mailbomb, selfping, processtable, udpstorm, warezclient
R2L	dict, netcat, sendmail, imap, nsftp, xlock, xsnoop, sshtroyan, framespoof, ppmacro, guest, netbus, snmpget, ftpwrite, httptunnel, phf, named
U2R	sechole, xtern, eject, ps, nukepw, secret, perl, yaga, fdformat, ffbcongig, casesen, ntfsdos, ppmacro, loadmodule, sqlattack

Атаки отказа в обслуживании или ***DoS*** атака, имеют цель ограничение или отказ в предоставлении услуг пользователю, компьютеру или сети с помощью сильной перегрузки системы, таким как поток SYN.

Probe или зондирование - категория атак, где злоумышленник исследует сеть, чтобы собрать информацию или обнаружить известные уязвимости, например, сканирование портов.

Remote to Local (R2L) атаки имеют цель заполучить локальный доступ к компьютеру или сети, к которой злоумышленник ранее имел удаленный доступ. Примером является попытка получить контроль над учетной записью пользователя.

Целью ***User to Root*** атаки (U2R) является получение доступа с правами root или суперпользователя на конкретном компьютере или системе, с которой злоумышленник ранее имел доступ на уровне пользователя. Это попытки непривилегированного пользователя получить административные права (например, Eject).

В наборе данных каждая запись промаркирована, и, если эта запись соответствует вредоносному трафику, то ей присваивается определенный тип атаки. Всего представлено 22 основных типа атак, 18 дополнительных типов (не указанных в документации), нормальный и неизвестный трафик – итого **41** различные **метки** каждой записи.

Каждая запись включает в себя поля, информационные признаки, описанные в *Таблице 2.* Если обозначить каждую метку записи как класс, то каждый признак можно назвать *атрибутом* этого класса.

Таблица 2

Описание признаков набора данных NSL-KDD

	Признак	**Описание**	**Тип**
Данные TCP соединения			
1	duration	Продолжительность сессии, сек	числовой
2	protocol_type	Тип протокола (TCP, UDP и т.д.)	символьный
3	service	Удаленный сервис (http, telnet и т.д.)	символьный
4	flag	Статус соединения (normal или error)	символьный
5	src_bytes	Количество исходящих байт (источник -> назначение)	числовой
6	dst_bytes	Количество входящих байт (назначение -> источник)	числовой
7	land	1, если подключен с того же хоста/порта, по умолчанию – 0.	числовой
8	wrong_fragment	Количество «неправильных» пакетов	числовой
9	urgent	Количество срочных пакетов	числовой
Данные домена			
10	hot	Количество «hot» индикаторов	числовой
11	num_failed_logins	Количество неудачных авторизаций	числовой
12	logged_in	1 при успешной авторизации, 0 – по умолчанию	числовой
13	num_compromised	Количество «скомпрометированных» условий	числовой
14	root_shell	1, если вход выполнен под root, 0 – по умолчанию	числовой
15	su_attempted	1, если была попытка входа под root, 0 – по умолчанию	числовой
16	num_root	Количество доступов суперпользователя	числовой
17	num_file_creations	Количество операций по созданию файла	числовой
18	num_shells	Количество сессий терминала	числовой
19	num_access_files	Количество операций по доступу к файлам	числовой
20	num_outbound_cmds	Количество исходящих команд в ftp сессии	числовой
21	is_host_login	1, если логин в списке «hosts», 0 – по умолчанию	числовой
22	is_guest_login	1, если логин гостевой, 0 – по умолчанию	числовой
Данные посчитанные в двухсекундном окне			
23	count	Количество подключений на один хост в рамках текущей сессии за последние 2 секунды	числовой
24	srv_count	Количество подключений к одному сервису в рамках текущей сессии за последние 2 секунды	числовой
25	serror_rate	% от подключений с «SYN» ошибкой	числовой
26	srv_serror_rate	% от подключений с «SYN» ошибкой при подключении на один сервис	числовой
27	rerror_rate	% от подключений с «REJ» ошибкой	числовой
28	srv_rerror_rate	% от подключений с «REJ» ошибкой при подключении на	числовой

		один сервис	
29	same_srv_rate	% от подключения к одному и тому же сервису	числовой
30	diff_srv_rate	% от подключения к разным сервисам	числовой
31	srv_diff_host_rate	% от подключения к разным хостам	числовой
Данные посчитанные в сто секундном окне			
32	dst_host_count	Количество подключений на один хост в рамках текущей сессии за последние 100 секунд	числовой
33	dst_host_srv_count	Количество подключений на один сервис в рамках текущей сессии за последние 100 секунд	числовой
34	dst_host_same_srv_rate	% от подключения к одному и тому же сервису	числовой
35	dst_host_diff_srv_rate	% от подключения к разным сервисам	числовой
36	dst_host_same_src_port_rate	% от подключение с одного и того же порта источника	числовой
37	dst_host_srv_diff_host_rate	% от подключения к одному и тому же хосту	числовой
38	dst_host_serror_rate	% от подключений с «SYN» ошибкой	числовой
39	dst_host_srv_serror_rate	% от подключений с «SYN» ошибкой при подключении на один сервис	числовой
40	dst_host_rerror_rate	% от подключений с «REJ» ошибкой	числовой
41	dst_host_srv_rerror_rate	% от подключений с «REJ» ошибкой при подключении на один сервис	числовой
42	**hersts**	**фрактальная размерность**	**числовой**

Выделение атаки осуществлялось на основе экспериментальных данных, в которых указано время начало атаки и введен интервал времени, в котором она наблюдалась. Полученный результат преобразовывался в виде интенсивности пакетов. В качестве примера на рисунке 1 представлен нормальный трафик, сформированный из исходных данных DARPA 1998 и содержащий 34070 выборок в виде интенсивности пакетов.

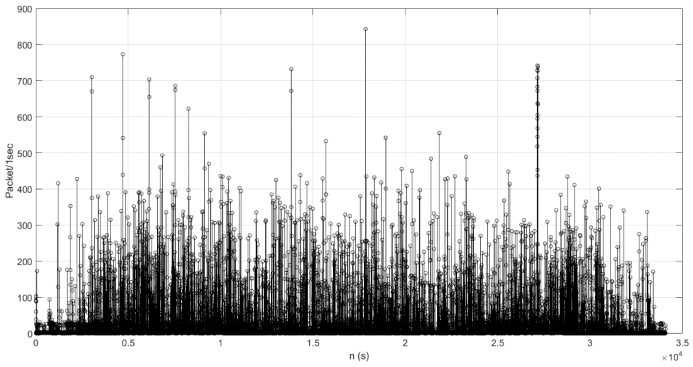


Рис. 2. Тестовый нормальный трафик

Атаки группируются по четырем классам: DoS, Probe, R2L, U2R. Результаты объединения по классам атак можно наблюдать на рисунках 3 в виде последовательности дискретных значений. При бинарной классификации й все типы атак, приведенные в таблице 1, объединялись в один класс под названием ***attack***. В качестве альтернативного класса рассматривался нормальный трафик (в отсутствие атак) под названием – ***normal***

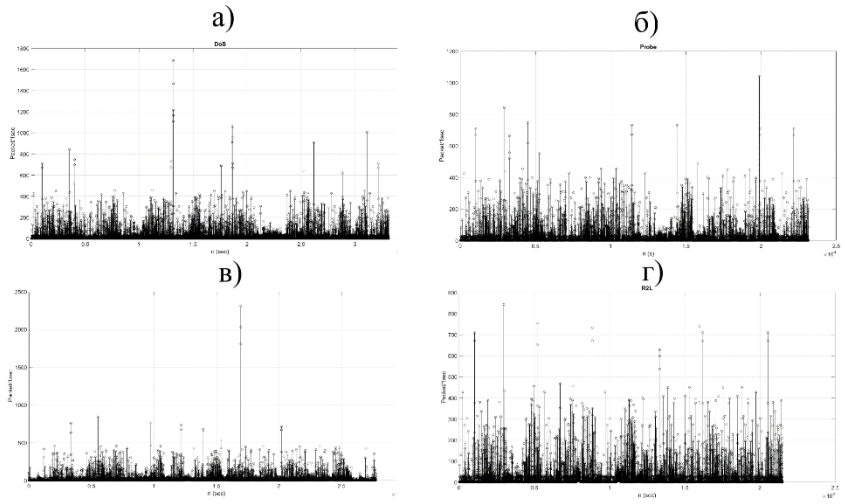


Рис. 3. Экспериментальный трафик с атаками: а): DoS; б) Probe; В) R2L, Г) U2R

Оценка фрактальной размерности атак

На основе исходных данных DARPA 1998, был составлен набор данных KDD'99 [22]. В результате оптимизации набора KDD'99 был получен набор NSL-KDD 2014 . Многоклассовая классификация атак в данном наборе рассматривалась в работе [7]. В результате данной работы был сделан вывод о том, что классы r2l и u2r определяются плохо и требуются дополнительные манипуляции над исходным набором данных или приведение к ***бинарной классификации***. Для повышения эффективности бинарной классификации этого набора предлагается ввести дополнительный признак (атрибут) для каждого из типа атак . В качестве такого атрибута предлагается использовать фрактальную размерность [4,5].

Оценка фрактальной размерности ***D*** или *показателя Херста* ***H*** зависит от многих факторов, и сама по себе является сложной задачей, поскольку при работе в реальных условиях всегда имеются ограничения, связанные конечным набором данных. Наиболее часто для оценки показателя Херста используются анализ нормированного размаха (R/S-метод), анализ графика изменения дисперсии и вейвлет-анализ [1,2].

Нормированная безразмерная мера, способная описывать изменчивость временного ряда, названа нормированным размахом (R/S). Для заданного набора наблюдений со средним – , где – количество наблюдений, вводится понятие размаха (разности между максимальным и минимальным отклонением , где

– .

Известно, что для многих природных явлений математическое ожидание нормированного размаха примерно равно при , где – положительная константа, не зависящая от . Тогда показатель можно получить, изобразив график зависимости —— от , и, используя полученные точки, подобрать по методу наименьших квадратов прямую линию с наклоном [7]. С целью определения количественного значения H используется эмпирический закон в виде

– – .

Результаты проведенного фрактального анализа атак, представленных в *таблице 1* R/S-методом и нормального трафика в отсутствие атак приведены в *таблице 3*. В таблице 3 представлены результаты оценки параметра Херста для атак DoS, U2R, R2L и Probe .

Представленные в таблице 3 данные были использованы в качестве дополнительного признака классификации под названием hersts- фрактальная размерность и помещены под номером 42 в таблицу №2 признаков классификации. В таблице 2 было добавлено среднее значение показателя Херста для

того или иного типа атаки. Для случая, когда этот параметр не был рассчитан (например, в силу малой длительности атаки), проставлялось значение равное 0.

Таблица 3

Параметр Херста для атак *DoS, U2R, R*2L, *Probe* и нормального трафика *normal*

	Номер наблюдения			
Тип атаки	**1**	**2**	**3**	среднее значение H
dos				
pod	0,6347	0,6094		**0,6221**
teardrop	0,6251	0,6632		**0,6442**
syslog	0,6678	0,6382	0,7190	**0,6750**
back	0,6934			**0,6934**
land	0,7013			**0,7013**
smurf	0,6859	0,3885	0,6029	**0,5591**
neptune	0,6357			**0,6357**
u2r				
ffb	0,6378	0,7143	0,6373	**0,6631**
loadmodule	0,5778	0,6963		**0,6371**
pearlmagic	0,5462	0,7339		**0,6401**
eject	0,6394	0,6721	0,6741	**0,6619**
format	0,6332	0,7051		**0,6692**
rootkit	0,7363			**0,7363**
r2l				
imap	0,5837	0,5468	0,6177	**0,5827**
ftp-write	0,6982			**0,6982**
guest	0,5504			**0,5504**
spy	0,5330	0,6859	0,6859	**0,6349**
multihop	0,6468	0,5999	0,6468	**0,6312**
warezmaster	0,6052	0,5713	0,7476	**0,6414**
probe				
nmap	0,5870	0,5713		**0,5792**
satan	0,6982	0,6859		**0,6921**
ipsweep	0,5504	0,6859		**0,6182**
portsweep	0,5330	2 x 0,6468	0,5999	**0,6066**
normal				
normal				**0,5887**

Значимость представленных в таблице 2 атрибутов атак полученная с помощью алгоритма RF можно оценить по гистограмме, приведенной на рисунке 4.

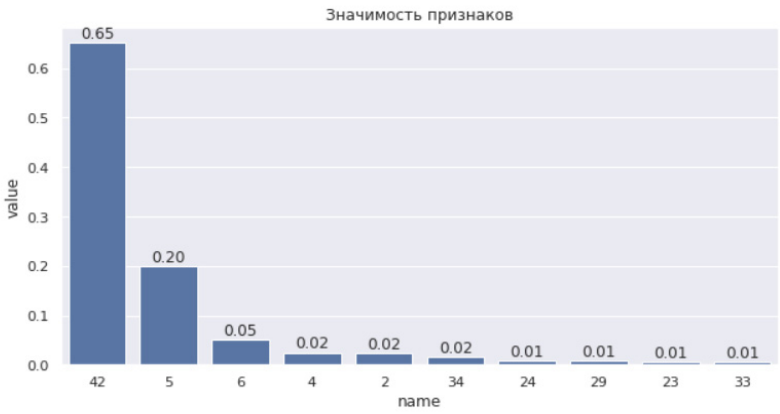


Рис. 4. Значимость наиболее значимых признаков для алгоритмов типа *« Дерево решений».*

Как видно из рисунка 4 – параметр Херста (номер 42 в таблице 2) имеет высокую значимость по сравнению с другими атрибутами, что иллюстрирует его значимость при бинарной классификации.

Результаты бинарной классификации

Результаты бинарной классификации при добавлении в список атрибутов фрактальной размерности представлены в виде гистограмм на рисунках 5-8.

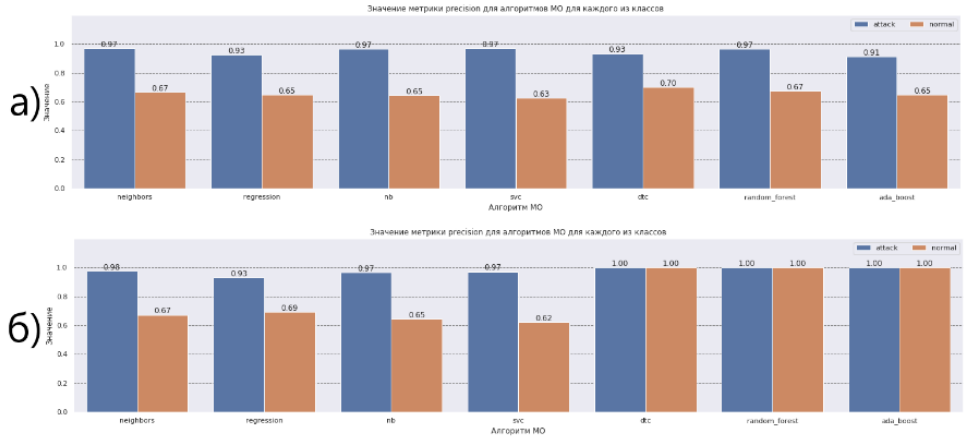


Рис. 5. Значения метрики precision для классификаций а) без параметра Херста б) с параметром Херста

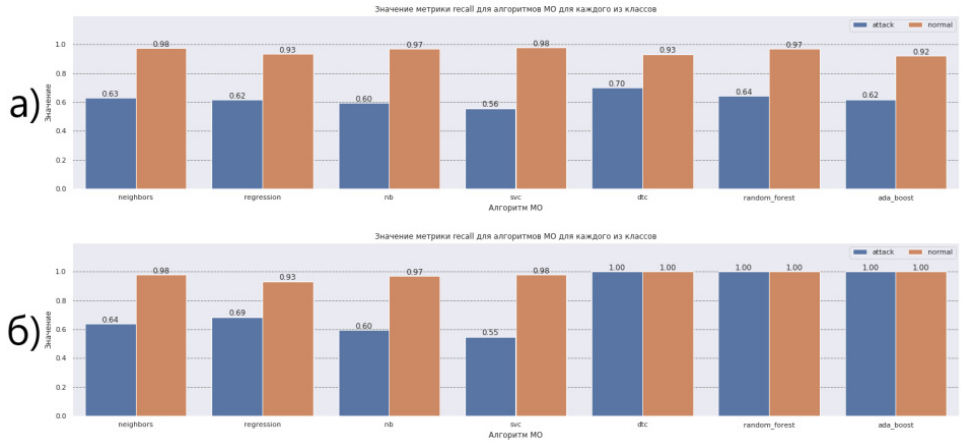


Рис.6. Значения метрики recall для классификаций а) без параметра Херста б) с параметром Херста

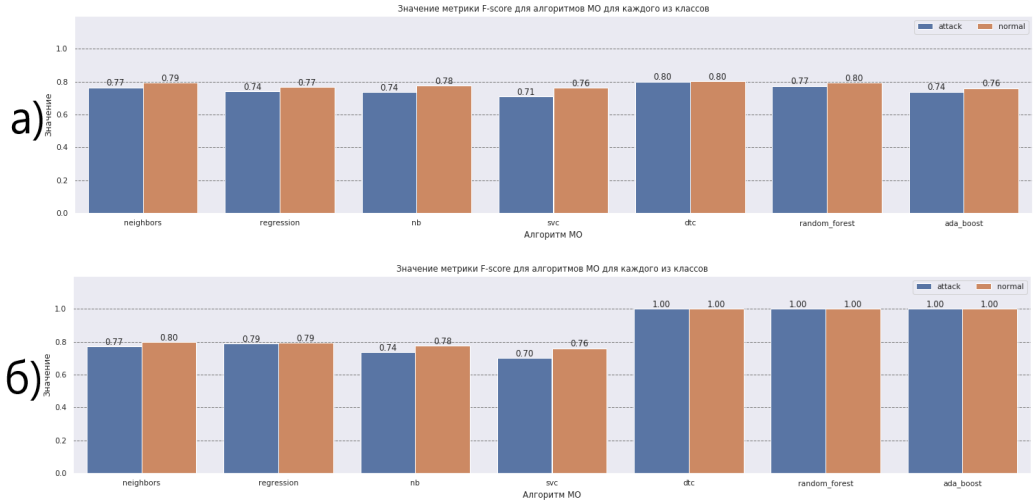


Рис. 7. Значения метрики F-score для классификаций а) без параметра Херста б) с параметром Херста

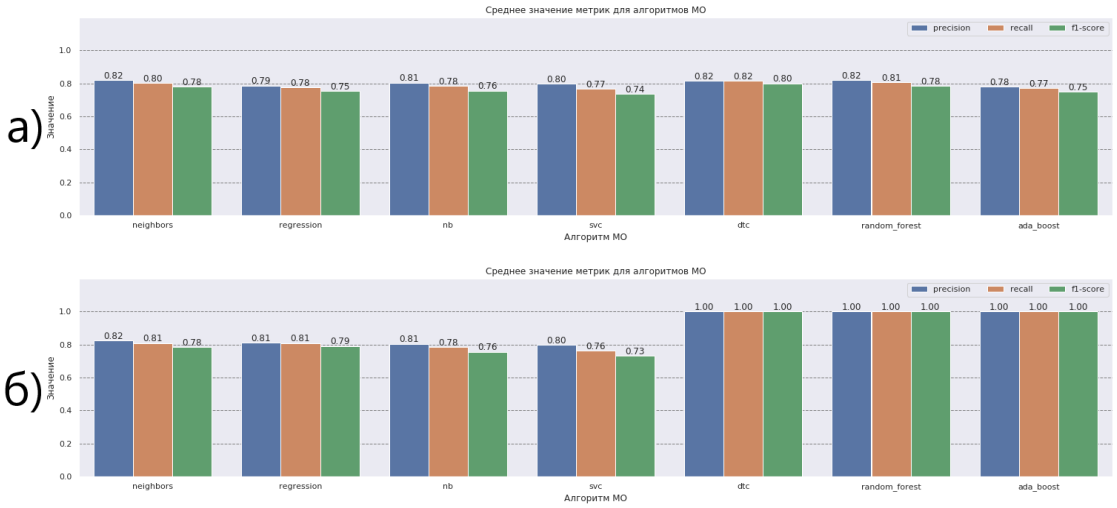


Рис. 8. Среднее значение каждой из метрик для классификаций а) без параметра Херста б) с параметром Херста

На рисунке 9 и таблице 4 представлены итоговые характеристики иллюстрирующие качество бинарной классификации при учете дополнительного признака (показателя Херста) характеризующего фрактальную размерность атак и нормального трафика.

Таблица 4

Итоговая сравнительная таблица для метрик на этапе тестирования

	precision				**recall**				**f1-score**				**AUC-ROC**				**AUC-PR**			
H	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**	**нет**	**да**
Алг	**attack**		**normal**		**attack**		**normal**		**attack**		**normal**		**attack**		**normal**		**attack**		**normal**	
kN	0,97	**0,98**	0,67	0,67	0,63	**0,64**	0,98	0,98	0,77	0,77	0,79	**0,80**	**0,84**	0,83	**0,84**	0,83	0,85	0,85	**0,71**	0,69
LR	0,93	0,93	0,65	**0,69**	0,62	**0,69**	0,93	0,93	0,74	**0,79**	0,77	**0,79**	0,90	**0,93**	0,90	**0,93**	0,93	**0,95**	0,86	**0,91**
NB	0,97	0,97	0,65	0,65	0,60	0,60	0,97	0,97	0,74	0,74	0,78	0,78	0,92	0,92	0,92	0,92	0,94	0,94	0,90	**0,91**
VM	0,97	0,97	**0,63**	0,62	**0,56**	0,55	0,98	0,98	**0,71**	0,70	0,76	0,76	**0,95**	0,92	**0,95**	0,92	0,95	0,95	**0,93**	0,79
DTC	0,93	**1,00**	0,70	**1,00**	0,70	**1,00**	0,93	**1,00**	0,80	**1,00**	0,80	**1,00**	0,82	**1,00**	0,82	**1,00**	0,82	**1,00**	0,68	**1,00**
RF	0,97	**1,00**	0,67	**1,00**	0,64	**1,00**	0,97	**1,00**	0,77	**1,00**	0,80	**1,00**	0,96	**1,00**	0,96	**1,00**	0,96	**1,00**	0,94	**1,00**
AB	0,91	**1,00**	0,65	**1,00**	0,62	**1,00**	0,92	**1,00**	0,77	**1,00**	0,76	**1,00**	0,91	**1,00**	0,91	**1,00**	0,91	**1,00**	0,90	**1,00**

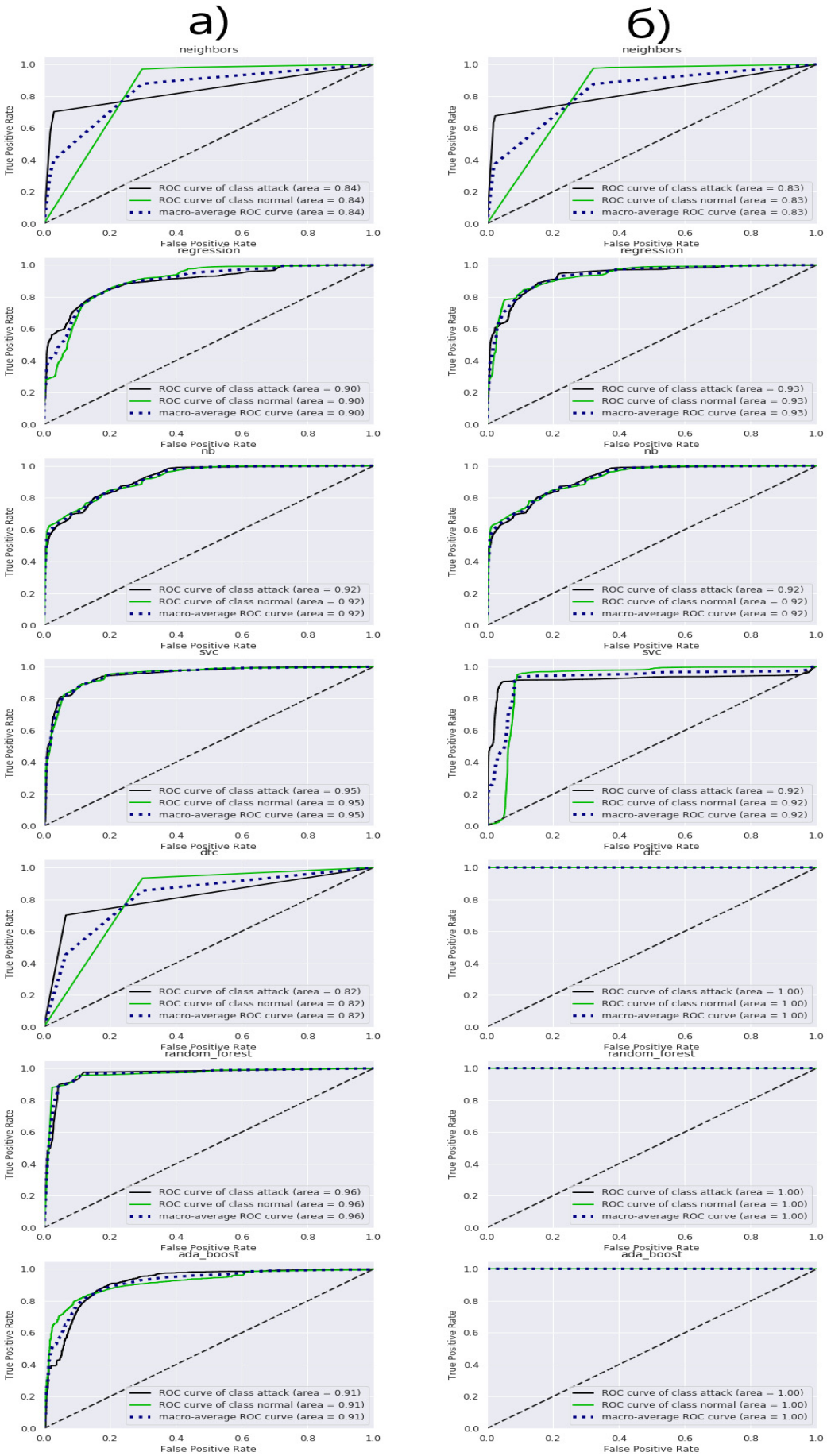


Рис. 9. ROC-кривые для бинарной классификаций, ***а)*** *без учета параметра Херста* ***б)*** *с учетом параметра Херста*

Как видно из рисунка 9 и таблицы 4 добавление дополнительного признака в виде показателя Херста положительно влияет на эффективность бинарной классификации для всех алгоритмов, представленных в исследовании. В наибольшей степени введение дополнительного признака оказывает влияние на алгоритмы, основанные на «деревьях» - *Decision Tree Classifier*, *Random Forest u* A*da Boost*. Для этих алгоритмов введение данного признака позволило существенно улучшить значения метрик, характеризующих качество бинарной классификации. Так при бинарной классификации атак улучшение метрики *precision* составило в среднем 6%, а для AUC-ROC около 10%.

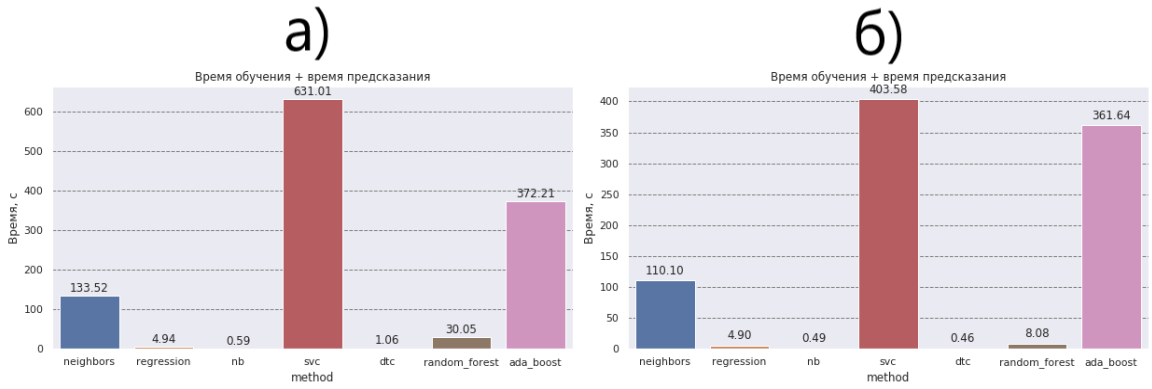


Рис. 10. Время обучения + время тестирования для бинарной классификаций а) без учета параметра Херста б) с учетом параметра Херста

Как видно из представленных на рисунке 10 гистограмм учет атрибута H приводит с существенному снижению времени обучения и тестирования для бинарной классификаций практически для всех алгоритмов классификации. Так для алгоритма RF уменьшение времени обработки составило более 3-х , а для DTC более 2х раз.

Выводы

Результаты проведенного фрактального анализа R/S-методом и атак DoS, U2R, R2L и Prob и нормального трафика в отсутствие атак показали, что нормальный трафик и атаки имеют четко выраженное различие в фрактальной размерности. Это различие может быть использовано в качестве дополнительного признака для повышения достоверности обнаружения атак.

Показано, что добавление в число атрибутов дополнительного параметра, характеризующего фрактальную размерность атак, положительно влияет на эффективность бинарной классификации и справедливо для всех алгоритмов, представленных в исследовании. В наибольшей степени введение дополнительного атрибута оказывает влияние на алгоритмы, основанные на «деревьях» - *Decision Tree Classifier*, *Random Forest u* A*da Boost*. Для этих алгоритмов введение дополнительного признака значительно, до 10% улучшает качество классификации и до 3-х раз уменьшает время обработки.

Литература

1. *Шелухин О.И.* Сетевые аномалии. Обнаружение, локализация, прогнозирование. М.: Горячая линия –Телеком, 2019. 448 с.

2. *Mohiuddin A., Abdun Naser M., Jiankun H.* A survey of network anomaly detection techniques // J. Network and Comp. App. 2015. No. 60. P. 21.

3. *Atayero A.A., Sheluhin O.I.* Integrated Model for Information Communication Systems and Metworks. Desigtn and Development. IGI Global. USA, 2013. P. 462.

4. *Шелухин О.И.* Самоподобие и фракталы. Телекоммуникационные приложения / О.И. Шелухин, А.В. Осин, С.М. Смольский. М.: Физматлит, 2008. 368 с.

5. *Sheluhin O.I., Lukin I.Yu.* Network traffic anomalies detection using fixing method of jumps of multifractal dimension in the real-time mode. Automatic Control and Computer Sciences, September 2018, Volume 52, Issue 5, pp. 421-430.

6. *Кажемский М.А., Шелухин О.И.* Многоклассовая классификация сетевых атак на информационные ресурсы методами машинного обучения // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 107-115. DOI:10.31854/1813-324X-2019-5-1-107-115.

7. *Шелухин, О.И., Ерохин С.Д., Ванюшина А.В.* Классификация IP-трафика методами машинного обучения. Москва: Горячая линия – Телеком», 2018. 284 с.

INFLUENCE OF FRACTAL DIMENSION ON THE QUALITY OF BINARY CLASSIFICATION OF NETWORK ANOMALIES BY MACHINE LEARNING METHODS

Oleg I. Shelukhin,
Head of the Department of IS of MTUCI, Doctor of Technical Sciences, Professor, Moscow, Russia
o.i.shelukhin@mtuci.ru
Mikhail A. Kazhemsky,
Post-graduate MTUCI, Moscow, Russia
m.kazhemskiy@gmail.com

Keywords: *classification, fractal dimension; Hurst exponent; attributes; training, testing; metrics; algorithms; anomalies; attacks*

The analysis showed that for solving information security problems it is advisable to use fractal analysis, which shows that anomalous packet traffic over a certain period of time can significantly change the self-similarity functions in the traffic process. To build an effective network protection system, a promising direction is the joint use of fractal and data mining. As a result, the problem of detecting network anomalies is reduced to a binary classification for the purpose of assigning the considered time series to one of two classes {"no attack", "presence of an attack"}. The results of the fractal analysis of attacks on the NSL-KDD dataset by the R/S method and normal traffic are presented, showing that the fractal dimension can be used as an additional feature of classification. It is shown that adding an additional parameter to the number of attributes characterizing the fractal dimension of attacks has a positive effect on the efficiency of binary classification and is valid for all algorithms presented in the study. The introduction of the additional attribute has the greatest impact on the algorithms based on "trees" - Decision Tree Classifier, Random Forest and Ada Boost. For these algorithms, the introduction of this parameter significantly improves the quality of the classification.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ТЕКСТА С ЦЕЛЬЮ ПОСТРОЕНИЯ QACИСТЕМЫ

Шимановичс Кирс,
ML-инженер ООО «Юнистар», Москва, Россия
kir.simanovic@gmail.com
Скородумова Елена Александровна,
доцент кафедры ТВиПМ МТУСИ, к.ф-м.н., Москва, Россия
eas@mtuci.ru

Ключевые слова: *NLP, предобработка текста, классификация текста, случайный лес, обработка естественного языка, машинного обучение, классификация, векторное представление слов.*

Представлены современные методы обработки текстовой информации. Рассмотрены различные методики предобработки текста. Подробно разобран метод векторизации текста на основе частотного анализа. Проведено исследование на основе различных методов машинного обучения, показывающее важность правильной предобратки текста и верной настройки векторного представления слов.

Последние годы все большую популярность приобретают автоматизированные линии технической поддержки, умные колл центры, голосовые колонки и др. Все их объединяет задача правильного понимания того, что сказал пользователь. Рынок NLP (обработки естественного языка) последние 5 лет показывает существенный прогресс, связанный в первую очередь с развитием голосовых ассистентов, таких, как Amazon Alexa, Google Assistant, Яндекс Алиса и др., которые предоставили совершенно новый канал взаимодействия с пользователями (см. рис. 1).

Рис. 1. Капитализация рынка голосовых ассистентов

В настоящее время в решении задачи классификации текста можно выделить несколько основных составляющих:

1. Предобработка текста – процедура подготовки текста. Включает в себя методы токенизации отдельных слов/предложений, очистки текста от шума (стопслова, пунктуация и др.), морфологический анализ слов, исправление орфографии и др.
2. Векторизация текста – процедура представления текста в виде числовых векторов.
3. Применение одного из известных алгоритмов классификации. В анализе текстов для классификации очень часто из классических методов машинного обучения используется метод опорных векторов с линейным ядром (SVM). Так же хорошую точность показывает метод прямого расчета расстояния между векторами, к примеру, на основе косинусной меры.

В целом задача классификации текста на сегодняшний день имеет очень широкий спектр решений с точки зрения выбора алгоритма классификации, однако для большинства языков с многообразной морфологией задача предобработки и векторизации текста остается сложной.

Предобработка текста

Хорошо проведенная предобработка текста является одной из важных задач при построении вопросно-ответных систем. В зависимости от решаемой проблемы можно выделить большое количество задач, связанных с предобработкой текстовой информации. В данной работе мы воспользуемся тремя методами: токенизация и очистка текста, нормализация и исправление ошибок.

Токенизация или сегментирование текста – один из первых шагов при анализе документа. Метод заключается в разделении длинного корпуса текста на более короткие: книгу на главы, каждую главу на абзацы, абзацы на предложения, предложения на слова. Очистка текста от «мусора» происходит или до токенизации, или после, в зависимости от того, какой именно «мусор» мы ищем. Слово «мусор» неспроста взято в кавычки, оно определяется, исходя из имеющихся данных и решаемой задачи. Так, к примеру, если стоит задача бинарной классификации текста на вопросительные предложения и невопросительные, то удаление вопросительного знака может сказаться на дальнейшей точности обученной модели. Но стоит отметить, что такие простые задачи встречаются крайне редко, и удаление пунктуации является обязательной процедурой при чистке текста.

Исправление орфографии является трудоемкой процедурой. Большинство современных подходов основаны на словарном методе, но также есть реализации на современных методах глубокого обучения, которые являются очень ресурсозатратными процедурами. Примером словарного подхода может служить использование редакционного расстояния.

Редакционное расстояние или расстояние Левенштейна – это метрика, которая позволяет измерить «разность» между двумя наборами символов. «Разность» определяется как количество посимвольных операций (удаление, вставка, замена), необходимых для того, чтобы превратить один набор символов в другой [1]. Пусть S_1 и S_2 – две строки длиной M и N, соответственно, над некоторым алфавитом. Тогда расстояние Левенштейна $d(S_1,S_2)$ можно рассчитать по следующей рекуррентной формуле: $d(S_1,S_2)=D(M,N)$, где

$$D(i,j) = \begin{cases} 0, & i=0,\ j=0 \\ i, & j=0,\ i>0 \\ j, & i=0,\ j>0 \\ \min\{ & \\ \quad D(i,j-1)+1, & \\ \quad D(i-1,j)+1, & j>0,\ i>0 \\ \quad D(i-1,j-1)+\mathrm{m}(S_1[i],S_2[j]) & \\ \} & \end{cases},$$

Здесь шаг по *i* обозначает удаление элемента из первого слова, по *j* – вставку в первое слово нового символа, а шаг по обоим индексам обозначает замену символа в слове или отсутствие изменений. Основная проблема использования метрики состоит в том, что расстояние между короткими словами, хоть и абсолютно разными, будет маленькое, но в тоже время между похожими, но длинными словами метрика оказывается большой.

Последняя и, наверное, самая важная задача из блока предобработки текстовой информации, – это нормализация текста. Приведение слова к нормальной форме можно разделить на два совершенно разных подхода. Первый подход основан на необходимости объявить некий стандарт (лемму) для каждого слова и привести слово к этой лемме. Обычно леммами выступают слова в словарной форме. В общем случае, используются следующие правила:

- Существительное – именительный падеж, единственное число.
- Прилагательное – именительный падеж, единственное число, мужской род.
- Глагол – глагол в инфинитиве несовершенного вида.

Данный метод носит название лемматизация. Пример работы алгоритма приведен на рис. 2. Метод имеет наибольшее распространение в сфере обработки естественного языка.

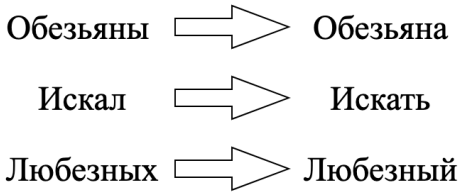


Рис. 2. Пример работы алгоритма лемматизации

Полной противоположностью алгоритму лемматизации является метод стематизации, то есть нахождения основы для заданного слова. Сразу стоит отметить, что основа слова не всегда совпадает с морфологическим корнем. Главная идея заключается в том, что от слова отрезается по кусочку: и с конца, и сначала удаляются окончания, приставки, суффиксы, и в итоге остается основная часть слова[2]. Пример применения стеммера Портера: слово «кошками» будет преобразовано в «кош».
Основной проблемой методов нормализации текста является необходимость проведения больших лингвистических исследований при подключении нового языка.

Векторизация текста

Мешок слов (bag of words) – наиболее интуитивно понятный метод. Провести векторизацию текста – это значит представить его в виде следующей конструкции. Подсчитаем количество уникальных слов во всей обучающей выборке, и каждому слову присвоим один единственный индекс. Далее, для каждого документа *i* из обучающей выборки подсчитаем количество употреблений данного слова и сохраним в , где – это индекс слова в словаре. Иллюстрация данного алгоритма представлена на рис. 3.

Фраза	гладить	и	кошка	люблю	собака	я
Я люблю собак	0	0	0	1	1	1
Я люблю гладить кошек и собак	1	1	1	1	1	1
Я глажу кошек	1	0	1	0	0	1

Рис. 3. Иллюстрация алгоритма мешка слов

Мешок слов является хорошим базовым методом для решения задачи векторизации текста, однако алгоритм обладает рядом проблем:

1. Мешок слов никак не учитывает порядок слов. Например, если слова «гладить» и «собака» встречаются в выборке достаточно часто, это никак не учитывается алгоритмом.
2. В длинных примерах из обучающей выборки среднее количество употребления слов будет выше, чем в коротких.

Для решения первой проблемы можно воспользоваться расширением словаря N-граммами [3]. N-грамма – это комбинация из *n* последовательных терминов для выделения из текста устойчивых словосочетаний. Сочетание из двух слов называются биграммой, из трех – триграмой, и т.д. В широком смысле N-граммой могут быть и определенные последовательности звуков, букв, слогов. Расширение признакового пространства N-граммами увеличивает скорость работы алгоритма, особенно для больших выборок, однако, в то же время, позволяет существенно увеличить точность работы алгоритма.

Вторая проблема находит решение в применении к алгоритму мешка слов статистической меры TF-IDF. TF-IDF – это мера для оценки важности конкретного признака в примере обучающей выборки. Вес признака в примере пропорционален частоте употребления данного признака в примере из обучающей выборки и обратно пропорционален частоте употребления признака во всех примерах обучающей выборки.

—— ————.(1)

Формула (1) состоит из произведения двух сомножителей. Первый сомножитель называется TF и отвечает за важность признака в пределах одного отдельно взятого примера из обучающей выборки. Второй сомножитель именуется IDF и показывает обратную частоту, с которой признак встречается во всех примерах из обучающей выборки. IDF позволяет уменьшить вес очень широкоупотребительных слов [4]. Иллюстрация применения меры TF-IDF приведена на рис. 4.

Фраза	гладить	и	кошка	люблю	собака	я
Я люблю собак	0	0	0	0.5774	0.5774	0.5774
Я люблю гладить кошек и собак	0.4082	0.4082	0.4082	0.4082	0.4082	0.4082
Я глажу кошек	0.5774	0	0.5774	0	0	0.5774

Рис. 4. Иллюстрация применения меры TF-IDF

К преимуществам применения мешка слов и статистической меры TF-IDF можно отнести следующие факторы:

1. Позволяет строить векторное представление документов в условиях очень малого количества данных.
2. Алгоритм работает очень быстро за счет небольшого объема операций.
3. Простота реализации.

Алгоритм векторизации на основе мешка слов и TF-IDF в связке с некоторыми моделями машинного обучения показывает действительно хорошие результаты, но, к сожалению, только в условиях действительно репрезентативной выборки.

Такая связка имеет ряд минусов. Прежде всего, стоит отметить, что алгоритм никак не учитывает слова-синонимы, поскольку сама по себе частота слова не позволяет учитывать их. Вектор признаков может иметь очень большую размерность, что в свою очередь приведет к дополнительным затратам ресурсов для обучения классификатора, или для визуализации.

Классификация

Задача классификации текстовой информации в современном мире может решаться по-разному. Самым простым подходом к классификации является сравнение векторов по какой-либо определенной метрике. Например, в качестве меры сравнения может выступать косинусная мера:

$$cos\theta = \frac{\sum_{i=1}^{n} x_i * y_i}{\sqrt{\sum_{i=1}^{n} x_i^2} * \sqrt{\sum_{i=1}^{n} y_i^2}}. (2)$$

Стоит отметить, что косинусная мера является не расстоянием, а функцией близости. Т.е. это такая функция, которая тем больше, чем больше объекты друг на друга похожи.

Для сравнения алгоритмов в данной работе было решено использовать алгоритмы машинного обучения из 4 различных классов.

- Ансамбль или комитет, который представляет собой обобщение большого количества базовых моделей, по отдельности дающие плохую точность, а в совокупности (ансамбле) хорошую. В данном классе был использован Случайный лес (Random forest).
- Линейные модели, делающие предположение о линейной сепарабельности классов, или, в случае восстановления уравнения регрессии, о зависимости между признаками, которая описывается линейно. В этом классе использовался метод опорных векторов с линейным ядром.
- Наивный байесовский классификатор – один из самых популярных вероятностных методов.
- Метод ближайших соседей – простой алгоритм из класса метрических алгоритмов.

Алгоритмы из различных классов были взяты без подбора гиперпараметров, для того чтобы наглядно показать важность процессов векторизации и предобработки текста.

Выборка для обучения представляет собой вопросы на 5 совершенно разных тематик, связанных с поступлением в университет, а именно: вопросы, связанные с заочным факультетом, вопросы, связанные с оплатой обучения или поступлением на платной основе, вопросы по вступительным испытаниям, вопросы по текущим баллам и вопросы, связанные с общежитиями. Всего было 55 вопросов, предоставленных приемной комиссией МТУСИ, которые распределены в соответствии с таблицей 1.

Таблица 1

Распределение вопросов по классам

	Заочный факультет	Платное обучение	Текущие баллы	Вступительные испытания	Вопросы по общежитию
Количество вопросов	12	13	12	8	10

Выборка вопросов является маленькой, но равномерной. В выборке нет шумовых вопросов, так как все вопросы отбирались вручную.

В первую очередь проведем обучение моделей, не используя предобработку данных, и со стандартными параметрами векторизации. Всего выделилось 213 признаков. Сравнение алгоритмов на тестовой выборке представлено в таблице 2.

Таблица 2

Сравнение алгоритмов без предобработки и настройки параметров векторизации.

	Точность	Полнота	F-мера
Наивный байесовский классификатор	29%	18%	16%
Случайный лес	29%	36%	30%
Метод опорных векторов	77%	64%	65%
Метод K-средних	40%	36%	35%

Результаты являются более чем предсказуемыми. Стандартным алгоритмам машинного обучения тяжело выделять суть из неподготовленных данных, содержащих много мусора, и к тому же очень плохо структурированных.

Выставим адекватные параметры векторизации, указав минимальную частоту слова 0.05, максимальную 0.7 и длину N-граммы равной 3. В результате было выделено существенно меньшее количество признаков, а именно 50, но эти признаки являются более информативными за счет добавления N-грамм.

Таблица 3

Сравнение алгоритмов с настройкой параметров векторизации.

	Точность	Полнота	F-мера
Наивный байесовский классификатор	60%	55%	51%
Случайный лес	77%	64%	65%
Метод опорных векторов	62%	73%	65%
Метод K-средних	68%	45%	45%

Из таблицы 3 видно, что правильная векторизация повлияла на все алгоритмы, кроме метода опорных векторов. Прирост по всем алгоритмам обуславливается более хорошей структурой признаков, отсеиванием редких и высокочастотных слов, а также добавлением N-грамм.

Добавим в векторизации предобработку текста, оставив параметры векторизации, как и в прошлом тесте. Количество выделенных признаков теперь составляет 29, что меньше, чем в предыдущем тесте. Однако в данном случае все признаки несут очень большую информационную ценность.

Таблица 4

Сравнение алгоритмов с предобработкой и настройкой параметров векторизации

	Точность	Полнота	F-мера
Наивный байесовский классификатор	86%	82%	83%
Случайный лес	95%	91%	92%
Метод опорных векторов	95%	91%	92%
Метод K-средних	91%	82%	83%

.

Как видно из таблицы 4, правильная предобработка текста и настройка параметров векторизации в среднем дают прирост почти в каждой метрике порядка 30%, даже несмотря на очень маленький размер выборки и небольшое количество признаков. Все тесты проводились с одной и той же тестовой выборкой.

В результате исследований можно заключить, что наилучшим образом в текстах себя показали более сложные модели, такие как случайный лес, являющийся ансамблем деревьев принятия решений, а также метод опорных векторов с линейным ядром, которые показали одинаковую оценку по F-мере, равную 92%.

Заключение

Построение вопросно-ответных систем в данное время является одной из ключевых задач развития области NLP в целом. Многие разработчики, впервые сталкивающиеся с этой задачей, уделяют большое количество времени подбору алгоритма машинного обучения или его оптимизации с помощью тонкой настройки гиперпараметров, уделяя при этом мало времени предобработке данных и правильной векторизации текста, хотя самый большой прирост дают именно они. В данной работе показана важность этих двух составляющих и разобраны основные методы для их проведения.

Литература

1. *Левенштейн В.И.* Двоичные коды с исправлением выпадений, вставок и замещений символов // Доклады Академий Наук СССР, 1965. 163.4:845-848.
2. *Леонтьева Н.Н.* Автоматическое понимание текстов: системы, модели, ресурсы: учеб. пособие для студ. лингв. фак. вузов. М.: Издательский центр “Академия”, 2006.
3. *Воронцов К.В.* Вероятностное тематическое моделирование // www.machinelearning.ru :web. 2013.
4. *Jones K. S.* A statistical interpretation of term specificity and its application in retrieval // Journal of Documentation :журнал. MCB University: MCB University Press, 2004. Vol. 60, no. 5. P. 493-502.

MATHEMATICAL MODELING OF A TEXT MINING SYSTEM IN ORDER TO BUILD A QA SYSTEM

Shimanovichs Kirs,
ML-engineer "Unistar" LLC, Moscow, Russia
kir.simanovic@gmail.com
Elena A. Skorodumova,
Associate Professor of TViPM Department MTUCI, PhD., Moscow, Russia
eas@mtuci.ru

Keywords: *NLP, text preprocessing, text classification, random forest, natural language processing, machine learning, classification, vector word representation.*

The modern methods of processing text information are presented. Various methods of text preprocessing are considered. The method of text vectorization based on frequency analysis is analyzed in detail. A study based on various machine learning methods has been carried out, showing the importance of correct text preproduction and correct adjustment of the vector representation of words.

ИНТЕГРАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ В СФЕРЕ ЗАКУПОК И СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ДЛЯ ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССА «ВВОД ОБЪЕКТА В ЭКСПЛУАТАЦИЮ»

Волкова Марина Дмитриевна,
ведущий аналитик ООО "ИТАРГО", Москва, Россия
msodincova@gmail.com
Маклачкова Виктория Валентиновна,
старший преподаватель кафедры СИТиС МТУСИ, Москва, Россия
v.v.maklachkova@mtuci.ru

Ключевые слова: *процесс, бизнес-процесс, электронный документооборот, информационная система, единая информационная система в сфере закупок, оплата по контракту.*

Рассматривается проблема своевременного обновления данных в контексте информационных систем электронного документооборота и единой информационной системы в сфере закупок. Анализируются ключевые особенности рассматриваемых технологических решений, выявляются риски получения неоптимального результата. Вследствии отсутствия необходимых данных, обосновывается необходимость интеграции сервисов на основе сопоставления атрибутов. Основным результатом работы является построение бизнес-процесса «Ввод объекта в эксплуатацию» функционирования информационных систем.

Одной из целей создания/формирования электронного правительства является повышение исполнения государственных функций. Так, реализовав Единую информационную систему в сфере закупок (ЕИС) появилась необходимость своевременного обновления данных о закупке в реестре контрактов, включая если объектом закупки являются строительно-монтажные работы.

В соответствии с действующим на сегодняшний день Федеральным законом от 05.04.2013 N 44-ФЗ (ред. от 31.07.2020) "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" (с изм. и доп., вступ. в силу с 01.09.2020) учреждение-заказчик обязано в течение пяти рабочих дней с даты подписания документов о приемке выполненных работ, об оплате по контракту направить сведения в ЕИС [1]. За нарушение сроков обновления данных в реестре контрактов ЕИС предусмотрены административные штрафы для должностных и юридических лиц в зависимости от количества просроченных дней вне зависимости от цены контракта [2].

Зачастую одной из причин несвоевременного обновления данных о закупке является отсутствие отлаженного процесса выполнения задач внутри организации. В данной работе предлагается решение проблемы путем интеграции системы электронного документооборота и единой информационной системы в сфере закупок. Предложенная интеграция позволит упростить и ускорить процедуру размещения информации в ЕИС и, как результат, уменьшить количество нарушений, связанных с публикацией сведений о закупке.

Для достижения заявленной цели необходимо решить следующие задачи:

- осуществить анализ работы процесса “Ввод объекта в эксплуатацию” и визуализировать его;
- определить и декомпозировать слабо проработанный шаг процесса;
- определить задачи, связанные с публикацией документации в ЕИС;

- предложить внедрение системы электронного документооборота внутри одного участника-организации процесса;
- построить бизнес-процесс для одного участника-организации;
- предложить интеграцию системы электронного документооборота и ЕИС, определив информационные связи между ними.

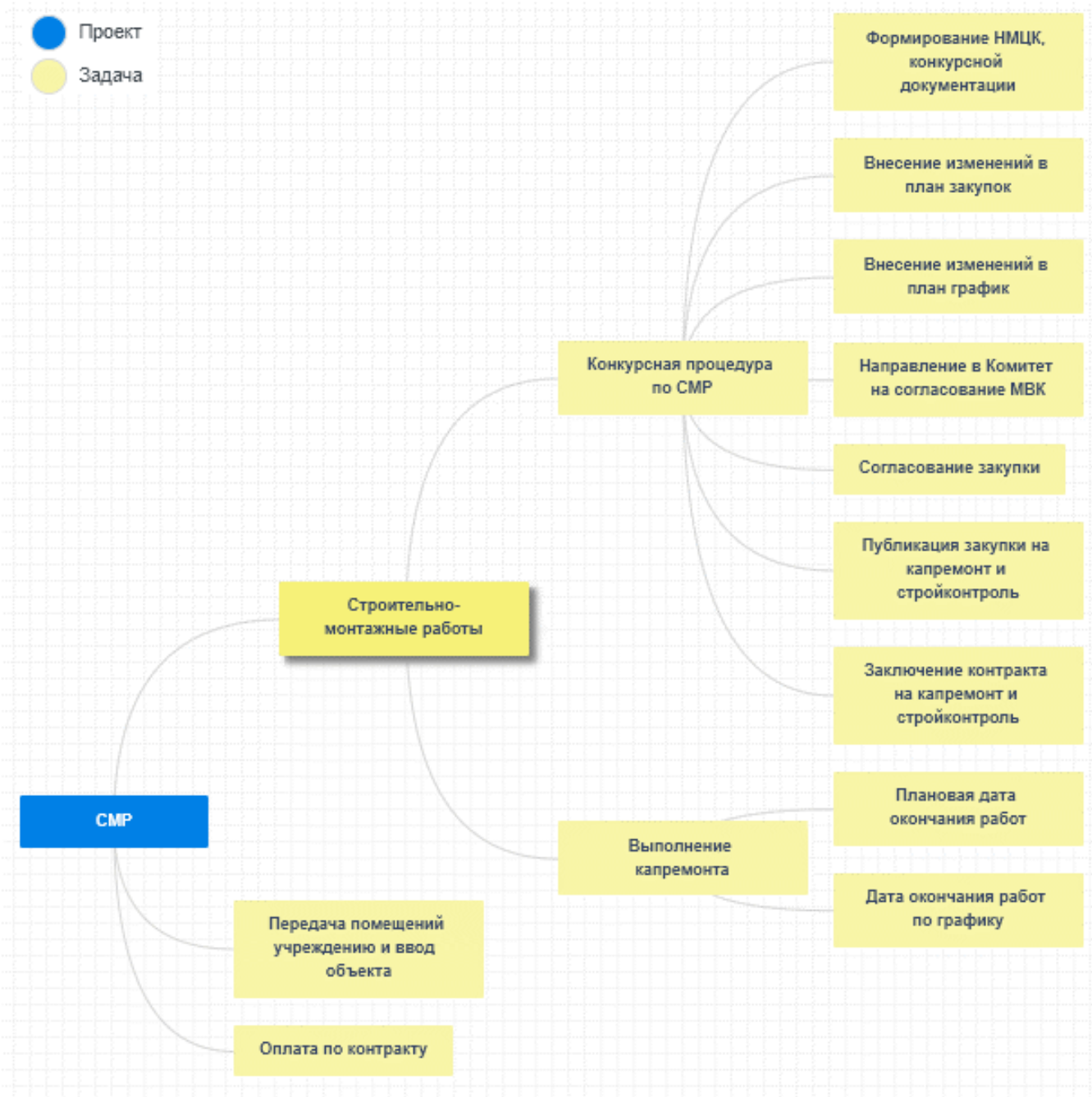


Рис. 1. Иерархическая структура работ “Строительно-монтажные работы (СМР)”

Проект “Ввод объекта в эксплуатацию” представляет собой строительно-монтажные работы (СМР), включающие в себя следующие взаимосвязанные задачи в заданной последовательности (рис. 1):

- Строительно-монтажные работы:
  - Конкурсная процедура по СМР:
    - Формирование начальной максимальной цены контракта (НМЦК), конкурсной документации;
    - Внесение изменений в план закупок;

- Внесение изменений в план график;
- Направление в комитет на согласование;
- Согласование закупки;
- Публикация закупки на капремонт и стройконтроль;
- Заключение контракта на капремонт и стройконтроль.

- Выполнение капремонта:
  - Плановая дата выполнения работ;
  - Дата окончания работ по графику.

- Передача помещений учреждению и ввод объекта;
- Оплата по контракту.

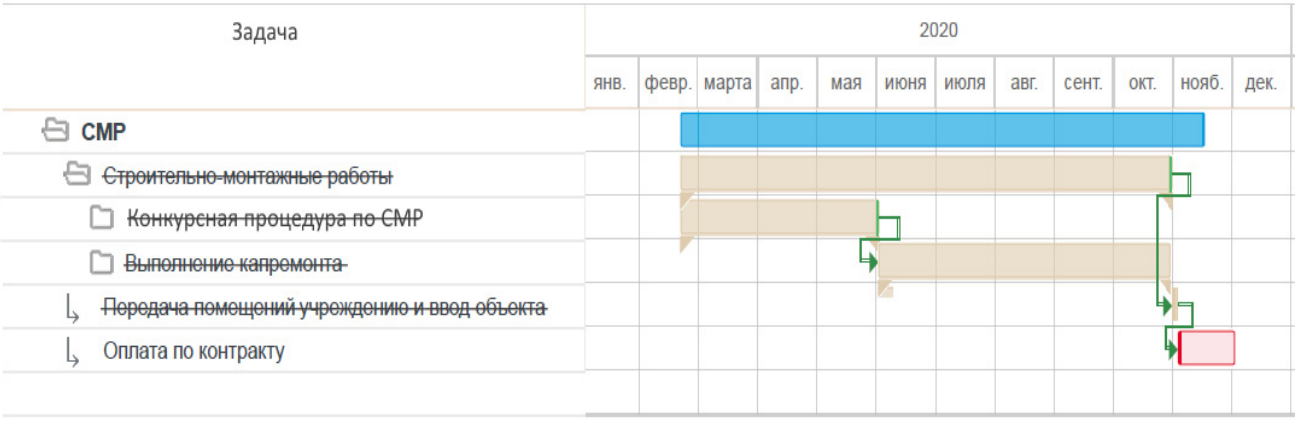


Рис. 2. Диаграмма Ганта проекта СМР

Для принятия эффективных и целесообразных решений правительство занимается вопросом создания единой комплексной модели информационной системы в сфере закупок, которая должна представлять собой учет, мониторинг, оценку эффективности предпринятых мер и выделенных средств. Однако на данный момент слабо проработаны и организованы отдельные задачи проекта.

Например, Диаграмма Ганта на рисунке 2 иллюстрирует завершенные задачи такие как: «Строительно-монтажные работы» и ее подзадачи («Конкурсная процедура по СМР», «Выполнение капремонта»), «Передача помещений учреждению и ввод объекта». На примере невыполненной в срок задачи «Оплата по контракту», завершающей проект «СМР» рассмотрим проблему своевременного обновления данных. По регламенту на выполнение задачи “Оплата по контракту” отводится не более 30 дней (44-ФЗ).

В процессе “Оплата по контракту” задействованы следующие участники (рис. 3):

- Учреждение заказчик;
- Организация-поставщик;
- Учреждение-получатель;
- Оператор электронного документооборота (ЭДО).

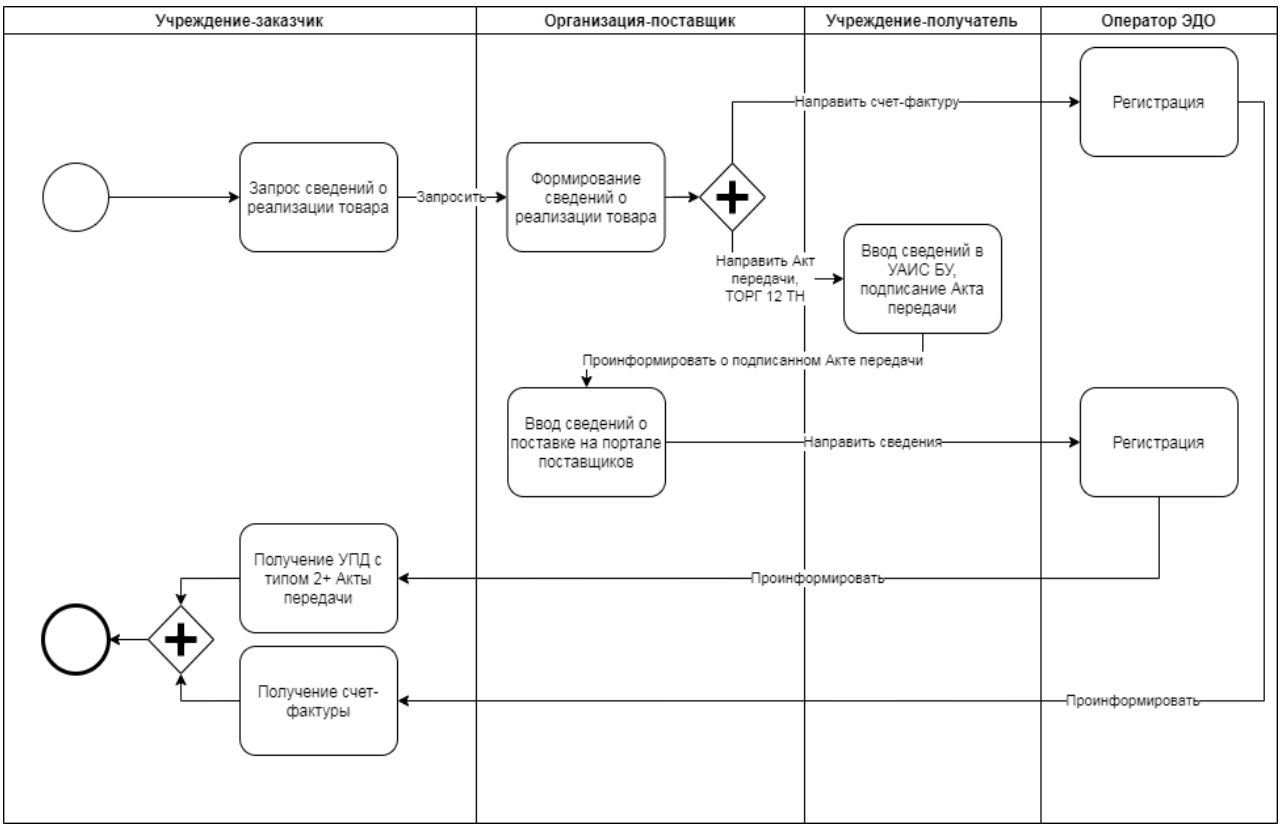


Рис. 3. Схема документооборота между участниками процесса “Оплата по контракту”

Каждый участник процесса имеет свою роль. Так, учреждение-заказчик запрашивает сведения о реализации товара или услуги у поставщика. Организация-поставщик в свою очередь формирует сведения о реализации товара или услуги и направляет счет-фактуру оператору ЭДО для регистрации и дальнейшей отправки документа учреждению-заказчику. Также организация-поставщик направляет Акт приема-передачи (Акт передачи) с сопутствующими документами учреждению - получателю на подписание. После успешной процедуры подписания организация-поставщик обязана ввести сведения о поставке на портале поставщиков (подсистема Единой автоматизированной информационной системы торгов) и направить оператору ЭДО на регистрацию для дальнейшей отправки сведений учреждению-заказчику. Процесс “Оплата по контракту” считается завершенным, если учреждение-заказчик получил следующие документы: универсальный передаточный документ (УПД) с типом 2, Акт приема-передачи товара (Акт передачи), счет-фактура.

К настоящему времени можно считать успешно решенной задачу обеспечения связи между организациями с помощью электронного документооборота. Данная система является достаточно отлаженной и на сегодняшний день не требует значительных изменений.

Однако внутри каждой отдельной организации все еще обмениваются документами в бумажном виде. С целью ускорения согласования документов, принятия решений, повышения производительности сотрудников предлагается ввести электронный документооборот между отделами одного участника процесса (учреждение-заказчик), а также ввести интеграцию системы электронного документооборота (СЭД) и ЕИС с целью повышения эффективности бизнес-процессов учреждения-заказчика. Процесс «Оплата по контракту» внутри зоны ответственности «Учреждение-заказчик» представлен на рисунке 4.

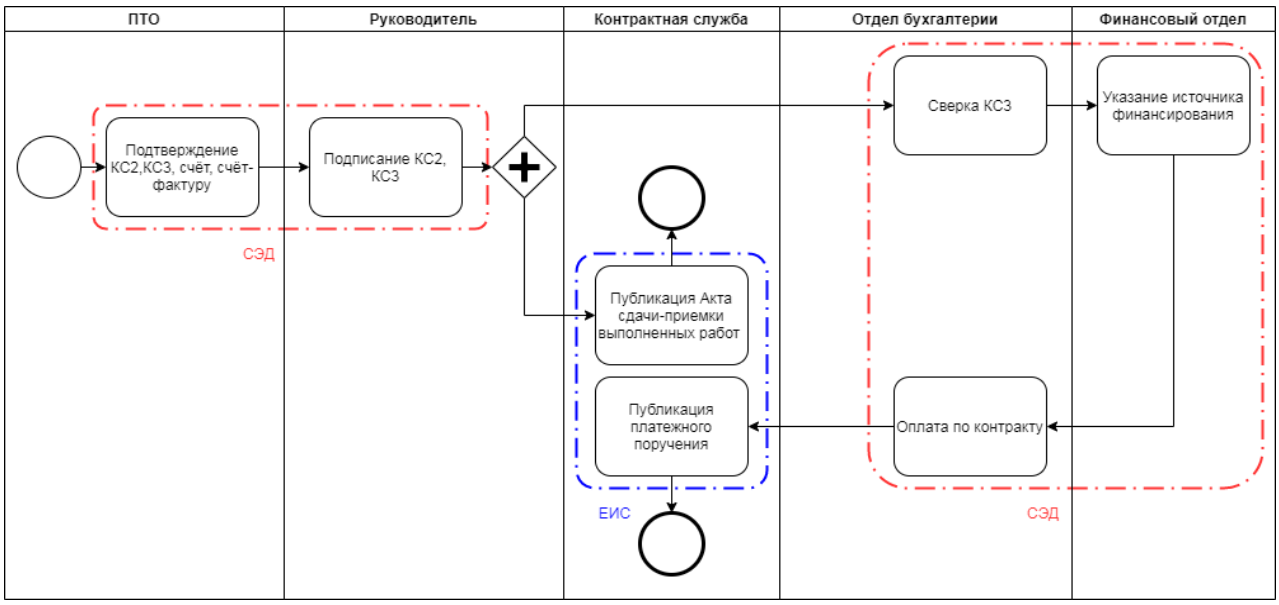


Рис. 4. Процесс “Оплата по контракту” внутри зоны ответственности “Учреждение-заказчик”

В предложенном процессе задействованы следующие участники:

- Производственно-технический отдел (ПТО);
- Руководитель учреждения-заказчик (Руководитель);
- Контрактная служба;
- Отдел бухгалтерии;
- Финансовый отдел.

В предложенной блок-схеме по методологии BPMN представлено решение взаимодействия отделов учреждения-заказчика с помощью СЭД и передаче данных в ЕИС.

Целью внедрения системы электронного документооборота является упрощение процедуры контроля исполнения документов и поручений, что влечет повышение исполнения государственных функций. За счет использования общих информационных ресурсов уменьшается время на поиск, обработку и представление информации в электронной форме. Система электронного документооборота формирует напоминания о приближении срока исполнения или извещения, если срок исполнения просрочен. Система позволяет оперативно составлять отчеты о состоянии исполнительской дисциплины.

Как представлено на рисунке 4 система электронного документооборота в процессе “Оплата по контракту” необходима для связи следующих работ и участников:

- Подтверждение Акта о приемке выполненных работ по форме КС2 и справки КС3, счета, счет-фактуры (участник - ПТО);
- Подписание Акта о приемке выполненных работ по форме КС2 и справки КС3 (участник - Руководитель);
- Направление подписанных Актов о приемке выполненных работ по форме КС2 и справки КС3 контрактной службе и отделу бухгалтерии (участник - Руководитель);
- Сверка КС3 (участник - Отдел бухгалтерии);
- Указание источника финансирования (участник - Финансовый отдел);
- Оплата по контракту (участник - Отдел бухгалтерии).

Единая информационная система в сфере закупок - информационная система, содержащая информацию о закупках, предусмотренную 44 Федеральным законом [1]. В единой информационной системе формируются, обрабатываются, хранятся и предоставляются данные о закупке посредством официального сайта единой информационной системы в сети Интернет.

В ЕИС работники контрактной службы учреждения-заказчика обязаны внести следующие сведения, входящие в реестр контрактов, установленные частью 2 статьи 103 44 Федерального закона

"О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" [1].

- Публикация Акта сдачи-приемки выполненных работ;
- Публикация платежного поручения.

Единую информационную систему и систему электронного документооборота предлагается интегрировать с целью автоматизации работы с электронными документами и дать сотрудникам учреждения-заказчика возможность работать в одном, привычном для них интерфейсе.

Интеграцией информационных систем называется процесс установки связей между информационными системами предприятий и организаций для получения единого информационного пространства [3].

Для интеграции СЭД и ЕИС необходимо отправлять следующие данные:

- Сведения о заказчике;
- Сведения о поставщике;
- Сведения о лоте;
- Сведения о контракте;
- Сведения о работнике контрактной службы;
- Акт приемки;
- Платежное поручение.

В результате интеграции единой информационной системы в сфере торгов и системы электронного документооборота возможно ускорить процесс размещения информации о закупках на официальном сайте ЕИС, обеспечив тем самым непротиворечивость и достоверность информации.

Заключение

На ближайшее время в планы по развитию Единой информационной системы в сфере закупок входит доработка подсистемы риск-мониторинга, которая позволит анализировать закупки по ряду рискоемких критериев, которые вошли в классификатор возможных нарушений [4]. Предложенные в работе решения о введении в учреждение-заказчик системы электронного документооборота СЭД и интеграции СЭД с ЕИС позволят минимизировать количество нарушений путем повышения производительности сотрудников, упрощения процедуры контроля исполнения документов и поручений.

Литература

1. Российская Федерация. Федеральный закон. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: Федеральный закон от 05.04.2013 № 44-ФЗ (ред. от 31.07.2020 с изм. и доп., вступ. в силу с 01.09.2020): [принят Государственной Думой 22 марта 2013 года : одобрен Советом Федерации 27 марта 2013 года].

2. Российская Федерация. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30.12.2001 N 195-ФЗ (ред. от 15.10.2020, с изм. от 16.10.2020) : [принят Государственной Думой 20 декабря 2001 года : одобрен Советом Федерации 26 декабря 2001 года].

3. Datareon: официальный сайт – Москва. URL: https://www.datareon.ru/uslugi-integracii-informacionnyh-sistem/ (дата обращения 27.11.2020).

4. Единая информационная система в сфере закупок : официальный сайт – Москва. URL : https://zakupki.gov.ru/epz/main/public/news/news_preview.html?newsId=30639 (дата обращения 27.11.2020).

INTEGRATION OF PROCUREMENT INFORMATION SYSTEM AND THE SYSTEM OF ELECTRONIC DOCUMENT WORKFLOW FOR OPTIMIZING THE «COMMISSIONING OF THE OBJECT» BUSINESS PROCESS

Marina D. Volkova,
Leading Analyst, ITARGO LLC, Moscow, Russia
msodincova@gmail.com
Victoria V. Maklachkova,
Senior Lecturer Department of NITaS Department MTUCI, Moscow, Russia
v.v.maklachkova@mtuci.ru

Keywords: *process, business process, electronic document workflow, information system, unified information system in the field of procurement, contract payment.*

The problem of timely data update in the context of information systems of electronic document management and a unified information system in the field of procurement is considered. The key features of the considered technological solutions are analyzed, the risks of obtaining a non-optimal result are identified. Due to the lack of the necessary data, the necessity of integrating services based on matching attributes is justified. The main result of the work is the construction of the business process "Putting the object into operation" of the functioning of information systems.

ОБОСНОВАНИЕ ХАРАКТЕРА ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА И ИНФРАСТРУКТУРЫ ИНФОКОММУНИКАЦИОННЫХ КОМПАНИЙ

Кузовкова Татьяна Алексеевна,
профессор кафедры ЦЭУиБТ МТУСИ, д.э.н., Москва, Россия
t.a.kuzovkova@mtuci.ru
Кокленков Максим Андреевич,
магистрант МТУСИ, Москва, Россия
koklemaks@mail.ru
Ткаченко Дмитрий Николаевич,
аспирант кафедры ЦЭУиБТ МТУСИ, Москва, Россия
chiker17@yandex.ua

Ключевые слова: *цифровая трансформация, сетевые бизнес-структуры, системная интеграция услуг, экосистема инфокоммуникационных компаний.*

В условиях кардинального изменения структуры и бизнес-моделей экономики актуальна задача определения характера цифровой трансформации бизнеса в сфере инфокоммуникаций. На основе монографического анализа стратегических направлений развития крупнейших операторов связи: ПАО «Ростелеком» и ПАО МТС, обосновывается сущность трансформации инфокоммуникационного бизнеса, состоящий в переводе деятельности по передаче информации и оказания услуг к формированию сетевых бизнес-структур и экосистемы цифровых сервисов. На основе выявления тесной взаимосвязи развития сетевой инфраструктуры, продуктовых и сервисных экосистем установлен каталитический характер цифровой трансформации бизнеса инфокоммуникаций, непосредственно воздействующий на экосистему цифровой экономики.

Введение

Современный этап формирования информационного общества и цифровой экономики характеризуется кардинальным изменением структуры производства и потребления, моделей и методов ведения экономической деятельности [1, 3, 10]. Отсутствие физических границ в цифровом пространстве способствует широкому распространению многосторонних бизнес-моделей, а результативность цифровой экономики становится зависимой от масштабов и глубины использования нематериальных активов, цифровых технологий, больших данных [6, 7, 14].

Цифровая экономика включает рынки, основанные на цифровых технологиях, ускоряющих торговлю товарами и услугами путем электронной коммерции, и конвергенции систем, сетей, услуг связи и информатики, разных отраслей экономики. Повсеместное использование Интернет ведет к созданию глобальных сетевых бизнес-структур, включающих сети поставщиков, производителей и потребителей, сообщества по технологии и стандартам, что обеспечивает интеграцию производственных ресурсов и снижение издержек производства, приводя к рациональному их использованию и более полному удовлетворению потребностей пользователей [12, 13, 15].

Происходящие процессы непосредственно затрагивают инфокоммуникационные компании, находящиеся на стадии насыщения рынка услугами фиксированной и подвижной связи, что настоятельно требует поиска новых решений по увеличению доходности компаний и переосмыслению моделей бизнеса. Проведенная ОЭСР оценка приоритетности целей развития цифровой экономики показала, что из 20 целей наиболее значимыми для инфокоммуникаций оказались развитие инфраструктуры и управленческие решения по адаптации бизнеса к динамично меняющейся среде на стратегическом и тактическом уровнях посредством трансформации видов и масштабов деятельности [5]. Переход на новый технологический уровень – информационное общество на основе ИКТ,

цифровизации экономики и социума вызывает необходимость кардинальной перестройки бизнеса, в том числе инфокоммуникационных компаний [9, 16].

Характеристика условий и стратегии деятельности операторов связи

ПАО «Ростелеком» (Ростелеком) является крупнейшим в Российской Федерации оператором цифровых услуг и сетей связи: широкополосный доступ к услугам фиксированной связи, цифровым каналам и Интернет, услуги интерактивного телевидения, подвижной связи, местной и дальней телефонной связи, а также комплексные услуги связи и интерактивного доступа в интернет для государственных органов и крупных корпоративных клиентов [4]. Общее число абонентов ШПД превышает 13 млн., платного цифрового ТВ – 10,2 млн., из них свыше 5,2 млн. домохозяи□ств - потребители уникального федерального продукта «Интерактивное ТВ» [4].

Ростелеком проводит активную инновационную деятельность в области обеспечения электронного правительства, здравоохранения, образования и жилищно-коммунальных услуг широкополосным доступом, разработки дата-центров и облачных вычислений, биометрии и систем кибербезопасности, что позволило обеспечить за 2018 год прирост выручки на 5% и чистой прибыли на 7%. При этом Ростелеком является основным участником национальной программы «Цифровая экономика Российской Федерации» и реализует федеральные технологические и ИТ-проекты [12]. Так начала работать созданная ПАО «Ростелеком» Единая биометрическая система (ЕБС), облачная услуга «Видеосервер», геоинформационная система Архангельской области, единая корпоративная сеть передачи данных «Почты России». Вместе с компанией Nokia и Фондом «Сколково» Ростелеком запустил первую в России открытую опытную зону сети нового поколения 5G, в том числе беспилотного транспорта, вместе с «Яндекс» - совместный тариф с облачным хранилищем до 12 Тб. По мнению специалистов, сети 5G/IMT-2020 и интернета вещей являются основой цифровой трансформации инфокоммуникаций [2]. Ростелеком начал подготовку к использованию технологии□ квантовых коммуникаций на своей сети и завершил первый этап тестирования оборудования для квантовых коммуникаций.

Для сохранения лидирующих позиций в условиях цифровой экономики ПАО «Ростелеком» в 2018 году разработал новую стратегию трансформации оператора телекоммуникационных услуг в цифровую компанию посредством расширения рынка услуг, функций провайдера цифровых услуг на территории страны, устранения цифрового неравенства России и охвата цифровыми услугами домохозяйств, социальных, государственных и частных организаций на период до 2022 года (рис. 1) [16].

Рис. 1. Стратегические цели устойчивого развития ПАО «Ростелеком» до 2022 года

В сфере подвижной связи ведущие операторы также принимают решения о трансформации бизнеса, создавая экосистему различных бизнесов. В условиях насыщения рынка ус

, увеличение скорости доступа. Однако для сохранения позиций ключевых игроков на рынке в условиях развития цифровой экономики и информационного общества операторам подвижной связи понадобилась другая стратегия, учитывающая технологические возможности инфокоммуникационной инфраструктуры по передаче больших объемов информации, ее накоплению и цифровой обработке в виртуальной среде. Для сохранения позиции ключевых игроков на рынке операторы подвижной связи стали формировать бизнес в новых для них сферах: финансовых технологий, облачных вычислений, аналитики больших данных, искусственного интеллекта, цифрового образования, телемедицины.

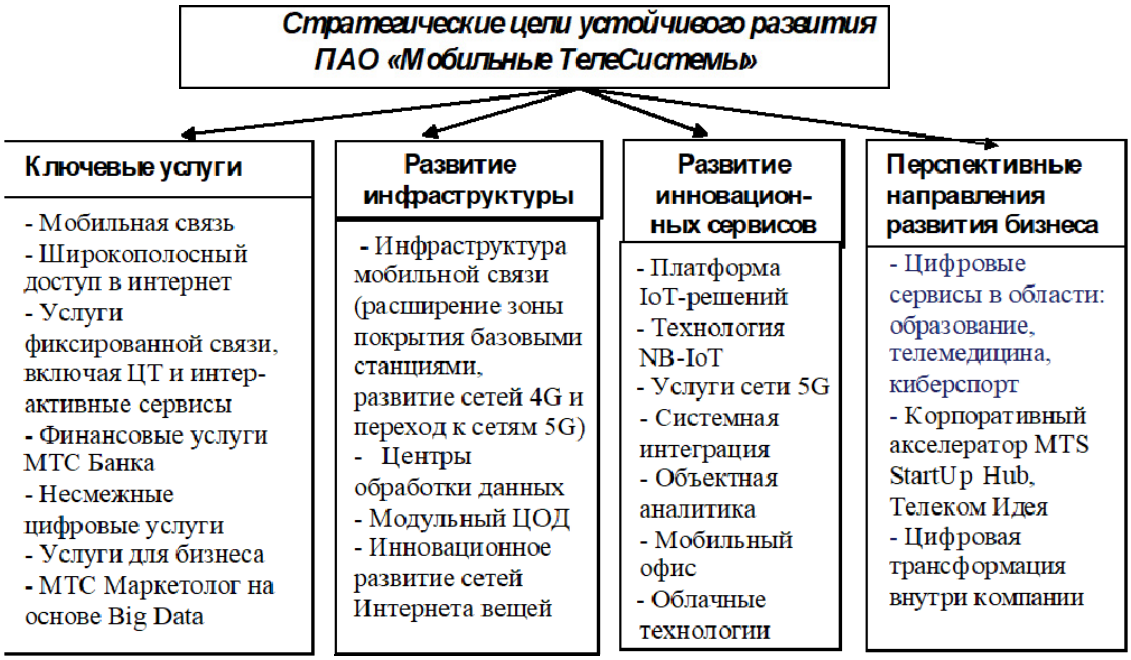


Рис. 2. Стратегические цели устойчивого развития ПАО МТС до 2020 года

ПАО МТС является ведущей компанией в России и странах СНГ по оказанию услуг мобильной и фиксированной связи, доступа в интернет, кабельного и спутникового ТВ-вещания, цифровых сервисов и мобильных приложений, финансовых услуг и сервисов электронной коммерции, а также конвергентных ИТ-решений в сфере системной интеграции, интернета вещей, обработки данных и облачных вычислений. МТС вносит значимый вклад в развитие не только России, но и стран присутствия (Армения, Украина, Туркменистан) и повышение качества жизни более 105 млн. человек [11]. В соответствии с целями ООН по устойчивому развитию МТС в 2016 году приняла Функциональную стратегию в области корпоративной социальной ответственности (КСО) и устойчивого развития до 2020 года (рис. 2). Этому способствовало развитие телекоммуникационной инфраструктуры на основе расширения зоны покрытия базовыми станциями, развития сетей 4G и перехода к с

ность работы и высокое качество облачных услуг.

Модульные центры обработки данных (ЦОД) позволяют увеличить объем услуг и сервисов для корпоративных клиентов в таких областях, как системная интеграция, хранение и обработка данных,

резервное копирование, перенос ИТ-систем в защищенное облако #CloudMTC, обработка больших массивов данных при помощи BDaaS-инфраструктуры МТС, решение задач интернета вещей. МТС первыми среди российских операторов построили инфраструктуру для сервисов и устройств интернета вещей в стандарте LTE на основе технологии NB-IoT (Narrow Band IoT), оптимально подходящей для сбора, анализа и управления данными, дистанционного контроля за приборами. Запуск сети NB-IoT переводит IoT-проекты в статус индустриальных продуктов, которые востребованы бизнесом в различных отраслях экономики, а решения на базе NB-IoT дают мощный толчок рынку интернета вещей благодаря энергоэффективности, высокому уровню безопасности и другим преимуществам нового стандарта связи, что способствует цифровизации экономики на федеральном и региональном уровнях.

Не менее важны услуги системной интеграции, направленные на автоматизацию экономической деятельности с использованием ПО и аппаратных платформ. Услуги по системнои интеграции позволяют унифицировать информационные потоки, создать единое пространство для работы, сделать бизнес-процессы прозрачными и гибкими и повысить выручку МТС - в 2018 году услуги системной интеграции обеспечили 33% выручки МТС. Для бизнеса важно также решение «Объектная видеоаналитика», позволяющее распознавать изделия с браком, контролировать присутствие людей на рабочих местах, осуществлять учет работников и продукции, идентифицировать и определять местоположение объектов, сжимать суточную съемку до важных событий.

Перспективными направлениями развития бизнеса МТС занимается Центр инноваций по шести направлениям: облака, здравоохранение, образование, искусственный интеллект, киберспорт и MTS StartUp Hub для работы со стартапами. В 2018 г. был создан Департамент M2M/IoT для создания новых продуктов и сервисов, а также координации вертикальных IoT-решений по индустриальному интернет в сельском хозяйстве, транспорте, «умного города», «умного дома», промышленности, ЖКХ и энергетике.

Сущность цифровой трансформации бизнеса и сетевой инфраструктуры инфокоммуникаций

Цель трансформации бизнеса состоит в формировании цифровых экосистем, технологической модернизации, развитии человеческого капитала и повышении эффективности крупнейших операторов связи на основе цифрового партнерства с другими компаниями для оказания различных цифровых услуг населению, бизнесу и государству, выполнения государственных задач по цифровизации государственных услуг, образования, медицины, обеспечение информационной безопасности инфокоммуникационной инфраструктуры, сохранение экологии страны [15, 16].

Цифровая экосистема инфокоммуникационных компаний будет представлять обширный набор инфокоммуникационных услуг и цифровых сервисов высокого качества для удовлетворения всего спектра потребностей. Основу новой модели бизнеса составляют цифровые, облачные и контент услуги. В условиях насыщения рынка традиционными услугами электросвязи для инфокоммуникационных компаний наиболее обоснованной стратегией становится цифровая трансформация бизнеса, состоящая в переходе от транзитной функции “трубы” по передаче информации на основе мощной магистральной и внутризоновой сети связи к операторской деятельности с расширением спектра услуг и далее к созданию цифровой экосистемы (рис. 3).

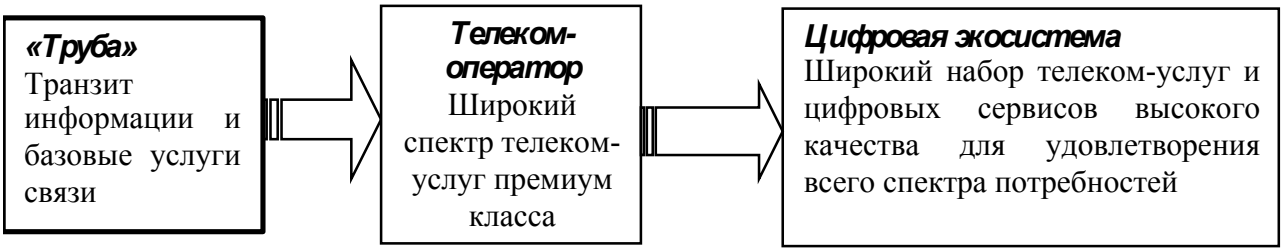


Рис. 3. Сущность цифровой трансформации производственной деятельности операторов связи

Основу новой модели бизнеса составляют цифровые, облачные и контент услуги. Основным источником прироста объемов инфокоммуникационного бизнеса в ближайшие годы становятся проекты цифровизации городского хозяйства («умные города»), услуги дата-центров и облачные сервисы, кибербезопасность, цифровое государство, анализ больших данных, искусственный интеллект, индустриальный интернет и цифровизация всех секторов национальной экономики. Большинство стратегических целей устойчивого развития компании базируется на процессах цифровизации: бизнеса, отношений с клиентами и партнерами, компетенций персонала, которые способствуют ее превращению в цифровую компанию. Проекты цифровых технологий охватывают все сферы производства услуг, развития партнерства и интеграции бизнеса, модернизации сетей связи и централизации ИТ-ландшафта и системы корпоративного управления.

В качестве важнейшего перспективного направления развития бизнеса операторы связи приняли облачные технологии, переход к которым является частью цифровой трансформации экономики. Преимущества «облаков» состоят в возможности хранить большие объемы информации, производить облачные вычисления и обмен документов, фотографий, музыки и видео, не загромождая память телефона или компьютера, поэтому МТС из стартапа превратилась в крупного облачного провайдера с собственными дата-центрами, связанными магистральными каналами связи. Поскольку требования российского бизнеса к информационной безопасности постоянно растут, а уберизация и цифровизация меняют традиционные решения в этой сфере, то МТС вышла на этот рынок с сервисом с выделенным защищенным сегментом облака #CloudMTC и отказоустойчивой инфраструктурой на базе виртуальной платформы VMware, который надежно защищает от угроз безопасности и избавляет клиентов от затрат на собственное ИТ-оборудование [11].

Цифровая трансформация системы управления компаний основывается на системном подходе к автоматизации бизнеса, состоящем в диагностике существующих производственных процессов и комплексной кросс-функциональной диджитализации внутренних бизнес-процессов по программе iDA (Internal Digital Automation) с целью снижения их трудоемкости и повышения эффективности. Для создания новых услуг в рамках цифровых сервисов и облачных платформ инфокоммуникационные компании трансформируют организационные структуры и системы управления на основе внедрения новых бизнес-моделей и бизнес-технологий, инструментов управления интегрированным производством [8].

Развитие инфокоммуникационной инфраструктуры за счет инновационных сетей связи, стандартов и сетей Интернета вещей, виртуализации сетевых функций, облачных технологий, системной интеграции и цифровизации процессов производства и потребления услуг, а также рост производительности средств связи в целях сверхскоростной передачи больших данных, неограниченной масштабируемости облачных ресурсов, информационной безопасности обусловливают модернизацию ключевых услуг на основе интеллектуальных сетей, мультисервисного и интегрального обслуживания, развитие продуктовых и сервисных экосистем, партнерских платформ совместного бизнеса и интеграцию систем связи с системами глобального позиционирования и навигации, государственного управления, медицины, образования, тем самым обеспечивают формирование глобального информационного пространства цифровой экономики.

Заключение

Переход на новый технологический уровень – информационное общество на основе ИКТ и цифровизации экономики и социума вызвал необходимость кардинальной перестройки бизнеса, в том числе инфокоммуникационных компаний. Принципиальным вектором развития инфокоммуникаций является трансформация бизнеса операторов связи в цифровых партнеров для населения, бизнеса и государства, провайдеров широкого спектра продуктов и услуг. Проведенный анализ бизнес-процессов производства и управления, целей устойчивого развития крупнейших инфокоммуникационных компаний показал, что для достижения целей цифровой трансформации

необходимо создание экосистем продуктов, услуг и клиентского сервиса на основе цифровых технологий.

Проведенный анализ стратегических направлений развития крупнейших операторов связи в условиях цифровизации экономики и социума позволил обосновать сущность трансформации инфокоммуникационного бизнеса, состоящий в переводе деятельности на формирование сетевых бизнес-структур и экосистемы цифровых сервисов. На основе выявления тесной взаимосвязи развития сетевой инфраструктуры, продуктовых и сервисных экосистем установлен каталитический характер цифровой трансформации бизнеса операторов связи, имеющий научное и практическое значение для экономики и управления инфокоммуникаций.

Литература

1. *Багиев Г.Л., Яненко М.Б., Яненко М.Е.* К вопросу формирования и совершенствования цифровой платформы организации и управления маркетинговой деятельностью фирмы: проблемы и задачи // Проблемы современной экономики. 2017. No 2 (62). С. 127-132.
2. *Бутенко В., Веерпалу В., Девяткин Е., Федоров Д.* Сети 5G/IMT-2020, & IoT – основа цифровой трансформации // Электросвязь. 2018, № 12. С. 4-9.
3. *Гассман О., Франкерберг К., Шик М.* Бизнес-модели: 55 лучших шаблонов. М.: Албпина Паблишер, 2016. 432 с.
4. Годовой отчет ПАО «Ростелеком» 2018. Отчет об устойчивом развитии. https://ar2018.rostelecom.ru/ru.
5. Декларация о будущем экономики в сети Интернет (Сеульская декларация). Рекомендации С (2008) 99 RUS.doc.
6. Доклад Всемирного банка о мировом развитии «Цифровые дивиденды». – Вашингтон, Международный банк реконструкции и развития / Всемирный банк, 2016. 43 с.
7. *Кузовкова Т.А., Кузовков Д.В., Шаравова О.И.* Задачи и требования цифровой экономики к развитию инфокоммуникаций // Экономика и качество систем связи. 2019. № 4 (14). С. 20-28.
8. *Кузовкова Т.А., Кухаренко Е.Г., Салютина Т.Ю.* Методы и способы комплексного измерения эффективности цифрового развития и применения цифровых технологий. М.: Медиа Паблишер, 2019. 171 с.
9. *Кузовкова Т.А., Кузовков Д.В., Кузовков А.Д., Шаравова О.И.* Синергетический характер эффективности развития инфокоммуникационной инфраструктуры в условиях цифровой экономики // РИСК: Ресурсы, Информация, Снабжение, Конкуренция. 2020. № 1. С. 116-123.
10. *Маркова В.Д.* Цифровая экономика: Учебник. М.: ИНФРА-М, 2018. 186 с.
11. Отчет в области устойчивого развития группы МТС 2018. М.: 2019. С. 109.
12. Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержденный президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24.12.2018 № 16. С. 90.
13. *Рихтер К.К., Пахомова Н.В.* Цифровая экономика как инновация 21-го века: вызовы и шансы для устои□чивого развития // Проблемы современной экономики. 2018. No 2 (66). С. 22-30.
14. Сопутствующий эффект цифровизации. Измерение реального воздействия цифровой экономики. Отчет компании Huawei Technologies Co., Ltd, Oxford Economics Ltd. 2017. 56 с.
15. Управление бизнесом в цифровой экономике: вызовы и решения /под ред. *И.А. Аренкова, Т.А. Лезиной, М.К. Ценжарик, Е.Г. Черновой.* СПб.: Изд-во С.-Петерб. ун-та, 2019. 360 с.
16. Цифровая экосистема экономики будущего. М.: Ростелеком. 2019. 201 с.

JUSTIFICATION OF THE NATURE OF DIGITAL TRANSFORMATION OF BUSINESS AND INFRASTRUCTURE OF INFORMATION AND COMMUNICATION COMPANIES

Tatyana A. Kuzovkova,
Doctor of Economics, Professor Dep. Digital economy, management and business technologies MTUCI, Moscow, Russia
t.a.kuzovkova@mtuci.ru
Maxim A. Coklenkov,
Graduate MTUCI, Moscow, Russia
koklemaks@mail.ru
Dmitry N. Tkachenko,
Post-graduate MTUCI, Moscow, Russia
chiker17@yandex.ua

Keywords: *digital transformation, network business structures, system integration of services, ecosystem of infocommunication companies.*

In the context of a radical change in the structure and business models of the economy, the task of determining the nature of digital business transformation in the field of Infocommunications is urgent. Based on the monographic analysis of the strategic directions of development of the largest Telecom operators: Rostelecom and MTS, the author substantiates the essence of the transformation of the infocommunication business, which consists in the transfer of information transfer and service provision to the formation of network business structures and an ecosystem of digital services. Based on the identification of a close relationship between the development of network infrastructure, product and service ecosystems, the catalytic nature of the digital transformation of the infocommunication business is established, which directly affects the ecosystem of the digital economy.