Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники

ФАКУЛЬТЕТ
ИНФОКОММУНИКАЦИЙ

ИНФОКОММУНИКАЦИИ

Сборник материалов 57-ой научной конференции аспирантов, магистрантов и студентов

Минск 2021

Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИНФОКОММУНИКАЦИИ

**57-я научная конференция
аспирантов, магистрантов и студентов**

Сборник тезисов докладов

19–23 апреля 2021 года
Минск, БГУИР

УДК 621.391

57-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 19-23 апреля 2021 г., БГУИР, Минск, Беларусь: тезисы докладов. – Мн. – 2021. – 121 с.; ил.

В сборнике опубликованы тезисы докладов, представленных на 57-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

СОДЕРЖАНИЕ

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

СЕКЦИЯ «СИСТЕМЫ РАСПРЕДЕЛЕНИЯ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ»

СЕКЦИЯ «СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ»

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

УДК 004.732, 004.728.3.057.4

МЕТОДЫ ЛИКВИДАЦИИ КОЛЛИЗИЙ ПРИ ПЕРЕДАЧЕ ДАННЫХ В БЕСПРОВОДНЫХ СЕТЯХ

Алейникова Д.И., студентка гр. 961402

Белорусский государственный универитет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В работе описано понятие коллизии, ее разновидности и причины возникновения при передаче данных в сети. Подробно изучены методы ликвидации коллизий CSMA/CD и CSMA/CA, их особенности и основные отличия. Проведен анализ использования протокола MACA в беспроводных сетях передачи данных для решения проблемы скрытой и засвеченной станций в беспроводных сетях.

Ключевые слова. Беспроводные сети, коллизии, ошибки при передаче данных, CSMA/CD, CSMA/CA, MACA.

Коллизия – столкновение данных, передаваемых в разделяемой среде передачи, приводящее к потере или искажению этих данных. Существует три разновидности коллизий: на дальнем конце (в среде передачи), на ближнем конце (в сетевой карте устройства), в активном оборудовании (перегрузка входящими данными коммутаторов/концентраторов). Наиболее распространены коллизии на дальнем конце. Они возникают, когда несколько устройств передают данные по каналу одновременно или одно из них начинает передачу раньше другого, но сигнал первого еще не успел достигнуть второго, который также начинает передавать данные. Как следствие, сигналы накладываются друг на друга и становятся недоступными для декодирования принимающим устройством. Для ликвидации такого вида коллизий был разработан метод множественного доступа с контролем несущей (CSMA, Carrier-sense multiple access). Существует две разновидности данного метода: с обнаружением коллизий (CSMA/CD, Carrier-sense Multiple Access with Collision Detection) и с предотвращением коллизий (CSMA/CA, Carrier-sense Multiple Access with Collision Avoidance).

Метод CSMA/CD применим в сетях, построенных с использованием сетевых кабелей. Обеспечивает использование канала передачи только одним устройством в определенный момент времени. Это достигается тем, что отправитель передает данные только тогда, когда среда передачи свободна. Чтобы определить состояние среды, устройство прослушивает ее на наличие основной гармоники сигнала, несущей частоты. Если несущая частота сигнала не была обнаружена, отправитель передает данные по каналу. В это же время он проверяет, не появилась ли коллизия. Для этого передача и прием сигнала с данными происходят одновременно. Если принимаемый сигнал отличается от передаваемого, значит произошла коллизия. После успешного завершения передачи данных канал освобождается, и другие устройства конкурируют между собой, чтобы как можно быстрее занять его для передачи своих сигналов.

Если же отправитель обнаруживает коллизию, он прекращает передачу данных и отправляет в канал Jam-последовательность, усиливая искажение сигнала. Таким образом, все устройства узнают о произошедшей коллизии и прекращают отправку данных на некоторое время. Этот временной интервал называется интервалом простоя (*T*) и рассчитывается по формуле:

$$T = L \cdot B, \tag{1}$$

где *B* – время между появлением двух последовательных битов данных, обычно используется 512 битовых интервалов;

L – выбирается случайно из диапазона [0, 2^n–1], где n – номер попытки оправки данных.

Следовательно, у устройств разное значение времени простоя. Первым отправлять сигнал начнет устройство с меньшим значением этого параметра. Если же значение простоя совпало, предпринимается следующая попытка отправки с выбором нового значения *L*, уже из большего диапазона. После 10-ой попытки диапазон перестает увеличиваться, а после 16-ой – среда считается неработоспособной.

Метод CSMA/CD эффективен в сетях с небольшим количеством компьютеров или при низкой нагрузке в среде. Так как это влияет на значение *L*, а чем оно выше, тем больше длительность простоя и ниже скорость передачи данных.

Метод CSMA/CA разработан для беспроводных сетей, в отличие от CSMA/CD вместо обнаружения коллизий происходит их предотвращение. Это обусловлено особенностями среды передачи. В беспроводных сетях вероятность возникновения коллизии выше, чем в проводной; мощность передаваемого сигнала выше, чем принимаемого. Также существует проблема скрытой и засвеченной станций. Направление в канал Jam-последовательности нежелательно, чтобы не перегружать среду радиосигналами. Для обнаружения коллизии используется подтверждение получения данных. Если подтверждение не было получено, значит, произошла коллизия.

В методе CSMA/CA, как и в CSMA/CD, отправитель сначала прослушивает канал на наличие основной гармоники сигнала. При ее отсутствии он направляет в среду передачи сигнал с данными. После успешной передачи данных у каждого устройства случайным образом генерируется свое число так называемых слотов ожидания – время «молчания». Слоты необходимы для предотвращения последующей конкуренции за среду передачи. Следовательно, первым передавать данные начнет устройство с наименьшим числом слотов ожидания. В отличие от CSMA/CD, устройства не конкурируют между собой, а «пропускают» друг друга передавать данные.

Таким образом, метод CSMA/CA позволяет ликвидировать возникновение коллизии в беспроводных сетях. Однако вместе с этим возникают проблемы скрытой и засвеченной станций (рисунки 1 и 2).

Скрытая станция подразумевает, что при одновременном намерении двух устройств передавать данные третьему, они находятся в таких областях распространения радиоволн, в которых не могут зафиксировать наличие в среде передачи основных гармоник сигналов друг друга. Следовательно, они передают данные одновременно и вызывают коллизию.

Засвеченная станция возникает, когда два устройства собираются передавать данные одновременно и они могут это сделать, но не делают, так как находятся в зоне видимости друг друга, следовательно фиксируют в канале несущие частоты друг друга, считая среду передачи непригодной для отправки сигнала с данными.

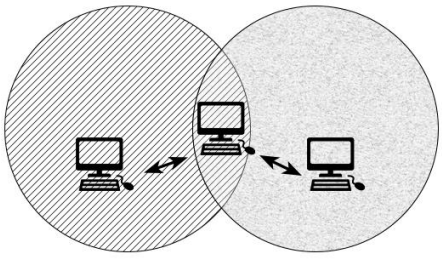


Рисунок 1 – Проблема скрытой станции

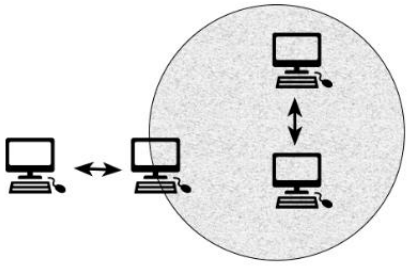


Рисунок 2 – Проблема засвеченной станции

Для решения этих проблем был разработан протокол множественного доступа с предотвращением коллизий (MACA). Суть протокола заключается в следующем: сначала устройство направляет в канал сообщение о своем намерении отправить сигнал с данными, в котором дополнительно указан размер этих данных. Получатель в ответ сообщает о своей готовности принимать данные. При скрытой станции устройство, отправившее намерение первым, получает ответ и передает свои данные, а второе устройство ответ не получает, ожидая своей очереди. При засвеченной станции оба отправителя получают ответ и передают данные одновременно, будучи уверенными, что коллизии не возникнет. Дополнительно все устройства одной сети могут узнать, сколько времени будет затрачено на передачу данных и подтверждения получения. Этот временной интервал соответствует времени «молчания», благодаря которому происходит предотвращение появления коллизий.

Таким образом, существует два метода ликвидации коллизий – CSMA/CD и CSMA/CA с поддержкой протокола MACA. CSMA/CD эффективен в небольших или малозагруженных проводных сетях, и его особенностью является обнаружение коллизий с использованием Jam-последовательности. CSMA/CA применяется в беспроводных сетях, и его особенностью является избегание коллизий с использованием слотов ожидания. Метод CSMA/CA можно оптимизировать, сочетая его с работой протокола MACA, решающего проблемы скрытой и засвеченной станций.

Список использованных источников:

1. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=s-uDMX4X2jQ – Дата доступа: 01.04.2021.

2. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=9eWeUaHA_Us – Дата доступа: 01.04.2021.

UDC 004.732, 004.728.3.057.4

METHODS FOR COLLISIONS ELIMINATING DURING DATA TRANSFER IN WIRELESS NETWORKS

Aleinikova D.I., Student of the group 961402

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Belousova E.S. – PhD

Annotation. The paper describes the concept of collision, its types and causes of occurrence during data transmission in the network. Methods for eliminating collisions CSMA / CD and CSMA / CA, their features and main differences have been studied in detail. The analysis of the use of the MACA protocol in wireless data transmission networks is carried out to solve the problem of hidden and illuminated stations in wireless networks.

Keywords. Wireless networks, collisions, data transmission errors, CSMA/CD, CSMA/CA, MACA.

УДК 621.37

МОДЕЛИРОВАНИЕ ИНТЕРМОДУЛЯЦИОННЫХ ПОМЕХ РАДИОПРИЕМНИКА ИЗМЕРИТЕЬНОЙ СИСТЕМЫ СВЧ

Булавко Д.Г., аспирант; Лисов Д.А., аспирант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусинский А.В. – канд. техн. наук

Аннотация. В докладе приводятся результаты моделирования интермодуляционных помех радиоприемника измерительной системы сверхвысокочастотного (СВЧ) диапазона.

Ключевые слова. Радиоприемник, СВЧ, моделирование, интермодуляция, помехи.

Введение

В настоящее время находят все большее применения измерительные системы радиотехнической разведки и радиомониторинга СВЧ диапазона. Основное назначение таких систем – обнаружение и измерение следующих параметров и характеристик радиосигналов: несущая частота, энергетический уровень (мощность), ширина спектра, вид модуляции, а также определение направления на источник радиосигнала. Одним из основных блоков аппаратной части рассматриваемых систем является радиоприемник. Основными требованиями, которые следует учитывать при разработке таких приемников являются очень широкие частотный и динамический диапазоны, приемлемый уровни отношения сигнал-шум и интермодуляционных искажений, а также минимизация массогабаритных параметров.

Одним из основных этапов проектирования является разработка принципиальных электрических схем отдельных узлов и радиоприемника в целом. На этом этапе весьма важным является компьютерное моделирование всего приемника с помощью пакетов программ схемотехнического моделирования. Это позволяет еще до этапа производства проводить анализ разработанного устройства и формировать техническое задание для смежных с ним блоков аппаратуры.

В докладе приводятся результаты моделирования параметров радиоприемника измерительной системы СВЧ диапазона.

Модель радиоприемника и результаты моделирования

Приемник построен по супергетеродинной схеме приема с двумя преобразованиями частоты. Рабочий диапазон частот принимаемых сигналов составляет от 1 до 18 ГГЦ и разбит на два поддиапазона: от 1 до 6 ГГЦ и от 6 до 18 ГГц.

Для анализа интермодуляционных искажений приемника была составлена его графическая модель, представленная на рисунке 1. На изображении схемы используются следующие обозначения: СМ – смеситель; МШУ – малошумящий усилитель.

Как известно [1], смешение полезного сигнала, сигналов гетеродина и их гармоник приводит к образованию мешающих интермодуляционных сигналов в полосе пропускания приемника.

Моделирование интермодуляционных помех приемника проводилась с использованием программы SystemVue. Исходными данными для расчетов являлись параметры, функциональных узлов приемника (параметры элементов графической модели), на которых планировалась его техническая реализация, а также параметры входного сигнала приемника и сигналов гетеродинов. В качестве источника полезного принимаемого сигнала (RF) на входе приемника задавался сигнал в диапазоне частот от 1 до 18 ГГц с шагом перестройки 1 ГГц и с различными уровнями мощности, отражающими работу приемника на уровне минимальной чувствительности, в середине динамического диапазона и при максимальном усилении радиоприемника. Сигналы первого (LO1) и второго (LO2) гетеродинов задавались в различных частотных точках – соответствующих плану частотного преобразования приемника и с фиксированным уровнями мощности 15 дБм и 13 дБм достаточными для работы балансных смесителей соответственно.

Для этих уровней мощности входного сигнала и сигналов гетеродинов были рассчитаны частоты и уровни по мощности образующихся интермодуляционных помех. Результаты этих расчетов представлены в таблице 1.

Полученные результаты моделирования показывают, что при значении частоты второго гетеродина равной 7050 МГц и частотах входного сигнала от 2 ГГц до 3 ГГц образуется помеха с частотой 1350 МГц, попадающая в полосу пропускания выходных фильтров приемника.

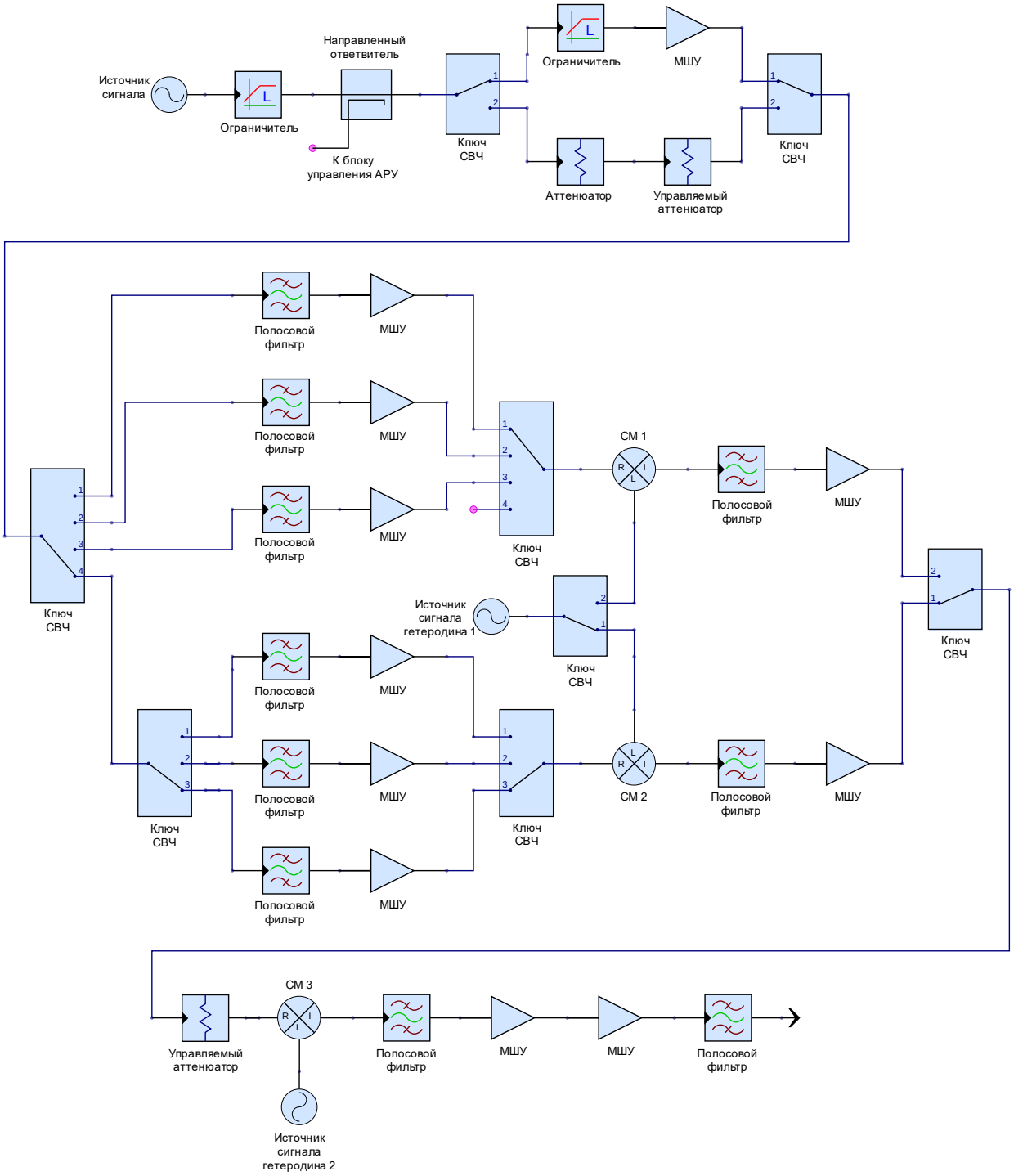


Рисунок 1 – Графическая модель радиоприемника с двумя преобразованиями частоты

При частотах входного сигнала от 3 ГГц до 4 ГГц образуется помеха с частотой 950 МГц. Уровни данных помех составляют минус 44 дБм, что является достаточным для детектирования на последующем аналогово-цифровом преобразователе (АЦП). При частотах входного сигнала от 6 ГГц до 18 ГГц и значении второго гетеродина 5200 МГц образуется постоянная помеха с частотой 1600 МГц, находящаяся на границе полосы пропускания выходных фильтров. При частотах входного сигнала 13 ГГц и значениях первого гетеродина 9 ГГц и второго гетеродина 5200 МГц

образуется помеха с частотой 1400 МГцс максимальным уровнем сигнала минус 39,4 дБм попадающая в полосу пропускания выходных фильтров приемника.

Таблица 1 – Результаты моделирования интермодуляционных помех.

RF, МГц	Мощность RF, дБм	LO1, МГц	LO2, МГц	Частота помехи, МГц	Мощность помехи, дБм	Схема образования помехи
1000	-74	9250	7050	2200	-49,3	LO1-LO2
2000	-50	10250	7050	1350	-79,2	RF+2LO1-3LO2
2000	-25	10250	7050	1350	-79,6	RF+2LO1-3LO2
3000	-74	11250	7050	1350	-58,9	2*LO1-3*LO2
3000	-50	11250	7050	1350	-63,9	2*LO1-3*LO2
4000	-50	12250	7050	950	-69,5	2*RF-LO2
4000	-25	12250	7050	950	-44,6	2*RF-LO2
4000	0	12250	7050	950	-47,8	2*RF-LO2
5000	-74	13250	7050	850	-55,1	2*LO2-RF
5000	-50	13250	7050	850	-60,1	2*LO2-RF
5000	-25	13250	7050	850	-61,7	2*LO2-RF
6000	-25	10000	5200	1600	-22	3*(LO1-RF)-2*LO2
6000	0	10000	5200	1600	-29,4	3*(LO1-RF)-2*LO2
7000	-25	11000	5200	1600	-19,7	3*(LO1-RF)-2*LO2
7000	0	11000	5200	1600	-26,8	3*(LO1-RF)-2*LO2
8000	-25	12000	5200	1600	-19,1	3*(LO1-RF)-2*LO2
8000	0	12000	5200	1600	-26,1	3*(LO1-RF)-2*LO2
9000	-25	13000	5200	1600	-19	3*(LO1-RF)-2*LO2
9000	0	13000	5200	1600	-26	3*(LO1-RF)-2*LO2
10000	-74	14000	5200	1600	-29,2	3*(LO1-RF)-2*LO2
10000	-25	14000	5200	1600	-19,8	3*(LO1-RF)-2*LO2
10000	0	14000	5200	1600	-26,9	3*(LO1-RF)-2*LO2
11000	-25	15000	5200	1600	-22,3	3*(LO1-RF)-2*LO2
10000	0	15000	5200	1600	-29,6	3*(LO1-RF)-2*LO2
12000	-25	16000	5200	1600	-20,2	3*(LO1-RF)-2*LO2
12000	0	16000	5200	1600	-27,4	3*(LO1-RF)-2*LO2
13000	-74	9000	5200	1400	-41,6	2*LO2-LO1
13000	-50	9000	5200	1400	-46,6	2*LO2-LO1
13000	-25	9000	5200	1400	-39,4	2*LO2-LO1
13000	-25	9000	5200	1600	-19,6	3*(LO1-RF)-2*LO2
13000	0	9000	5200	1400	-41,6	2*LO2-LO1
13000	0	9000	5200	1600	-26,7	3*(LO1-RF)-2*LO2
14000	-25	10000	5200	1600	-19,7	3*(LO1-RF)-2*LO2
14000	0	10000	5200	1600	-26,8	3*(LO1-RF)-2*LO2
15000	-25	11000	5200	1600	-20,7	3*(LO1-RF)-2*LO2
15000	0	11000	5200	1600	-27,9	3*(LO1-RF)-2*LO2
16000	-25	12000	5200	1600	-19,1	3*(LO1-RF)-2*LO2
16000	0	12000	5200	1600	-26,1	3*(LO1-RF)-2*LO2
17000	-25	13000	5200	1600	-19,1	3*(LO1-RF)-2*LO2
17000	0	13000	5200	1600	-26,1	3*(LO1-RF)-2*LO2
18000	-25	14000	5200	1600	-21,5	3*(LO1-RF)-2*LO2
18000	0	14000	5200	1600	-28,8	3*(LO1-RF)-2*LO2

Выводы

Анализ результатов моделирования показывает, что интермодуляционные помехи образуются в значительной степени из-за несовершенства смесителей, малой развязки между входами сигналов гетеродинов и выходами промежуточной частоты. Применение смесителей с лучшими параметрами может улучшить ситуацию на 7-10 дБ, однако вызовет значительное удорожание приемника. Применение дополнительных фильтров сигналов гетеродина после смесителей так же даст малый результат. Так как после первого преобразователя промежуточная частота достаточно высока и находится близко к частоте сигнала гетеродинов, что не позволяет использовать фильтры с большой крутизной амплитудно-частотной характеристикой. После

второго преобразователя частоты интермодуляционные сигналы так же попадают в полосу пропускания фильтров либо близки к промежуточной частоте. Наиболее приемлемым решением данных проблем является расчет ожидаемых мешающих сигналов и учет их при последующей цифровой обработке сигналов.

UDC 621.37

MODELING OF INTERMODULATION INTERFERENCE IN THE RADIO RECEIVER OF THE MICROWAVE MEASURING SYSTEM

Bulavko D.G., PG Student; Lisov D.A., PG Student

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Gusinsky A.V. – PhD

Annotation. The report presents the results of modeling the intermodulation interference of a radio receiver in the measuring system of the microwave range.

Keywords. Radio receiver, microwave, intermodulation, modeling, interference.

УДК 621.3.011

СПОСОБ УМЕНЬШЕНИЯ ФАЗОВЫХ ШУМОВ ИЗМЕРИТЕЛЬНЫХ СИГНАЛОВ В ГЕТЕРОДИННЫХ ВЕКТОРНЫХ АНАЛИЗАТОРАХ ЦЕПЕЙ КВЧ ДИАПАЗОНА

Кузюков А.Н., аспирант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусинский А.В. – канд. техн. наук

Аннотация. В докладе приводится описание способа уменьшения фазовых шумов измерительных сигналов в гетеродинных векторных анализаторах цепей КВЧ диапазона.

Ключевые слова. Векторный анализатор цепей, фазовые шумы, КВЧ диапазон.

К числу наиболее эффективных измерительных средств, предназначенных для анализа параметров СВЧ и КВЧ устройств (цепей), относятся векторные анализаторы цепей (ВАЦ). Современные ВАЦ являются высокопроизводительными информационно-измерительными системами, позволяющие провести необходимые измерения параметров устройств с гарантированной точностью в широких диапазонах с представлением и хранением измеренной информации о параметрах и характеристиках испытуемых устройств.

В докладе рассматривается способ уменьшения фазовых шумов измерительных сигналов в гетеродинном векторном анализаторе цепей КВЧ диапазона Р4-МВМ-178.

Одними из наиболее важных узлов гетеродинных ВАЦ КВЧ диапазона являются генератор измерительных сигналов и гетеродин. Погрешность установки частоты и нестабильность во многом определяют метрологические характеристики анализаторов. Для достижения необходимой точности измерения S-параметров в качестве таких генераторов используют синтезаторы частоты.

Различают несколько схем построения синтезаторов частоты [1, 2]:

1) Аналоговые синтезаторы частоты прямого синтеза. Основными преимуществами таких синтезаторов являются высокая скорость перестройки частоты и возможность использования компонентов с исключительно малым уровнем собственных шумов, т.е. шумы аналогового синтезатора определяются в, в основном, шумами используемых базовых источников частоты и могут быть очень низкими. Основные недостатки указанной топологии – ограниченные количеством смесительных каскадов диапазон и разрешение по частоте; сложность построения; множество нежелательных спектральных составляющих, которые генерируют смесительные каскады.

2) Косвенные синтезаторы частоты с фазовой автоподстройкой (ФАПЧ). Такие синтезаторы построены по принципу сравнения частоты и фазы выходного сигнала, формируемого генератором, управляемым напряжением (ГУН), с сигналом опорного генератора. К недостаткам таких синтезаторов относятся высокие фазовые шумы, неизменность шага перестройки частоты, низкая скорость перестройки. Для получения малого шага перестройки по частоте иногда объединяют в одном синтезаторе несколько петель ФАПЧ. Однако, такой синтезатор является весьма дорогим и громоздким устройством, что сдерживает его широкое применение.

3) Синтезаторы прямого цифрового синтеза (*DDS*). *DDS* уникальны своей цифровой определенностью – генерируемый ими сигнал синтезируется со свойственной цифровым системам точностью. Частота, амплитуда и фаза сигнала в любой момент времени точно известны и подконтрольны. *DDS* практически не подвержены температурному дрейфу и старению. Единственным элементом, который обладает свойственной аналоговым схемам нестабильностью, является ЦАП. Основные преимущества *DDS* заключаются в очень высоком разрешении по частоте и фазе, экстремально быстрая перестройка частоты, цифровой интерфейс.

Используемые в векторном анализаторе цепей Р4-МВМ-178, структурная схема которого представлена на рисунке 1, синтезаторы построены по гибридной схеме *PLL/DDS* синтезатора, где *DDS* используется в качестве опорного генератора для *PLL* синтезатора. Такое построение синтезатора обеспечивает относительную простоту реализации, широкую полосу синтезируемых частот (15 ГГц), высокую скорость перестройки частоты без разрыва фазы выходного сигнала, чистоты спектра выходного сигнала, мелкий шаг перестройки частоты, что критично для гетеродинных ВАЦ серии Р4-МВМ-178, т.к. съем измерительной информации производится с помощью гармонических смесителей, работающих на 8 гармонике.

В качестве опорного генератора используется малошумящий кварцевый генератор с частотой 100 МГц. Для получения необходимого рабочего диапазона частот векторного анализатора цепей в качестве источника измерительного сигнала используются синтезатор частоты 5 – 20 ГГц и

необходимый набор умножителей, в качестве гетеродина так же используется синтезатор частоты 5 - 20 ГГц. Структурная схема синтезатора 5 – 20 ГГц приведена на рисунке 2.

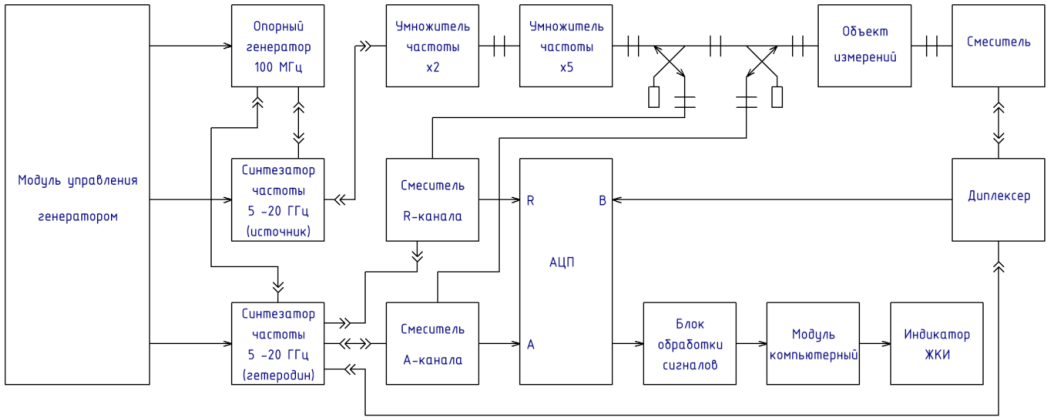


Рисунок 1 – Структурная схема векторного анализатора цепей

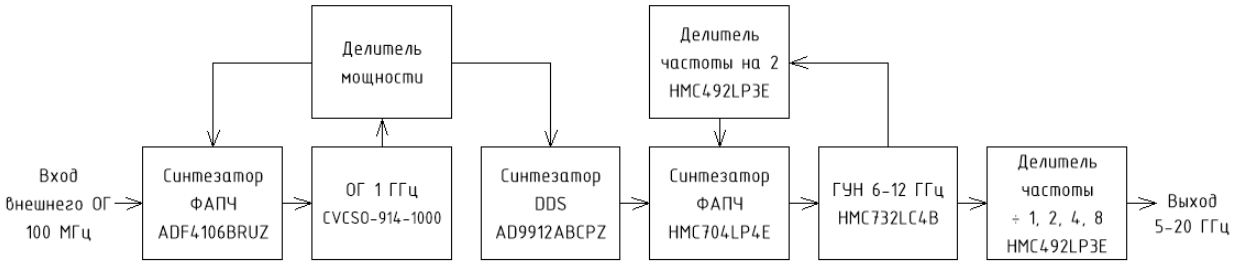


Рисунок 2 - Структурная схема синтезатора частоты 5 – 20 ГГц

Из структурной схемы устройства видно, что синтезатор DDS использует внутренний опорный сигнал частотой 1 ГГц от встроенного в схему опорного генератора (ОГ), который в свою очередь имеет собственную петлю ФАПЧ, работающей от внешнего опорного генератора 100 МГц. Из вышеизложенного следует, что используемый в схеме ВАЦ Р4-МВМ-178 опорный генератор 100 МГц служит лишь для синхронизации источника и гетеродина внутри прибора. Это обусловлено тем, что дальнейшее преобразование частоты опорного сигнала неизбежно приводит к возрастанию фазовых шумов, определяемых из выражения:

$$PN = 20 \cdot log\left(\frac{F_{out}}{F_{REF}}\right), \quad (1)$$

где F_{OUT} – частота выходного сигнала;
F_{REF} – частота опорного сигнала.

Однако, на практике оказалось, что для обеспечения высоких метрологических характеристик векторного анализатора цепей Р4-МВМ-178 предпринятых мер недостаточно. С целью исключения некоторых предполагаемых составляющих фазовых шумов была произведена модернизация схемы соединения цепочки устройств опорный генератор-источник измерительного сигнала-гетеродин, а именно:

1) Исключена линия связи между опорным генератором и гетеродином.

2) Из схемы гетеродина исключены синтезатор ФАПЧ *ADF*4106 и кварцевый генератор *CVCSO*-914-1000.

3) Сформирована линия связи от кварцевого генератора 1 ГГц источника до синтезатора *DDS* гетеродина.

Итоговая схема соединений представлена на рисунке 3.

Были проведены экспериментальные исследования фазовых шумов выходных сигналов промежуточной частоты смесителей. На рисунке 4 представлены сравнительные результаты исследований фазовых шумов до и после модернизации схемы анализатора соответственно.

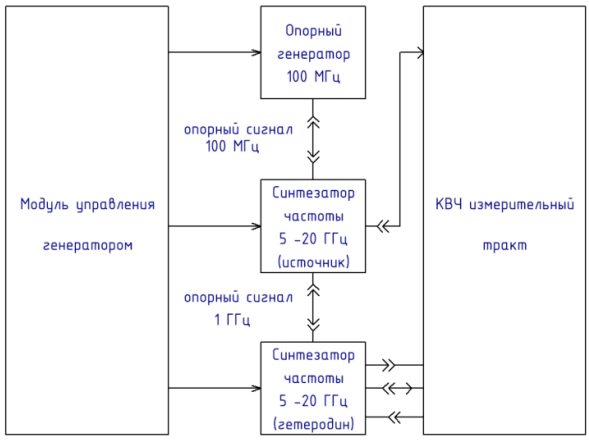
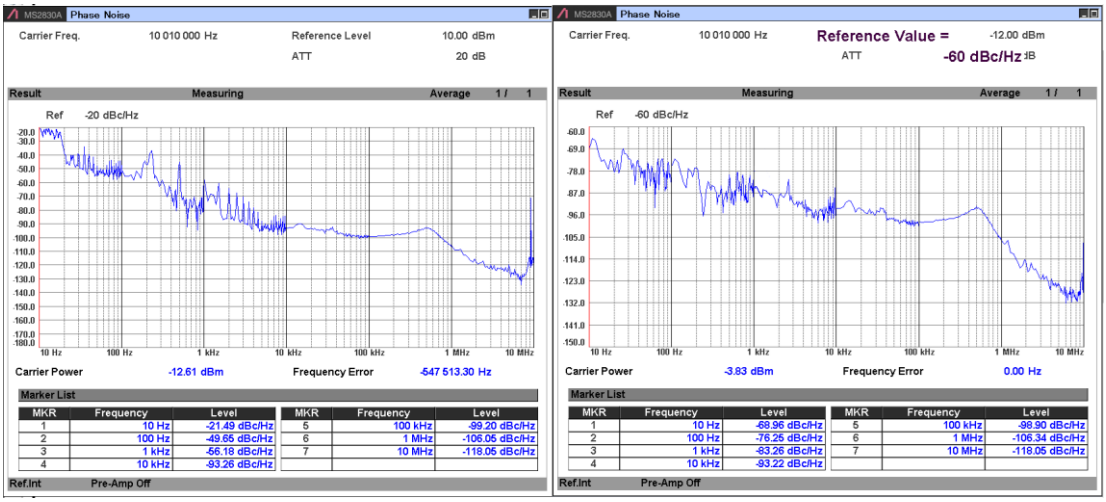


Рисунок 3 – Структурная схема векторного анализатора цепей после модернизации



а) б)

Рисунок 4 – Экспериментальные исследования фазовых шумов ВАЦ до (а) и после (б) преобразования структурной схемы анализатора

Анализ полученных результатов показывает, что предложенные изменения в структурной схеме векторного анализатора цепей КВЧ диапазона позволяют уменьшить уровень фазовых шумов на 25-35 дБ/Гц при отстройке по частоте до 1 кГц. Данный способ опробован и применяется в векторных анализаторах цепей Р4-МВМ-178.

Список использованных источников:

1. Белошицкий, А. П. Измерения в оптическом и микроволновом диапазонах длин волн. В 2 ч. Ч.1. Учебно-методическое пособие. / А. П. Белошицкий, А. В. Гусинский, А. М. Кострикин. – Минск : БГУИР, 2016.

2. Гусинский, А. В. Векторные анализаторы цепей миллиметровых волн: монография В 3 ч. Ч. 3 (кн. 1) : Принципы построения и анализ схем векторных анализаторов цепей / А. В. Гусинский, Г. А. Шаров, А. М. Кострикин. – Минск : БГУИР, 2008.

UDC 621.3.011

METHOD FOR REDUCING THE PHASE NOISE OF MEASURING SIGNALS IN HETERODYNE VECTOR ANALYZERS OF EHF CIRCUITS

Kuziukou A.N., PG Student

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Gusinsky A.V. – PhD

Annotation. The report describes a method for reducing the phase noise of measuring signals in the heterodyne vector analyzers of EHF circuits.

Keywords. Vector network analyzer, phase noise, EHF range.

УДК 004.934

ПРОГРАММНЫЙ МОДУЛЬ БИОМЕТРИЧЕСКОЙ ВЕРИФИКАЦИИ

Куницкий Ю.О., магистрант группы 067241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Аннотация. Предложен алгоритм взаимодействия пользователя с программным модулем текстозависимой верификации диктора по голосу в системах контроля и управления доступом.

Ключевые слова. Верификация, система распознавания, речь.

Работа систем распознавания пользователей по голосу содержит два основных этапа: регистрация пользователей в системе и сам процесс распознавания (попытка идентификации или верификации) [1]. Пользователи предварительно регистрируются в системе, записав свои голоса. Образец голоса каждого диктора обрабатывается с целью извлечения признаков, которые могут быть использованы для распознавания. На основе извлеченных признаков строятся модели пользователей. Модель представляет собой структуру, позволяющую при данных признаках оценить степень подобия либо сразу принять решение. В случае верификации пользователь пытается войти в систему, предъявляя идентификатор и образец голоса. Признаки, извлеченные из предъявленного образца, сравниваются с соответствующей моделью, сохраненной в базе, а так-же, возможно, с референтной моделью, представляющей фиксированное множество некоторых пользователей, либо наиболее близких к данному голосу. Результат сравнивается с заданным порогом и выдается положительное или отрицательное решение о допуске.

На пути проектирования системы верификации личности по голосу стоит задача определения весовых коэффициентов, определяющих степень вклада каждого из существенных параметров речевого сигнала в меру различимости двух голосов, при этом получаемые весовые коэффициенты должны быть оптимальны в смысле поставленного критерия. Качество работы (точность) систем верификации и идентификации личности по голосу принято характеризовать тремя следующими параметрами [2]:

1) вероятность ошибки первого рода α, т.е. вероятность отказа в допуске «своему»;
2) вероятность ошибки второго рода β, т.е. вероятность допуска «чужого»;
3) средняя вероятность ошибки: $P_e = \frac{1}{2}(\alpha + \beta)$.

В задачах проектирования взаимодействия человека и компьютера важнейшей проблемой является снижение коэффициента когнитивного сопротивления конечного пользователя. Низким коэффициентом когнитивного сопротивления обладают такие последовательности действий, результат выполнения которых предсказуем и непротиворечив [3].

В случае биометрической верификации взаимодействие пользователя с программным обеспечением должно быть переведено в голосовой формат, что значит - все вопросы, на которые человек должен дать ответ голосом должны озвучиваться, либо быть записаны заранее, либо воспроизводиться с помощью систем преобразования текста в речь. При таком подходе у конечного пользователя возникает иллюзия живого межличностного общения, что снижает коэффициент когнитивного сопротивления, избавляя человека от необходимости отвечать вслух на вопросы, написанные текстом, что в свою очередь создает ощущение неестественности происходящего и разговора с самим собой.

Предлагается разделить задачу аутентификации пользователя на два этапа, соответствующих классическому текстовому вводу логина (идентификация пользователя) и пароля (верификация пользователя).

На первом этапе пользователю предлагается произнести свои фамилию, имя и отчество. Происходит процесс идентификации пользователя, результатом которого является список подходящих учетных записей из базы данных. На этом этапе важно избегать ошибок первого рода. После того как пользователя удалось идентифицировать происходит второй этап аутентификации – верификация пользователя. Идентифицированному пользователю необходимо произнести парольную фразу. На этом этапе следует минимизировать вероятность возникновения ошибок второго рода. Таким образом удается избежать необходимости эмпирического поиска баланса между возможностью возникновения ошибок первого и второго рода, при этом понижая коэффициент когнитивного сопротивления конечного пользователя.

Список использованных источников:

1. Первушин, Е.А. Обзор основных методов распознавания дикторов / Е.А. Первушин // Математические структуры и моделирование. 2011. Вып.24. С. 41-54

2. Назаров, М.В., Прохоров, Ю.Н. Методы цифровой обработки и передачи речевых сигналов. – М.: Радио и Связь, 1985. – 176 с.

3. Купер, А. Психбольница в руках пациентов. Алан Купер об интерфейсах. – СПб.: Питер, 2020. – 384 с.

UDC 004.934

BIOMETRIC VERIFICATION SOFTWARE MODULE

Kunitskiy Yu.O., Master Student of the group 067241

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Zelmansky O.B. – PhD

Annotation. An algorithm for user interaction with a software module for text-dependent speaker verification by voice in access control and management systems is proposed.

Keywords. Verification, recognition system, speech.

УДК 616.9: 004.56(476)

ВЛИЯНИЕ COVID-19 НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ

Купрейчик А.С., студентка гр. 972302

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Смирнова Н.А. – магистр техн. наук

Аннотация. Пандемии относятся к числу социальных катастроф, сеющих панику, стрессовые и посттравматические стрессовые психологические травмы, массовую агрессию и прочие нарушения поведенческих реакций общества. Сила данных реакций связана с информационным влиянием на человека в период, когда в его психике оказывается постоянное, не поддающиеся рациональному контролю, воздействие. Хотя угрозы пандемии еще не отступили, уже пришло время анализа реакций, возникавших в социуме в период COVID-19.

Ключевые слова. Интернет, фишинг, атака, мошенничество, COVID-19, пандемия, безопасность.

Пандемия превратила Интернет в «золотую жилу» - часто единственный путь выживания, обеспечение продуктами, организации работы и образования. Данная ситуация поспособствовала росту количества новых способов мошенничества с использованием Интернет-технологий. Мошенничество всегда растет в периоды кризиса, и не важно с чем они связаны, так как в такие периоды в обществе начинается паника и уровень внимательности, к получаемой информации, снижается [1].

Фишинг, один из самых распространенных видов мошенничество в сети, – это вид интернет-атаки, цель которой получение доступа к конфиденциальным данным пользователей [2]. Особую тревожность вызывают факты активизации виртуальных мошенников во время пандемии коронавируса, когда мошенники используют тему коронавируса как «приманку» и просят переходить по ссылке в письмах, якобы отправленных из банка. В этих письмах может оказаться «сайт-ловушка». Цель таких рассылок – узнать пароли, логины, данные карты за счет подделки сообщений от доверенного источника. Фишинговые страницы похожи на оригинальные страницы сайта банков, вследствие чего люди становятся жертвами преступников. Другими последствиями киберпреступности в период карантина стала организация большого количества сбоев в работе информационных ресурсов. Финансовые угрозы нарушения целостности данных были связаны с переходом многих предприятий на удаленный режим работы без соблюдения необходимых мер безопасности. Помимо проблем для государственных структур и бизнеса в части нарушения целостности или хищения конфиденциальных данных, внедрение хакеров вызывало, например, сбои в процессе дистанционного образования и научной работы.

Новое исследование Anti-Phishing Working Group (APWG) показало, что уровень фишинговых атак на сайты финансовых учреждений, веб-почты и сайты SaaS. рос до 2020 года, удваиваясь в течение года. Приблизительно 70 % всех доменных имен в мире, зарегистрированных в злонамеренных целях, принадлежат китайскими преступниками для использования против различных брендов и предприятий. Число выявленных и заблокированных в глобальной сети за девять месяцев 2020 года фишинговых сайтов превысило показатель прошлого года [3].

Проблематика киберпреступности в период пандемии освещалась, прежде всего, в СМИ, а также через социальные сети, что, несомненно, в связи с мобильностью доведения информации о возможных угрозах, снизило риски и денежные потери населения. Несмотря на это, ряд информационных ресурсов подвергся DDoS-атакам, с них происходило массовое хищение персональных данных граждан, функционирование ресурсов приостанавливалось из-за создававшихся злоумышленниками сбоев в их работе.

Удавалось мошенничество, как правило, при наличии уязвимостей у информационного ресурса, а также благодаря неосведомленности, доверию и невнимательности граждан в моменты наибольшей психической уязвимости (сужения коридора восприятия, флуктуации внимания в момент паники). Прежде всего, были подвержены мошенничеству граждане, находящиеся в особо сложной жизненной ситуации (многодетные семьи, лишившиеся работы граждане, одинокие престарелые люди и др.), а также сотрудники в режиме удаленной работы, оперирующие данными организаций, не предназначенными для обнародования. Интернет-мошенничество особенную опасность представляло для населения с низкой финансовой, правовой и компьютерной грамотностью. Если речь идет о мошенничестве по отношению к гражданам, то кроме неосведомленности, оно апеллирует к сильным эмоциям и жизненным приоритетам потребителей: к сочувствию, тревоге за жизнь близких, к фобиям и страхам (например, к страху перед болезнью,

страху остаться без средств к существованию, а также страху дефицита продуктов потребления) [4].

Распространение информации о борьбе с мошенниками, помимо указанных выше каналов, шло через печатную прессу, радио, телевидение, видеоэкраны в общественных пространствах, объявления в общественном транспорте.

Применявшиеся меры профилактики мошенничества были связаны с усилением защиты информационных ресурсов с целью предотвращения их взлома, а также с информированием населения о приемах распознавания и о порядке реагирования на действия мошенников для исключения утечки персональных данных и финансовых потерь.

На мой взгляд, одной из причин подобного уровня мошенничества является недостаточное образовательное сопровождение. Отсутствие необходимых знаний в области Интернет и информационных технологий создает благоприятную почву для злоумышленников. В связи с этим следует сформировать систему образования соответствующим навыкам в информационном пространстве:

1) сегодня навыки пользования информационными технологиями в общих чертах преподаются в рамках информатики, но изучения вопросов информационной безопасности не имеется, в связи с чем следует ввести в школах специальную дисциплину касательно понятия и сущности сети Интернет, данная дисциплина также должна предусматривать обучение навыкам первичного пользования и поведения в виртуальном пространстве;

2) в системе высшего образования подготовка технических кадров в области информационной безопасности осуществляется в Белорусском государственном технологическом университете, Белорусском государственном университете, Белорусском государственном университете информатики и радиоэлектроники, Витебском государственном университете имени П. М. Машерова, Гродненском государственном университете имени Янки Купалы, Полоцком государственном университете, при этом современная тенденция в области кадровой политики требует подготовки специалистов в междисциплинарном русле, то есть кадров, обладающих как правовыми, так и техническими навыками обеспечения информационной безопасности;

3) следует создать программу повышения квалификации и переподготовки кадров, осуществляющих оперативно-розыскные мероприятия, дознание или следствие по преступлениям, связанным с информационной безопасностью, в правоохранительных органах [5].

В целом проблема доверия в сети Интернет является комплексной. В этой части необходимо формировать Интернет-культуру со стороны пользователей виртуального пространства путем проведения курсов и ознакомительных уроков, брошюр и иных материалов.

Список использованных источников:

1. Информационная безопасность в условиях пандемии: методы стабилизации состояния социума в электронных СМИ и Интернете / Кузина Н. В. // Бюллетень науки и практики, 2020 – №9. – С. 356-394.
2. Национальный правовой Интернет-портал [Электронный ресурс]. – Режим доступа : https://pravo.by.
3. APWG [Электронный ресурс]. – Режим доступа : https://apwg.org.
4. Onliner [Электронный ресурс]. – Режим доступа : https://www.onliner.by .
5. Информационная безопасность в условиях пандемии коронавируса / Расулев А. // Вестник юридических наук, 2020 – №2. – С. 224-228.

UDC 616.9: 004.56(476)

THE IMPACT OF COVID-19 ON THE INFORMATION SECURITY OF THE REPUBLIC OF BELARUS

Kupreijchik A.S., Student of the group 972302

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Smirnova N.A. – Master of Science in Engineering

Annotation. Pandemics are among the social catastrophes that sow panic, stress and post-traumatic stress psychological trauma, mass aggression and other violations of the behavioral reactions of society. The strength of these reactions is associated with the informational influence on a person during a period when there is a constant, not amenable to rational control, influence in his psyche. Although the threat of a pandemic has not yet receded, it is time to analyze the reactions that arose in society during the COVID-19 period.

Keywords. Internet, phishing, attack, fraud, COVID-19, pandemic, security.

УДК 621.37

МНОГОФУНКЦИОНАЛЬНЫЙ ГЕНЕРАТОР СЛОЖНЫХ СИГНАЛОВ СВЧ ДИАПАЗОНА

Лисов Д.А., аспирант; Булавко Д.Г., аспирант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусинский А.В. – канд. техн. наук

Аннотация. В докладе рассматривается структурная схема, принцип работы и параметры многофункционального генератора сложных измерительных и радиолокационных сигналов сверхвысокочастотного (СВЧ) диапазона.

Ключевые слова. Векторный генератор, СВЧ, структурная схема, параметры.

Введение

При настройке и тестировании оборудования различных широкополосных систем связи, радиолокационных и радионавигационных систем, цифровых приемников и других радиоэлектронных средств используются сложные испытательные сигналы. Непосредственная генерация сложных сигналов с цифровой модуляцией в СВЧ диапазоне труднореализуема и требует больших затрат. Поэтому для формирования таких сигналов используются так называемые векторные генераторы, которые позволяют формировать сложные испытательные сигналы с различными видами модуляции. Однако выходные сигналы известных векторных генераторов [1, 2] не позволяют имитировать различные ситуации реальной радиолокационной обстановки (наложением на полезные сигналы шумовых сигналов и сигналов с паразитной модуляцией, сигналов с частотой смещения Доплера и других).

В докладе рассматривается структурная схема, принцип работы и параметры многофункционального генератора сложных измерительных и радиолокационных сигналов сверхвысокочастотного (СВЧ) диапазона.

Структурная схема генератора

Обобщенная структурная схема многофункционального источника сложных измерительных и радиолокационных сигналов от 1 до 20 ГГц представлена на рисунке 1.

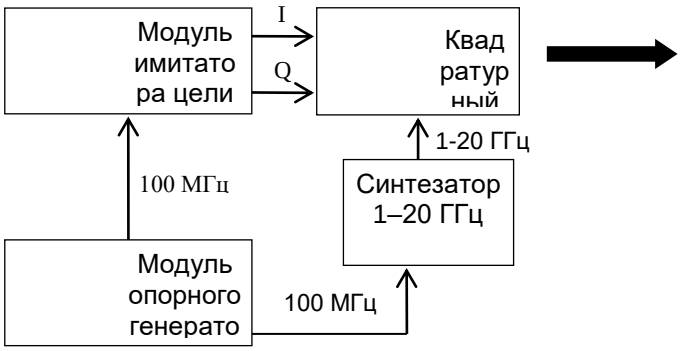


Рисунок 1 – Обобщенная структурная схема генератора

Модуль имитатора цели (МИЦ) структурная схема которого представлена на рисунке 2, предназначен для формирования сигналов сложной формы с различными законами модуляции и наложенными на них помеховых и шумовых составляющих.

Входные сигналы поступают в модуль и подаются через входной буфер в программируемую логическую интегральную схему (ПЛИС). ПЛИС накапливает данные и производит обработку информации, в результате которой формируется в цифровом виде сложный сигнал.

Тактирование ПЛИС производится кварцевым генератором 100 МГц или внешним тактовым генератором, сигнал которого поступает через буфер тактирования.

Для увеличения скорости обработки данных ПЛИС при сложных вычислениях используется быстродействующая память SRAM на 144 Мб. Управление ПЛИС производится по интерфейсу

SPI. Выходные цифровые сигналы ПЛИС поступают на цифро-аналоговый преобразователь (ЦАП) для представления их в аналоговом виде.

Управление МИЦ осуществляется с помощью микропроцессора, который обеспечивает

– управление контроллером Ethernet и RS-485 для обмена данными с внешними устройствами;

– управление ПЛИС с помощью интерфейса SPI;

– диагностику модуля на наличие ошибок;

– контроль готовности модуля к работе;

Тактирование микропроцессора производится с помощью кварцевого генератора 25 МГц. Управление микропроцессором производится по интерфейсу SPI или по интерфейсу USB.

Обмен данными между микропроцессором и ПЛИС осуществляется с помощью 16-ти битной шины.

В МИЦ предусмотрен специальный слот для подключения карты памяти формата MicroSD объемом до 32 ГБ, содержащей специальные данные-сценарии работы модуля.

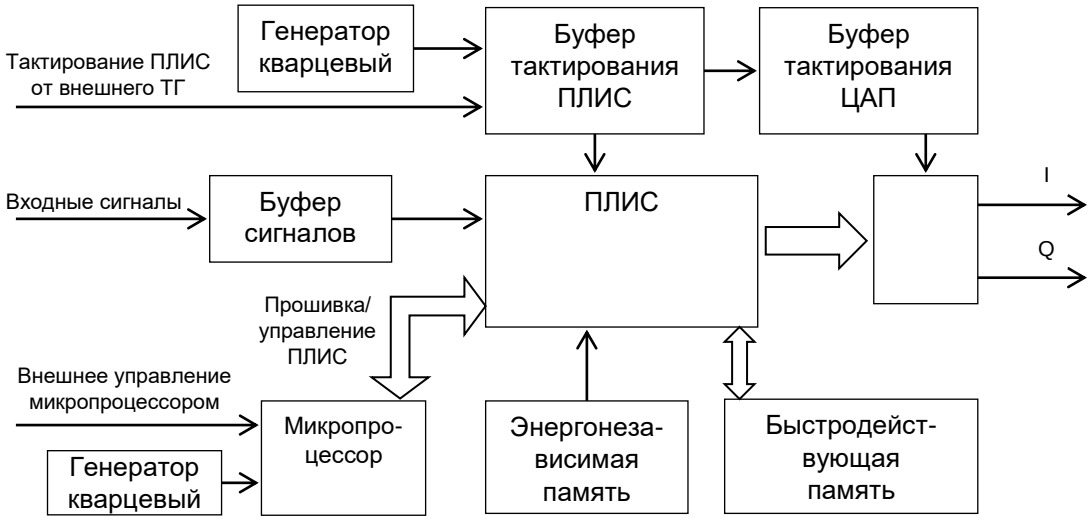


Рисунок 2 – Структурная схема модуля имитатора цели

На выходе ЦАП МИЦ формируются синфазная и квадратурная составляющие аналогового сигнала U(t)в виде комбинации

$$U(t) = A_1(t)\cos(\omega_0 t) + A_2(t)\sin(\omega_0 t)\,. \quad (1)$$

Первое слагаемое в этом выражении называется синфазной составляющей (или I – составляющей), а второе – квадратурной составляющей (или Q – составляющей). Это разложение лежит в основе квадратурной амплитудной модуляции на основе которой в свою очередь могут создаваться другие сложные виды модуляции.

Модуль имитатора цели может работать в двух режимах:

– циклическом (параметры радиолокационной обстановки до начала сеанса работы загружены в модуль и циклически воспроизводятся);

– динамическом (параметры радиолокационной обстановки в реальном масштабе времени рассчитываются и загружаются в модуль во время работы).

Модуль опорного генератора предназначен для формирования и управления сигналами опорной частоты 100 МГц, с помощью которых обеспечивается синхронизация (тактирование) работы модулей и блоков генератора.

Синтезатор 1–20 ГГц предназначен для формирования стабильных по частоте колебаний в диапазоне частот от 1 до 20 ГГц и выполняет функции гетеродина для модулятора. Для обеспечения стабильности частоты в синтезаторе применяется фазовая автоподстройка частоты.

Модуль может работать как от внутреннего, так и от внешнего источника опорной частоты 100 МГц.

В квадратурном модуляторе (I/Q смесителе) [3] несущий СВЧ сигнал модулируется сигналами I и Q, затем сигналы складываются вместе и образуют модулированный сигнал РЧ.

I/Q смесители обеспечивают хорошее подавление несущей СВЧ и паразитной боковой полосы, образующейся при смешении сигналов. Как и в обычных смесителях, частота сигнала РЧ равна сумме частоты СВЧ и промежуточной частоты ПЧ (то есть частоты I/Q сигналов). Если используется сдвиг частоты модулирующих сигналов, в спектре РЧ присутствует полезный сигнал

со сдвигом относительно остаточного пика сигнала СВЧ и сильно подавленный сигнал боковой полосы на зеркальной частоте.

Главным преимуществом I/Q смесителей является то, что они подавляют паразитный сигнал боковой полосы, это означает, что смесители работают как смесители с одной боковой полосой. Поэтому не требуется дополнительной фильтрации сигнала РЧ, так как несущая СВЧ и боковая полоса сильно подавляются самим смесителем, обычно на 30 – 40 дБ, в зависимости от частотного диапазона РЧ. Кроме того, I/Q смесители работают непосредственно с модулирующими сигналами. Следовательно, нет необходимости в генераторе векторных сигналов, достаточно генератора модулирующих сигналов для формирования входных I/Q сигналов.

Такое построение генератора позволяет реализовывать широкие функциональные возможности.

На выходе генератора могут быть сформированы: немодулированные импульсные сигналы, импульсы с линейно и нелинейно-частотной модуляцией, а также квадратурной фазовой манипуляцией; мультиплексирование с ортогональным частотным разделением каналов; сигналы со сложными законами модуляции.

В генераторе имеется возможность имитации эхо-сигналов целей с различными амплитудами, фазами и частотами смещения Доплера. К полезным сигналам возможно добавление мешающих отражений и активных шумовых помех с различными законами распределения и различными параметрами.

Рабочий диапазон частот генератора: от 1 до 20 ГГц. Мощность выходного сигнала: от –130 дБм до +18дБм.

Выводы

С помощью программного обеспечения и вариации различных параметров генератор позволяет формировать реальные радиолокационные и измерительные сигналы в том виде, в котором они появляются на входе СВЧ приемника. Благодаря этому генератор позволяет проводить недорогие проводные испытания радарных модулей и многоканальных СВЧ приемников в лабораторных условиях, вместо дорогостоящих полевых испытаний.

Список использованных источников:

1. R&S®SMW200A Vector Signal Generator [Электронный ресурс]. Режим доступа: https://www.rohde-schwarz.com/ru/product/smw200a-productstartpage_63493-38656.html. – Дата доступа: 10.02.2021.

2. Руководство по выбору генераторов сигналов Keysight [Электронный ресурс]. Режим доступа: https://www.keysight.com/ru/ru/assets/7018-03356/technical-overviews/5990-9956.pdf – Дата доступа: 01.10.2020.

3. Тростер С. Генерация векторных сигналов сверхвысоких частот //T-Comm: Телекоммуникации и транспорт. – 2009. – №. S5. – С. 4-10.

UDC 621.37

MULTIFUNCTIONAL GENERATOR OF COMPLEX MICROWAVE SIGNALS

Lisov D.A., PG Student; Bylavko D.G., PG Student

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Gusinsky A.V. – PhD

Annotation. The report examines the structural diagram, principle of operation and parameters of a multifunctional generator of complex measuring and radar signals of the microwave range.

Keywords. Vector generator, microwave, block diagram, parameters.

УДК 535.14

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ

Марчук А.А., студентка гр. 914302

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пухир Г.А. – ст. преподаватель

Аннотация. Рассматриваются причины возникновения квантовой криптографии, технология квантовой криптографии. Приводится обоснование применения алгоритмов шифрования на основе квантового распределения ключей. Выделяются проблемы квантовой криптографии.

Ключевые слова. Ключ шифрования, квантовая криптография.

История квантовой криптографии началась не с технологий связи, а с попытки решить совершенно другую задачу – создать деньги, которые невозможно подделать. Стивен Визнер из Колумбийского университета в 1983 году предложил создать квантовые банкноты государственного образца, которые нельзя скопировать даже в том случае, если у желающего сделать это есть типографское оборудование и бумага, при помощи которых изготавливался оригинал. Вероятность изготовления точной копии оригинала, защищенного квантовыми технологиями, стремится к нулю.

В криптографии, шифрование является процессом преобразования информации в шифротекст с помощью ключей. Этот процесс преобразует исходное представление информации, известное как открытый текст, в альтернативную форму, известную как зашифрованный текст. В идеале только авторизованные стороны могут расшифровать зашифрованный текст обратно в открытый и получить доступ к исходной информации. Шифрование само по себе не предотвращает возможность перехвата информации, но не позволяет потенциальному перехватчику получить доступное содержимое. Среди этапов практически любого алгоритма шифрования наиболее уязвимым считается этап распределения ключей. В большинстве стандартных подходов проблема решается с помощью инфраструктуры открытых ключей, однако это усложняет сам процесс шифрования и предъявляет повышенные требования к условиям его реализации.

Технология квантового распределения криптографических ключей решает одну из основных задач криптографии – гарантированное на уровне фундаментальных законов природы распределение ключей между удаленными пользователями по открытым каналам связи. Криптографический ключ – это числовая последовательность определенной длины, созданная для шифрования информации. Квантовая криптография позволяет обеспечить постоянную и автоматическую смену ключей при передаче каждого сообщения в режиме одноразового «шифроблокнота»: на сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью.

Чтобы скопировать банкноту, фальшивомонетчик должен измерить поляризации фотонов, но он не знает, в каком базисе поляризован каждый из них (эту информацию, как и параметры поляризации, банк держит в секрете, и только он знает, какие поляризации соответствуют номеру банкноты). Преступник может выбирать базисы случайным образом, и тогда у него есть некоторые шансы на успех, правда, очень небольшие. Но они становятся ничтожными, если создать фотонные ловушки: например, увеличить число фотонов на каждой банкноте (вероятность угадать снижается как обратная степенная функция от числа фотонов). Если каждый денежный знак снабдить десятком ловушек, вероятность успешной подделки падает почти до нуля.

Ограничениями первых реализаций квантовых систем шифрования были небольшая дальность передачи и очень низкая скорость. Еще одна проблема квантовой криптографии – это необходимость создания прямого соединения между абонентами, ведь только такой способ взаимодействия позволяет организовать защищенное распределение ключей шифрования. Стоимость квантовых систем на сегодняшний день составляет десятки и сотни тысяч долларов, так что разработчики коммерческих решений предлагают технологию квантового распределения ключей в виде сервиса, ведь большую часть времени оптические каналы простаивают.

UDC 535.14

QUANTUM KEY DISTRIBUTION

Marchuk A.A, Student of the group 914302

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Puhir G.A. – Senior Lecturer

Annotation. The reasons for the emergence of quantum cryptography, the technology of quantum cryptography are considered. The substantiation of the application of encryption algorithms based on quantum key distribution is given. The problems of quantum cryptography are highlighted.

Keywords. Encryption key, quantum cryptography.

УДК 004.491:004.423.24

ТЕСТИРОВАНИЕ ВЕБ ПРИЛОЖЕНИЙ НА НАЛИЧИЕ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ВНЕДРЕНИЕМ ВРЕДОНОСНОГО КОДА

Мирошниченко А.В., студент гр. 961402

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В последнее время актуализировались вопросы, связанные с тестированием веб приложений на наличие уязвимостей. Целью данной работы является подробное теоритическое и практическое изучение наиболее популярных уязвимостей, а именно SQL-инъекция и межсайтовый скриптинг. Таким образом в работе представлены понятия и виды данных уязвимостей, принцип их реализации и возможные последствия внедрения вредоносного кода посредством эксплуатации SQL-инъекций и межсайтового скриптинга. Практическое изучение уязвимостей, связанных с внедрением вредоносного кода, осуществлялась в веб-приложение PentesterLab. Также в работе предложены ряд мер по защите веб-приложений от уязвимостей, связанных с внедрением вредоносного кода. Предложенный материал будет интересен специалистам, которые занимаются тестированием веб-приложений, а также студентам, обучающимся по специальностям, связанными с информационными системами, программным обеспечением информационных технологий, программируемыми мобильными системами и др.

Ключевые слова. Уязвимость, тестирование, веб-приложение, внедрение вредоносного кода, OWASP, SQL-инъекция, межсайтовый скриптинг (XSS), PDO (PHP Data Object).

Веб-приложение – клиент-серверное приложение, в котором клиент взаимодействует с веб-сервером при помощи браузера. Логика веб-приложения распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети. Тестирование веб-приложений – это метод выявления, анализа и сообщения об уязвимостях, существующих в веб-приложении. Топ-10 уязвимостей по статистике OWASP приведен на рисунке 1.

Топ-10 OWASP 2013		Топ-10 OWASP 2017
A1 - Внедрение	→	A1:2017-Внедрение
A2 - Недостатки аутентификации и управления сессиями	→	A2:2017-Недостатки аутентификации
A3 - Межсайтовое выполнение сценариев (XSS)	↘	A3:2017-Разглашение конфиденциальных данных
A4 - Небезопасные прямые ссылки на объекты [Объединено с A7]	U	A4:2017-Внешние сущности XML (XXE) [Новое]
A5 - Некорректная настройка параметров безопасности	↘	A5:2017-Недостатки контроля доступа [Объединено]
A6 - Разглашение конфиденциальных данных	↗	A6:2017-Некорректная настройка параметров безопасности
A7 - Отсутствие контроля доступа на функциональном уровне [Объединено с A4]	U	A7:2017-Межсайтовое выполнение сценариев (XSS)
A8 - Межсайтовая подмена запросов (CSRF)	☒	A8:2017-Небезопасная десериализация [Новое, Сообщество]
A9 - Использование компонентов с известными уязвимостями	→	A9:2017-Использование компонентов с известными уязвимостями
A10 - Непроверенные перенаправления и переадресации	☒	A10:2017-Недостатки журналирования и мониторинга [Новое, Сообщество]

Рисунок 1 – ТОП-10 уязвимостей по статистике OWASP

SQL-инъекция – один из распространенных способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода. Внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения

Схема основного принципа действия SQL инъекций приведена на рисунке 2.

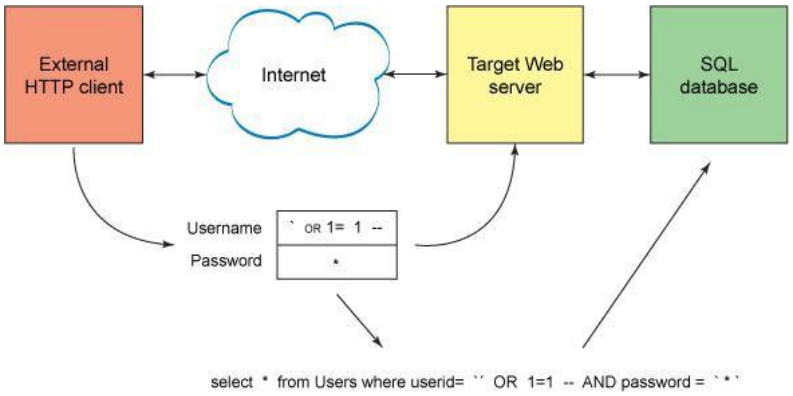


Рисунок 2 – Схема принципа действия SQL инъекций

Виды SQL-инъекций:

– инъекция в строковом параметре;

– инъекция в цифровом параметре.

Изучение данных видов SQL-инъекций было практически реализовано в веб-приложение PentesterLab. Так, например, было проверена работа приложения при реализации следующего запроса: *http://IP-address/sqli/example1.php?name=root' OR 1=1 --+*.

Реализация запроса *http://IP-address/sqli/example1.php?name=root' ORDER BY X* позволила установить количество столбцов в таблице пользователей в базе данных. В представленном запросе X соответствует номеру столбца. Изменяя значение *X* от 1, можно заметить, что приложение будет работать корректно, но при вводе значения *X*=6, приложение выдало ошибку, что позволяет сделать вывод, что общее количество столбцов в таблице пользователей равно 5.

Далее был использован SQL-оператор UNION, который позволяет объединять в одном запросе обращение к разным таблицам базы данных, что позволяет получить данные из таблиц, к которым доступ не предусмотрен. С помощью запроса *http://IP-address/sqli/example1.php?name=root' UNION+SELECT+1,2,3,4,5+FROM+users+WHERE+id=1* были получены данные из таблицы users, в том числе их имена и пароли, хотя приложением не предусмотрен доступ к данной таблице базы данных.

Можно сделать вывод, что вариаций использования SQL-инъекций очень много и большинство из них приводит к явному получению неправомерного доступа к информации.

Предложены следующие способы защиты от SQL-инъекций:

1) Использовать белые списки.
2) Не использовать метод GET в формах.
3) Проверять и обрабатывайте переменные.
4) Проверять источник запросов и сами запросы на наличие SQL-инъекций.
5) Использовать PDO (PHP Data Object).

Межсайтовый скриптинг (XSS) – это одна из разновидностей атак на веб-системы, которая подразумевает внедрение вредоносного кода на определенную страницу сайта и взаимодействие этого кода с удаленным сервером злоумышленников при открытии страницы пользователем. Схема принципа действия XSS приведена на рисунке 3.

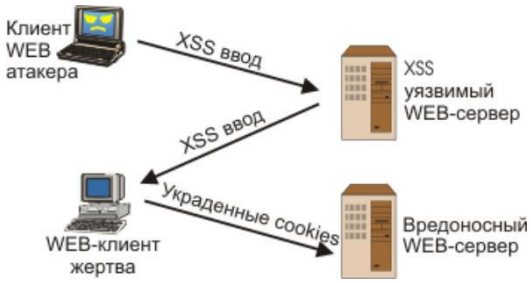


Рисунок 3 – Схема принципа действия межсайтового скриптинга

Выделяют следующие виды XSS атак: пассивные и активные.

В веб-приложение PentesterLab были практически реализованы основные виды XSS атак и установлены следующие особенности реализации данной атаки:

1) Для реализации простейшей XSS атаки достаточно использовать функцию alert.
2) PHP убирает тег из запроса, поэтому необходимо использовать заглавные символы.

3) PHP преобразует все символы в нижний регистр и убирает теги, поэтому необходимо добавлять один тег в другой.

4) Для обхода проверки запросов необходимо воспользоваться стандартным параметром onerror, который возникает при отсутствии изображения.

5) В случае запрета на уровне приложения использования функции alert, нужно проверять возможность внедрения любой другой JS функцию.

Таким образом, уязвимость межсайтового скриптинга является довольно опасной и распространенной. Основная опасность заключается в том, что при обработке HTML реализуются все функции, которые находятся между тегами. Поэтому злоумышленник может без проблем воспользоваться уязвимостью и получить пользовательские данные.

На основе практического изучения данной атаки предложены следующие способы защиты от XXS:

1) Защита функцией htmlspecialchars.
2) Защита функцией strip_tags.
3) BB-коды.
4) Регулярные выражения.
5) Самописные функции.

Список использованных источников:

1. OWASP. Топ-10 OWASP – 2017. Десять самых критических угроз безопасности веб-приложений. [Электронный ресурс]. – Режим доступа: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-ru.pdf/ – Дата доступа: 25.02.2021.

2. Уязвимости и угрозы веб-приложений в 2019 году / Positive Technologies Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020/. – Дата доступа: 25.02.2021.

3. Статья SQL injection для начинающих. Часть 1. / Habr [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/148151/. – Дата доступа: 25.02.2021.

UDC 004.491:004.423.24

TESTING WEB APPLICATIONS FOR VULNERABILITIES RELATED TO THE IMPLEMENTATION OF MALICIOUS CODE

Mirashnichenka A.V., Student of the group 961402

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Belousova E.S. – PhD

Annotation. Recently, issues related to testing web applications for vulnerabilities have been actualized. The aim of this work is a detailed theoretical and practical study of the most popular vulnerabilities, namely SQL injection and cross-site scripting. Thus, the paper presents the concepts and types of these vulnerabilities, the principle of implementation and the possible consequences of a malicious code injection through the exploitation of SQL injection and cross-site scripting. A practical study of vulnerabilities related to the injection of malicious code was carried out in the PentesterLab web application. The paper also proposes a number of measures for protection web applications from vulnerabilities associated with the malicious code injection. The proposed material will be of interest to specialists who are engaged in testing web applications, as well as to students studying in specialties related to information systems, information technology software, programmable mobile systems, etc.

Keywords. Vulnerability, testing, web application, injection of malicious code, OWASP, SQL-injection, cross-site scripting (XSS), PDO (PHP Data Object).

УДК 004.451

ОЦЕНКА ЗАЩИЩЕННОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Мурадов Э.К., магистрант гр. 067241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук

Аннотация. Представлены основные критерии для оценки защищенности операционной системы.

Ключевые слова. Информационная безопасность, операционная система, оценка защищенности.

Операционную систему (ОС) называют защищенной, если в ней реализованы средства защиты от основных классов угроз [1]. На основе данного определения, а также современных рекомендаций в области защиты информация, к основным оценочным критериям защищенности операционной системы можно отнести следующие.

1 Разграничение доступа к ресурсам системы и данным пользователей. В том числе возможность разграничения на разных уровнях.

2 Аутентификация, авторизация и идентификация пользователя при входе в систему, запросе доступа к ресурсу или данным.

3 Противодействие преднамеренному или случайному выводу из строя ОС или ее компонентов, в том числе установленного программного обеспечения.

4 Возможность использования шифрования данных пользователей и конфигураций системы.

5 Возможность ведения журнала событий, как действий пользователей и администраторов системы, так и событий самой системы и ее компонентов, для дальнейшего аудита.

6 Внедрение политик безопасности, в том числе дальнейшее управления ими.

7 Резервирование данных пользователя и конфигураций системы, в том числе с поддержкой шифрования таких данных.

Сетевое взаимодействие также должно контролироваться операционной системой. ОС должна определять, какое программное обеспечение и как использует сетевые возможности, журналировать события использования программным обеспечением сетевых ресурсов и при необходимости ограничивать взаимодействие с сетью.

Оценка защищенности должна учитывать архитектуру построения операционной системы. В случае комплексной архитектуры ОС должна иметь защищенные точки расширения функционала ядра системы для реализации отсутствующих средств обеспечения безопасности. В случае архитектур с модульным ядром или несколькими микроядрами необходимо обеспечение безопасных протоколов общения компонентов и отказоустойчивость фундаментальных сервисов.

При оценивании ОС необходимо производить испытание заявленных характеристик, в том числе анализировать предустановленные параметры для средств защиты информации. Такое тестирование может разделяться на активное и пассивное. Под активным тестированием подразумевается эмуляция действий потенциального злоумышленника по преодолению механизмов защиты, в том числе используя уязвимости разного уровня критичности. Положительным результатом тестирования считается отсутствие удачных попыток получить доступ к системе, данным в ней, а также отсутствие отказов в работе ОС и ее компонентов. Под пассивным тестированием подразумевается анализ конфигурационных файлов ОС, ее компонентов и установленного в базовой поставке программного обеспечения. Положительным результатом такого тестирования будет отсутствие уязвимостей, связанных с недостаточной настройкой объекта тестирования.

В качестве дополнительных критериев оценки предлагаются следующие:

1 Доступность исходного кода ОС и всех ее компонентов для изучения и анализа. Открытый исходный код позволяет быстрее обнаруживать критические и важные уязвимости, а также исправлять уже найденные.

2 Частота поставки стабильных обновлений для ОС и ее компонентов. В том числе возможность устанавливать только обновления безопасности, содержащие исправление ошибок и устраняющие уязвимости.

3 Отношение обнаруженных уязвимостей ОС и ее компонентов за определенный период к устраненным. Данная метрика позволяет оценить скорость реагирования компании-владельца ОС на найденные уязвимости в ОС и ее компонентах.

4 Публичность раскрытия факта обнаружения уязвимости в ОС и ее компонентах со стороны компании-владельца ОС. Своевременное оповещение о найденной уязвимости позволит предпринять некоторые действия для предотвращения угрозы безопасности.

Список использованных источников:
1.Информационная безопасность / Шаньгин В.Ф. // М.: ИНФРА-М, 2011. – с. 174.

UDC 004.451

ASSESSMENT OF THE OPERATING SYSTEM SECURITY

Muradov E.K., Master Student of the group 067241

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Petrov S.N. – PhD

Annotation. The main criteria for assessing of the operating systems security are presented.

Keywords. Information security, operating system, security assessment.

УДК 681.3

ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ПУТЕМ СОЗДАНИЯ РЕЧЕПОДОБНЫХ ПОМЕХ

Шакин К.П., магистрант группы 067241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Аннотация. Предложена структурная схема программного модуля защиты речевой информации путем создания речеподобных помех. Рассмотрен способ синтеза речи на основе компиляционного метода.

Ключевые слова. Защита информации, речеподобная помеха.

Существуют пассивные и активные способы защиты речи от несанкционированного прослушивания. Пассивные предполагают ослабление непосредственно акустических сигналов, циркулирующих в помещении, а также продуктов электроакустических преобразований в соединительных линиях ВТСС, возникающих как естественным путем, так и в результате ВЧ навязывания. Активные предусматривают создание маскирующих помех, подавление аппаратов звукозаписи и подслушивающих устройств, а также уничтожение последних.

Технический канал утечки информации образуют: источники конфиденциальной информации (люди, технические устройства), среда распространения (воздух, ограждающие конструкции помещений, трубопроводы), средства съема (микрофоны, стетоскопы).

Для защиты помещений применяют генераторы белого или розового шума и системы вибрационного зашумления. Качество этих систем оценивают превышением интенсивности маскирующего воздействия над уровнем акустических сигналов в воздушной или твердой средах. Величина превышения помехи над сигналом регламентируется руководящими документами. Известно, что наилучшие результаты дает применение маскирующих колебаний, близких по спектральному составу информационному сигналу. Шум таковым сигналом не является, кроме того, развитие методов шумоочистки в некоторых случаях позволяет восстанавливать разборчивость речи до приемлемого уровня при значительном (20 дБ и выше) превышении шумовой помехи над сигналом. Следовательно, для эффективного маскирования помеха должна иметь структуру речевого сообщения.

Для разработки такого устройства защиты речевой информации предлагается использовать систему синтеза речи на основе компиляционного метода, главная идея которого заключается в соединении готовых, заранее подготовленных, минимальных речевых единиц. При использовании этой модели составляется база данных звуковых фрагментов, из которых в дальнейшем будет синтезироваться речь. Размер элементов синтеза, как правило, не меньше слова. В ходе реализации программного модуля защиты речевой информации применяется система синтеза речи, у которой в качестве минимальной акустической единицы используется аллофон.

Систему синтеза речи целесообразно разбить на два больших модуля, это модуль обработки естественного языка и модуль обработки цифрового сигнала.

1. Модуль обработки естественного языка выполняет анализ и обработку входного орфографического текста. Непосредственно в прикладных системах модуль естественного языка делится на три подмодуля: лингвистической, фонетической и просодической обработки.

В подмодуль лингвистической обработки включены такие функции, как очистка текста, расшифровка числительных, даты и времени, аббревиатур, сокращений, Интернет ресурсов, автоматическая расстановка ударений, объединение слов в акцентные группы и членение на синтагмы.

В подмодуле фонетической обработки выполняется автоматическое транскрибирование текста в фонемный вид, а затем фонемного текста в аллофонный.

При этом ударные гласные маркируются индексом 0, предударные индексом 1, заударные индексом 2. В служебных словах ударная гласная маркируется индексом 5, а порядок индексирования заударных и предударных при их наличии остается прежний.

Просодическое оформление текстовой информации, в лингвистической обработке, заключается в сопоставлении интонационных контуров к соответствующим типам синтагм. Для этого необходимо классифицировать акцентные группы и разделить их на составляющие.

2. Модуль обработки цифрового сигнала заключается лишь в акустическом подмодуле. Основная задача акустического модуля – генерация (синтез) речевого сигнала на основе трех типов параметров:

просодических параметров (F0 – частота основного тона, Т – длительность звуков, А – амплитуда звуков), которые поступают от просодического подмодуля;

фонетических параметров, поступающих от фонетического подмодуля (в зависимости от типа фонетического процессора эти параметры могут быть различными: формантными параметрами (FI, F2, A1 ...), параметры сечений речевого тракта, номер аллофона или сегмента и т.д.);

параметры синтезируемого голоса, обеспечивающие желаемую тембровую индивидуальность.

В заключении стоит отметить, что этот способ обеспечивает высокое качество синтезируемой речи, т. к. позволяет воспроизводить форму естественного речевого сигнала. Еще один немаловажный плюс такого подхода: не требуется никаких знаний об устройстве речевого тракта и структуре языка.

Список использованных источников:

1. Фролов А., Фролов Г. Синтез и распознавание речи. – М.: Москва, 2008 г.

2. Рыбин С.В. Синтез речи.- СПб: Университет ИТМО, 2014.

3. Киселев В.В, Лобанов Б.М. Доклады БГУИР, 2004 г.

4. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие. М: Горячая линия – Телеком, 2005 г.

UDC 681.3

SPEECH PROTECTION SOFTWARE MODULE BY CREATING SPEECH-LIKE INTERFERENCES

Shakin K.P., Master Student of the group 067241

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Zelmansky O.B. – PhD

Annotation. The block diagram of the program module for the protection of speech information by creating speech-like interference is proposed. A method of speech synthesis based on the compilation method is considered.

Keywords. Information protection, speech-like interference.

УДК 004.93'1

ВЫЯВЛЕНИЕ СЕТЕВОЙ РАЗВЕДКИ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

Шараев Н.П., магистрант гр. 967241

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Петров С.Н. – канд. тех. наук

Аннотация. Сетевая разведка является первой стадией таргетированной или APT атаки, обнаружение которой позволит заблаговременно выполнить поиск возможных уязвимостей и предпринять меры по снижению рисков. Среди возможных унифицированных методов проведения сетевой разведки выделяются сканирование информационной сети и портов транспортного уровня. Процесс обнаружения данных типов сканирования основан на алгоритмах машинного обучения, в частности, методах классификации, кластеризации и ансамблирования. Обучающий датасет генерируется на базе сетевого трафика, в котором присутствуют отдельные пакет (сегменты) сетевой разведки.

Ключевые слова. Сетевая разведка, APT атака, машинное обучение.

В последнее время наблюдается тенденция перехода от массовых кибератак отдельных злоумышленников к масштабным атакам киберпреступных группировок на конкретные организации (таргетированные или APT атаки). Данные атаки в значительной мере опасны для организаций, что связано в первую очередь с созданием злоумышленниками вредоносного программного обеспечения с учетом специфики работы и сетевой инфраструктуры организации. В общем случае, APT атаки состоят из четырех этапов: подготовка, проникновение, распространение и достижение цели [1]. Обнаружить подобный тип атак на поздней стадии крайне сложно, а в отдельных случаях невозможно. По данной причине целесообразно провести обнаружение и анализ таргетированной атаки на этапе подготовки. На указанном этапе злоумышленники проводят процедуру сетевой разведки инфраструктуры организации. Сетевая разведка – это комплекс мероприятий, направленных на получения сведений об информационных системах, средствах защиты информации и используемом программном обеспечении [2].

Сетевая разведка может проводиться следующим образом:

– получение информации от whois-серверов (контактные данные владельца доменного имени, список DNS серверов и другое);

– получение информации от DNS серверов

– сканирование сети;

– сканирование портов транспортного уровня.

Наибольший интерес для обнаружения сетевой разведки представляют последние два пункта: сканирование информационной сети и портов транспортного уровня (так как невозможно повлиять на первые два пункта). Для выявление данных способов проведения сетевой разведки с помощью машинного обучения проведен анализ генерируемого ими сетевого трафика и выделены метрики, представленные в таблице 1 [3].

Таблица 1 – Анализируемые метрики

	Название метрики	Описание метрики
	count	Отношение количества отправленных сегментов (дейтаграмм) с одного IP адреса к общему количеству сегментов (дейтаграмм) с различных IP адресов.
	udp	Отношение количества отправленных дейтаграмм с одного IP адреса к общему количеству отправленных с этого же IP адреса сегментов (дейтаграмм).
	tcp	Отношение количества отправленных сегментов с одного IP адреса к общему количеству отправленных с этого же IP адреса сегментов (дейтаграмм).
	tcp_syn	Отношение количества отправленных с указанным флагом сегментов (SYN, ACK, FIN, NULL, XMAS, MAIMON, OTHER) с одного IP-адреса к общему количеству отправленных с этого же IP адреса сегментов.
	tcp_ack	
	tcp_fin	
	tcp_null	
	tcp_xmas	
	tcp_maimon	

	tcp_other	
	uniq_ports	Отношение количества уникальных портов, на которые были отправлены сегменты с одного IP адреса, к общему количеству отправленных с этого же IP адреса сегментов.

На основе указанных метрик сгенерировано два набора данных (датасета). Оба датасета представлены в формате JSON в виде словарей. Первый датасет состоит из 4025 событий, является лабораторным и генерируется автоматически на основании функции псевдослучаных чисел (random). Второй датасет состоит из 600 событий и является эмпирическим, то есть основанным на реальном трафике. Два датасета разработаны по той причине, что создание одного качественного датасета с большим количеством эмпирических событий сетевой разведки крайне сложно и требует значительного промежутка времени. Под качеством имеется ввиду наличие событий, полученных от различных средств проведения сетевой разведки. В настоящее время наиболее популярными утилитами для его проведения являются Nmap (Windows и Linux) и masscan (Linux), что недостаточно для создания разнообразия.

Визуализации обоих датасетов с помощью метода главных компонент (PCA) представлены на рисунках 1 и 2.

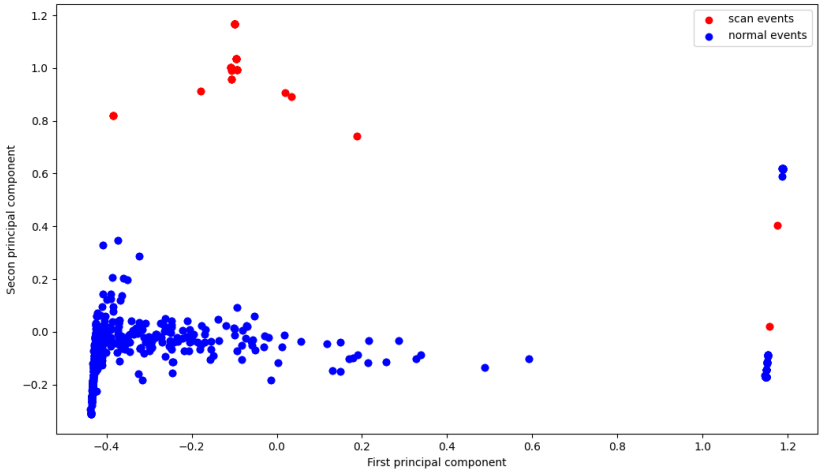


Рисунок 1 — Метод главных компонент для эмпирического датасета

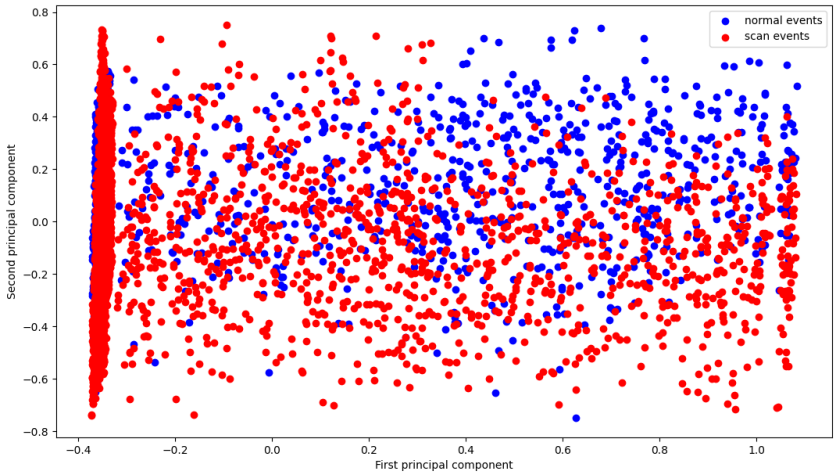


Рисунок 2 – Метод главных компонент для лабораторного датасета

Для обнаружения факта сетевой разведки выбраны методы машинного обучения, решающие задачи классификации и кластеризации. В основе алгоритмов классификации лежит тип машинного обучения с учителем, то есть создание правил по размеченным данным. Для целей настоящей работы используются следующие методы классификации: метод опорных векторов, метод логистической регрессии, гауссовский наивный байесовский классификатор, дерево принятий решений и многослойный персептрон. Данные алгоритмы были выбраны по причине простоты и скорости работы, а также высокой эффективности. В свою очередь решение задачи кластеризации

базируется на обучении без учителя (создание правил только по входным данным). В качестве методов кластеризации реализованы следующие алгоритмы: изолированный лес, метод обнаружение выбросов в гауссовском распределенном наборе данных, метод K-средних, пространственная кластеризация приложений с шумом на основе плотности (DBSCAN), метод сбалансированного итеративного сокращения и кластеризации с помощью иерархий (BIRCH). Указанные методы используются по причине их популярности, относительной простоты и скорости работы.

При обучении и тестировании эффективности методов машинного обучения оба датасета были дифференцированы на обучающую и тестовую выборку. Процентное соотношение для указанных выборок составляет 80% и 20% от общего количества событий соответственно. Для всех методов проведено обучение и измерение точности (accuracy). Точности обнаружения для лабораторного и эмпирического датасетов представлены в таблице 2.

Таблица 2 – Анализируемые методы машинного обучения

	Название метода	Сокращение	Тип метода	Точность лаб. датасета, %	Точность эмпир. датасета, %
	Метод опорных векторов	SVM	Классификация	92,42	100,00
	Метод логистической регрессии	LR		84,22	99,12
	Многослойный персептрон	MLP		92,52	100,00
	Гауссовский наивный байесовский классификатор	GaussianNB		76,40	99,12
	Дерево принятия решений	DecsicionTree		98,63	100,00
	Изолированный лес	IsolationForest	Кластеризация	61,87	87,72
	Метод обнаружения выбросов в гауссовском распределенном наборе данных	EllipticEnvelope		66,50	91,23
	Метод K-средних	KMeans		63,52	70,18
	Пространственная кластеризация приложений с шумом на основе плотности	DBSCAN		69,63	92,98
	Метод сбалансированного итеративного сокращения и кластеризации с помощью иерархий	BIRCH		65,26	98,25

Самыми перспективными методами обнаружения для классификации и кластеризации являются Дерево принятий решений и метод BIRCH соответственно. Тем не менее, эффективность указанных выше алгоритмов можно увеличить и стабилизирована путем использования ансамблей. Одинаковые алгоритмы (например, задачи классификации) могут быть объединены в один ансамбль, предназначенный для исправления ошибок друг друга. Так, несколько не очень эффективных методов обучения могут показать результат выше, чем каждый

метод в отдельности. При этом в ансамбль обычно объединяют алгоритмы максимально не стабильные и сильно зависящие от входных данных, в частности, регрессию и дерево принятия решений. Данная практика позволяет стабилизировать их результат несмотря на возможное наличие сильных аномалий в множестве входных объектов. Выделяют следующие виды ансамблей [4]:

– стекинг (stacking);
– бэггинг (bootstrap aggregating);
– бустинг (boosting).

Дополнительное применение алгоритмов бустинга (AdaBoost) или бэггинга для алгоритма Дерево принятия решения показало уменьшение точности (в среднем на 0,6%), что связано со стабилизацией результатов работы алгоритма. Применение указанных методов на алгоритм BIRCH не дало результатов по причине неустойчивости алгоритмы AdaBoost к выбросам. В дальнейшем планируется перейти на алгоритм градиентного бустинга (GBM).

Стоит отметить, что формально метод BIRCH является более подходящим для обнаружения факта сетевой разведки, так как нацелен на поиск аномалий в сетевом трафике. В то же время алгоритм Дерева принятия решений дает большую точность и позволяет описать условия обнаружения сетевой разведки языком программирования. В этой связи для дальнейших исследований предлагается выбрать лучший метод обнаружения признаков сетевой разведки используя практический подход, то есть разработать программное обеспечение, перехватывающее сетевой трафик и анализирующее его с использованием двух описанных алгоритмов.

Список использованных источников:

1. Левцов, В. Ю. Анатомия таргетированной атаки. Часть 1 / В.Ю. Левцов, П. Демидов // Системный администратор. – 2016. – №4 (161).

2. Шараев, Н. П. Обнаружение признаков сетевой разведки с использованием машинного обучения / Шараев Н. П., Петров С. Н. // Современные средства связи : материалы XXV Междунар. науч.-техн. конф., 22–23 окт. 2020 года, Минск / Белорусская государственная академия связи ; редкол.: А. О. Зеневич [и др.]. – Минск : БГАС, 2020. – С. 209-210.

3. Шараев, Н. П. Выявление и анализ признаков сетевой разведки методом машинного обучения / Шараев Н. П., Петров С. Н. // Управление информационными ресурсами: материалы XVII Междунар. науч.-практ. конф., 12 мар. 2021 года, Минск / Акад. упр. при Президенте Респ. Беларусь ; редкол. : А. С. Лаптенок. – Минск: Академия управления при Президенте Республики Беларусь, 2021. – С. 238-240.

4. Игнатов Д. И. Ансамблевый метод машинного обучения, основанный на рекомендации классификаторов / Д. И. Игнатов, Ю. С. Кашницкий // Интеллектуальные системы. Теория и приложения. – 2015. – Т. 19. – № 4. – С. 37-55.

UDC 004.93'1

IDENTIFICATION OF NETWORK INTELLIGENCE BY MACHINE LEARNING METHODS

Sharaev N.P., Master Student of the group 967241

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Petrov S.N. – PhD

Annotation. Network reconnaissance is the first stage of a targeted or APT attack, the detection of which will allow you to search for possible vulnerabilities in advance and take measures to mitigate the risks. Among the possible unified methods of conducting network reconnaissance, scanning the information network and ports of the transport layer stand out. The detection process for these scan types is based on machine learning algorithms, in particular, classification, clustering and ensemble methods. The training dataset is generated on the basis of network traffic, in which there are separate packet (s) of network intelligence.

Keywords. Network intelligence, APT attack, machine learning.

УДК 681.3

ПОМЕХОУСТОЙЧИВАЯ ПЕРЕДАЧА ДАННЫХ ПО РАДИОКАНАЛУ В ТЕЛЕМЕТРИЧЕСКОЙ СИСТЕМЕ

Шилко К.Н., магистрант; Паскробка Г.С., магистрант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белошицкий А. П. – канд. техн. наук

Аннотация. Доклад посвящен проблеме повышения защищенности телеметрической информации от несанкционированного доступа и помех структурно-алгоритмическими методами. Рассматриваются особенности, возникающие при передаче телеметрической информации по радиоканалу. Для устранения возникающих искажений предлагается использовать избыточность.

Ключевые слова. Помехоустойчивое кодирование, телеметрическая система, шифрование.

В системах передачи телеметрический информации между летательным или иным объектом и наземным приемным пунктом важное значение имеет помехозащищенность и информационная защита данных при передаче их по радиоканалу.

При разработке способов передачи телеметрической информации по радиоканалу необходимо учитывать следующие факторы передачи сигнала [1]: распространение, дальность и покрытие.

Распространение: Путь и способ, который радиоволна проходит от ее источника (передатчик) до места назначения (приемник). Путь распространения различается в зависимости от частоты радиосигнала. Также он зависит от частоты преломления или отражения радиосигнала от объектов или при прохождении через слои ионосферы.

Дальность: расстояние, на котором качество радиосвязи является достаточным для решения конкретной задачи.

Покрытие: доступность радиосигнала на ожидаемой дальности, когда сигнал не блокирован техногенными или природными преградами.

Эти факторы необходимо учитывать при выборе диапазона частот телеметрической системы, ее технической реализации, методов и способов передачи и обработки информации.

Обобщенная структурная схема телеметрической системы представлена на рисунке 1. Блоки сбора и передачи данных расположены на объекте телеметрии, а блоки приема и обработки данных – у получателя.

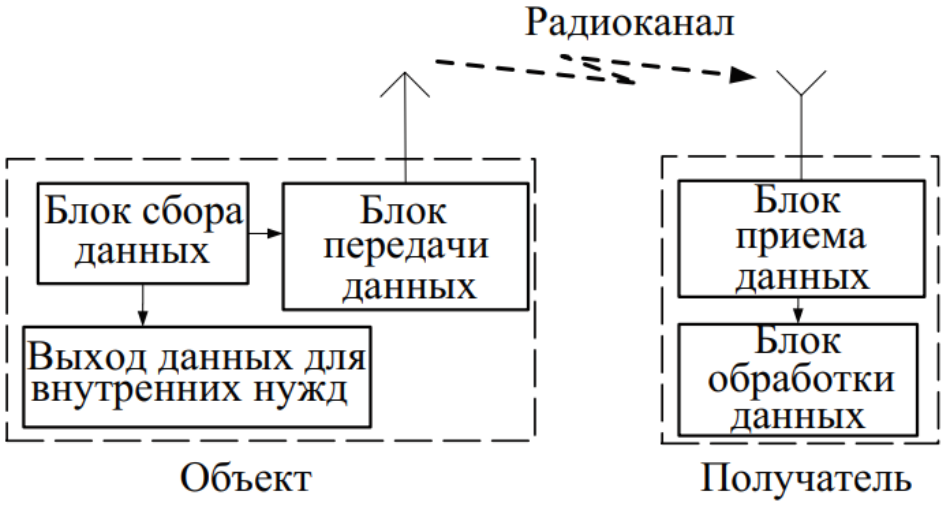


Рисунок 1 – Обобщенная структурная схема телеметрической системы

В системах цифровой передачи данных информации при прохождении сигнала по каналу передачи данных (рисунок 2) сигнал подвергается различным изменениям (искажениям) под действием шумов [1,2]. Это ведет за собой нарушение целостности передаваемой информации и может привести к сбоям в работе.

Рисунок 2 – Обобщенная структурная схема канала передачи данных телеметрической системы

Для контроля целостности данных предлагается использовать циклические избыточные коды (CRC). Алгоритм CRC базируется на свойствах деления с остатком двоичных многочленов, то есть многочленов над конечным полем $GF(2)$. Значение CRC является по сути остатком от деления многочлена, соответствующего входным данным, на некий фиксированный порождающий многочлен. Количество различных многочленов степени, меньшей N, равно 2^N, что совпадает с числом всех двоичных последовательностей длины N. Значение контрольной суммы в алгоритме с порождающим многочленом $G(x)$ степени N определяется как битовая последовательность длины N, представляющая многочлен $R(x)$, получившийся в остатке при делении многочлена $R(x)$, представляющего входной поток бит, на многочлен $G(x)$:

$$R(x) = P(x) * x^n \bmod G(x) \quad (1)$$

Где $R(x)$ – многочлен, представляющий значение CRC, $P(x)$ – многочлен, коэффициенты которого представляют входные данные, $G(x)$ – порождающий многочлен, N – степень порождающего многочлена.

Для защиты данных от несанкционированного доступа предлагается использовать шифр AES128. AES – блочный шифр с длиной блоков равной 128 битам, и шифр поддерживает ключи длиной N_k, равной 128, 192 или 256 бит.

В начале зашифровывания input копируется в массив State по правилу $state[r,c] = input[r+4c]$, для $0 \le r \le 4$ и $0 \le c \le Nb$. После этого к State применяется процедура AddRoundKey(), и затем State проходит через процедуру трансформации (раунд) 10, 12, или 14 раз (в зависимости от длины ключа), при этом надо учесть, что последний раунд несколько отличается от предыдущих. В итоге, после завершения последнего раунда трансформации, State копируется в output по правилу $output[r+4c] = state[r,c]$.

В помехоустойчивом кодировании широко применяется код Рида – Соломона. При использовании этого кода на выходе кодера образуется избыточное сообщение для дальнейшей передачи. В кодах Рида-Соломона сообщение представляется в виде набора символов некоторого алфавита. При построении кода Рида-Соломона задается пара чисел N, K, где N – общее количество символов, а K – «полезное» количество символов, остальные $N-K$ символов представляют собой избыточный код, предназначенный для восстановления ошибок. Структура данных в этом случае имеет вид, представленный на рисунке 3.

Рисунок 3 – Структурная схема пакета данных

Такой код будет иметь так называемое «расстояние Хэмминга» D = N–K+1; Расстояние Хэмминга является параметром кода и определяется как минимальное число различий между двумя различными кодовыми словами. В соответствии с теорией кодирования, код, имеющий расстояние Хемминга D = 2t+1, позволяет восстанавливать t ошибок данных при передаче по радиоканалу в телеметрической системе.

Для оценки достоверности передачи с использованием помехоустойчивого кодирования и без него использовалась среда имитационного моделирования MATLAB. Установлено, что применение кодирования позволяет повысить достоверность при передаче информации через канал передачи данных. Преимуществами использования выбранных кодов являются: простота реализации, кодирование и декодирование потоков данных непрерывно во времени, возможность обнаруживать и частично восстанавливать практически уничтоженную информацию.

Список использованных источников:

1. Рихтер С.Г. Кодирование и передача речи в цифровых системах подвижной радиосвязи. – М.: Горячая линия – Телеком, 2018. – 302 с.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

UDC 681.3

INTERFERENCE DATA TRANSMISSION ON A RADIO CHANNEL IN A TELEMETRIC SYSTEM

Shilko K.N., Master Student; Paskrobka G.S., Master Student

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Beloshitskiy A.P.– PhD

Annotation. The report is devoted to the problem of increasing the security of telemetric information from unauthorized access and interference by structural and algorithmic methods. The features that arise during the transmission of telemetric information over a radio channel are considered. To eliminate the arising distortions, it is proposed to use redundancy.

Keywords. Anti-jamming coding, telemetry system, encryption.

УДК 004.428.4:004.4'242

РЕАЛИЗАЦИЯ ИНФРАСТРУКТУРЫ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ С ПОМОЩЬЮ IAC

Шуба М.А., студент гр. 961402

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В данной работе представлен сравнительный анализ различных облачных технологий, проведено изучение принципов работы с облачными технологиями на основе IAC и Terraform, практически реализована инфраструктура для веб-приложения, которая может быть использована как основа для различных веб-приложений с широким спектром использования.

Ключевые слова. Веб-приложения, инфраструктура как код, программируемая инфраструктура, облачные технологии, DevOps, AWS, IAC, Terraform.

Под облачными технологиям понимают технологии распределенной обработки цифровых данных, с помощью которых компьютерные ресурсы предоставляются интернет-пользователю как онлайн-сервис.

К основным преимуществам облачных технологий относят следующее:

– возможность получения удаленного доступа из любой точки мира;

– снижение капитальных расходов на приобретение и установку оборудования и программного обеспечения, их обслуживание;

– удобство и простота доступа и обслуживания сервисов;

– мгновенное масштабирование потребляемых ресурсов в зависимости от изменения нагрузок

– быстрое обновление используемого программного обеспечения;

– повышенная безопасность и надежность работы.

DevOps (Development Operations) – это движение, возникшее в 2008 году с целью решить проблемы взаимодействия команд разработки и эксплуатации, которые приводили к увеличению времени разработки и тестирования приложений, появлению большого числе версий и изменений, что отражалось на качестве работы самого приложения. DevOps выступает в качестве связующего звена между командой разработчиков и командой эксплуатации. Условно, в DevOps можно выделить несколько ролей:

– Build Engineer – специалист, отвечающий за сборку кода, обнаружение ошибок в коде;

– Release Engineer – специалист, отвечающий за доставку кода от разработки в реализацию;

– Automation Engineer – инженер по автоматизации сборки кода, тестов и др;

– Security Engineer – специалист, который отвечает за проведение тестов на проникновение (пентестов) и изучение уязвимостей в используемых компонентах.

На сегодняшний день в мире облачных технологий крупнейшими облачными платформами являются Amazon Web Services, Microsoft Azure, Google Cloud Platform, Becloud.

Среди перечисленных наиболее распространенной в мире облачной платформой с самыми широкими возможностями является Amazon Web Services, которая предоставляет 165 полнофункциональных сервисов для центров обработки данных по всей планете. Данная платформа предоставляет такие сервисы как хранилища баз данных, сетевых конфигураций, машинного обучения и искусственного интеллекта интернета вещей (IoT) и др.

В свою очередь платформа Microsoft Azure предоставляет возможность разработки, выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центра.

Google Cloud Platform (GCP), предлагаемая Google, представляет собой набор сервисов облачных вычислений, которые работают на той же инфраструктуре, которую Google использует для своих продуктов для конечных пользователей, таких как Google Search и YouTube . Наряду с набором инструментов управления, она обеспечивает ряд модульных облачных сервисов, включая вычисления, хранения, анализа данных и машинного обучения.

Также нужно отметить платформу поставщика облачных решений BeCloud, который является одним из ведущих провайдеров в Беларуси. BeCloud занимаемся проектированием, строительством, оснащением и эксплуатацией следующих ключевых для белорусского ИТ-рынка проектов: опорная сеть передачи данных для Единой республиканской сети передачи данных (ЕРСПД), Республиканский центр обработки данных (РЦОД), развитие и тестирование высокоскоростного мобильного интернета 5G и др. Выбор AWS обоснован тем, что облачный

сервис предоставляет несравнимо больше сервисов и их функций, чем любой другой поставщик облачных услуг: от инфраструктурных технологий, таких как инструменты для вычисления, хранилища и базы данных, до инноваций, например машинного обучения и искусственного интеллекта, аналитики, а также Интернета вещей. AWS также предоставляет самые широкие функциональные возможности для своих сервисов, например, AWS предлагает на выбор много баз данных, специально созданных для различных типов приложений, чтобы клиент мог подобрать правильный инструмент для эффективной работы.

В рамках данной работы была изучена возможность создания виртуальной машины с операционной системой Windows в AWS и инфраструктуры веб-приложения с помощью IAC.

Часто привлекательным является распространение инфраструктуры по нескольким облакам для повышения отказоустойчивости. При использовании только одного региона или облачного поставщика отказоустойчивость ограничена доступностью этого поставщика. Развертывание в нескольких облаках позволяет более плавно восстанавливать потери региона или всего провайдера.

Реализация развертывания в нескольких облаках может быть очень сложной, так как многие существующие инструменты для управления инфраструктурой являются облачными. Terraform – это инструмент для безопасного и эффективного построения, изменения и создания версий инфраструктуры. Terraform может управлять существующими и популярными поставщиками услуг, а также индивидуальными собственными решениями. Terraform не зависит от облаков и позволяет использовать единую конфигурацию для управления несколькими провайдерами и даже для обработки межоблачных зависимостей. Это упрощает управление и оркестровку, помогая операторам создавать крупномасштабные мультиоблачные инфраструктуры.

Файлы конфигурации описывают для Terraform компоненты, необходимые для запуска одного приложения или всего центра обработки данных. Terraform генерирует план выполнения, описывающий, что он будет делать для достижения желаемого состояния, а затем выполняет его для построения описанной инфраструктуры. По мере изменения конфигурации Terraform может определить, что изменилось, и создать дополнительные планы выполнения, которые можно применять. Инфраструктура, которой может управлять Terraform, включает в себя компоненты низкого уровня, такие как вычислительные экземпляры, хранилище и сеть, а также компоненты высокого уровня, такие как записи DNS, функции SaaS и т. Д.

В рамках данной работы была реализована инфраструктура для веб-приложений на основе модели «Инфраструктура как код (IaC)», которую иногда называют «программируемой инфраструктурой». Суть данной модели заключается в том, что процесс настройки инфраструктуры аналогичен процессу программирования ПО. По сути, она положила начало устранению границ между написанием приложений и созданием сред для этих приложений. Приложения могут содержать скрипты, которые создают свои собственные виртуальные машины и управляют ими. Это основа облачных вычислений и неотъемлемая часть DevOps. Инфраструктура как код позволяет управлять виртуальными машинами на программном уровне. Это исключает необходимость ручной настройки и обновлений для отдельных компонентов оборудования. Инфраструктура становится воспроизводимой и масштабируемой. Оператор может выполнять развертывание и управление как одной, так и 1000 машинами, используя один и тот же набор кода. Среди гарантированных преимуществ инфраструктуры как кода можно отметить высокую скорость, экономичность и уменьшение риска.

Таким образом, в AWS с помощью Terraform была создана инфраструктура для веб-приложения, которая имеет широкий спектр применения. Написание кода для Terraform может осуществляться на YAML и JSON. При добавлении клиентского интерфейса, алгоритма работы приложения и базы данных из данной инфраструктуры может получится любое WEB-приложение обеспечивающее связь клиента с базой данных через клиентский интерфейс.

Список использованных источников:

1. Облачные вычисления с помощью AWS / Amazon Web Services, Inc. [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/what-is-aws/?nc2=h_ql_le_int – Дата доступа: 10.02.2021.

2. Ветчинкин, К. Инфраструктура как код, выигрываем на масштабе / Habr [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/438748/ – Дата доступа: 10.02.2021.

3. Deliver Infrastructure as Code / HashiCorp [Электронный ресурс]. – Режим доступа: https://www.terraform.io/ – Дата доступа: 10.02.2021.

UDC 004.428.4:004.4'242

IMPLEMENTATION OF WEB APPLICATION INFRASTRUCTURE BASED ON CLOUD TECHNOLOGIES VIA IAC

Shuba M.A., Student of the Group 961402

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Belousova E.S. – PhD

Annotation. This paper presents a comparative analysis of various cloud technologies, the principles of working with cloud technologies based on IAC and Terraform were studied, infrastructure for a web application was practically implemented, it can be used as a basis for various web applications with a wide range of uses.

Keywords. Web-application, Infrastructure as Code, IAC, Programmable Infrastructure, Cloud Technologies, DevOps, AWS, Terraform.

UDC 681.3

ANALYSIS OF BASIC SPEECH INFORMATION FOR CONSTRUCTING SPEECH-LIKE NOISE

Amiry Homayoon, Master Student

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vrublevsky I. – PhD

Annotation. The main stages of creating speech-like noise signal for means of vibroacoustic protection of speech information based on the phonetic-acoustic base and words of the Russian language are considered. The choice of jamming signal of the speech chorus type is described.

To generate speech-like noise, the synthesis of sound signals is used by random sampling of speech elements from the generated database. The advantage of the method is the generation of a noise signal shape with a spectrum envelope similar to a speech signal and a similar signal structure [1]. In this case, the task of separating the noise signal from the useful signal becomes more complicated, which makes it possible to increase the overall stability of the speech information protection system [2]. Investigations in the field of psychoacoustics have shown that the most effective type of noise signal is “speech chorus” [3].

The formation of speech-like noise signal included several stages. At the first stage of the formation of speech-like noise signal, a speech array was created, including a set of Russian words and containing all the necessary allophones. The sound array of the text and the formed phonetic-acoustic database are input data for the synthesis and subsequent allophonic marking of the speech signal. The synthesized speech signal is used for segmentation and allophone marking of natural speech signal. The next stage was listening with a possible manual adjustment of the boundaries of the allophones. For the first stage, a phonetic-acoustic database of the speaker with the necessary set of allophones was formed. In Russian, there are 42 phonemes, of which 6 are vowels and 36 consonants. In the flow of speech, phonemes, depending on the environment, can change their acoustic characteristics, which leads to the appearance of their modifications (allophones). For systematization, each allophone was placed in a separate file. The following designations were adopted: the first character in the file name was a letter forming a sound, then three indices followed in the name, characterizing the position of the allophone. After compiling a database of allophones, software was used that accepts an array of created files as input. Then the synthesis and reproduction of the input text took place using the recorded allophones. The “speech chorus” noise was formed similarly to the speech-like noise with the overlapping of the voices of several speakers at the same time.

References:

1. Trushin V.A., Ivanov A.V. Possibilities of reducing the integral level of interference in the means of active protection of information of speech information (state and prospects) // Doklady TUSUR. – 2018. – Vol. 21, No. 2. – P. 38–42. (In Russ.)

2. Blintsov V., Nuzhniy S., Kasianov Y., Korytskyi V. Development of a mathematical model of scrambler-type speech-like interference generator for system of prevent speech information from leaking via acoustic and vibration channels // Technology audit and production reserves.– 2019. – Vol. 5, No. 2(49). – P. 19–26.

3. Davydau H.V. et al. Method for protecting speech information // Doklady BGUIR. – 2015. – Vol. 8 (94). – P. 107–110.

UDC 681.3

MODEL REPRESENTATION OF VIBROACOUSTIC CHANNELS OF SPEECH INFORMATION LEAKAGE

Hasani Ahmed Nezar Salih, Master Student

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vrublevsky I. – PhD

Annotation. The vibroacoustic channel of speech information leakage in the protected room is considered. It is shown that the spectrum of speech signals can overlap with a set of a number of natural resonant frequencies for the enclosing structural elements.

When considering the vibroacoustic channel of speech information leakage in the protected room, it was assumed that the source of information is a person, and the propagation medium is air. The speech signal is created by the human voice, which causes vibrations of the air environment in the form of acoustic vibrations [1–3]. In the calculations, the speech signal range was taken to be 300–400 Hz.

The mathematical description of the process of spreading speech information behind the enclosing structural elements was built using an approximation in the form of a rectangular plate for such structures as a wall, floor, ceiling. By solving the differential equation in partial derivatives of the transverse vibrations of a rectangular plate, the frequencies of natural vibrations of the plate are determined for the case of gypsum blocks of given sizes and characteristics.

It is shown that the spectrum of speech signals can be overlapped by a set of a number of natural resonance frequencies for the enclosing structural elements. As a result, an acoustic wave with speech information is generated, which is excited by the reverse side of the enclosing structure. Thus, the vibrations are unevenly distributed throughout the structure. There are certain areas with maximum values of natural vibrations. Such areas with maximum natural vibrations of structures must be localized by placing a vibration transducer to generate an interference signal.

References:

1. Dvorjankin S.V., Harchenko L.A., Kozlachkov S.B. Estimation of security of voice information based on modern technology for noise reduction // Voprosy zashhity informacii. – 2007. – No. 2 (77). – P. 37–40. (In Russ.).

2. Horev A.A. Technical protection of information: Uchebnoe posobie dlja studentov vuzov. – M.: NPC Analitika, 2008. – Vol. 1. –436 p. (In Russ.)

3. Davydau H.V. et al. Method for protecting speech information // Doklady BGUIR. – 2015. – Vol. 8 (94). – P. 107–110.

СЕКЦИЯ «СИСТЕМЫ РАСПРЕДЕЛЕНИЯ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ»

Процесс Переноса корпоративных мультимедиа данных из локальных серверов в облачные сервисы

Желудкович В.В., магистрант гр.067041

Белорусский государственный университет информатики и радиоэлектроник
г. Минск, Республика Беларусь

Бобов М.Н. – профессор, доцент технических наук

Аннотация. В докладе рассмотрены основные принципы алгоритма переноса корпоративных мультимедиа данных на облачные сервисы, независимо от версий операционных систем, а также обеспечение сохранности всех уровней доступа сотрудников компаний с минимальными финансовыми и трудовыми затратами, а также обеспечение удалённого безопасного доступа ко всем данным находящимся в облачных сервисах

Ключевые слова. Microsoft, windows server, office 365, active dirrectory, локальный сервер, резервное копирование.

В быстроразвивающемся мире, существующие корпоративные решения в области хранения и взаимодействия с корпоративными данными перестают быть актуальными и не отвечают требованиям безопасности, отсутствует возможность обновления. В связи с этим компания теряет способность сохранять свои данные в безопасности. А также существует ряд проблем, которые компания испытывает, поддерживая устаревшую структуру хранения данных. На примере одной из существующих страховых компаний рассмотрим возникающие проблемы.

Компания имеет следующую структуру хранения данных:

1. Локальный сервер, развернутый на территории предприятия
2. Высокоскоростной интернет, установленный для подключения сервера к сети.
3. Настроенное Vpn подключение для удалённого безопасного доступа сотрудников компании

Вышеописанная структура несёт за собой ряд проблем.

Создание и поддержка локального сервера требует затрат на оборудование, высокоскоростной интернет, сотрудников, осуществляющих поддержку и обслуживание. При возникновении проблем на стороне сервера у всей компании отсутствует доступ к данным, что может негативно повлиять на деятельность компании.

Сотрудникам компании, на стороне пользователя, необходимо постоянное подключение к интернету, для возможности доступа к корпоративным данным, что несёт за собой затраты на техническую поддержку пользователей, обеспечение интернетом и необходимым программным обеспечением для доступа к локальному серверу.

Уязвимая система безопасности, которая обеспечивается, только по средствам VPn подключения. На стороне сервера, как правило безопасность обеспечивается инженерами системы безопасности и их собственной логикой защиты сервера, что в свою очередь несёт затраты на квалифицированные кадры и не даёт гарантии в применяемых ими решений.

Всё вышеописанное заставляет прибегать к новым средствам, которые обеспечат безопасность на высоком уровне, позволит иметь доступ к данным с любой точки мира, будет отсутствовать требование постоянного подключения к интернет сети, снизят затраты на поддержку оборудования и сотрудников технической поддержки.

Наилучшим решением для любой компании будет переход к облачным технологиям, которые обеспечат: должный уровень безопасности, объём памяти необходимый компании, защищенный доступ к данным без специального программного обеспечения с любой точки мира.

Наиболее подходящим решением будет переход к продукту от компании Microsoft, office 365. Данный продукт предоставляет следующие возможности:

1. Использование классических версий приложений Office: Outlook, Word, Excel, PowerPoint, OneNote (а также Access и Publisher только для компьютеров с Windows)
2. Хранение и совместное использование файлов в облачном хранилище OneDrive емкостью 1 ТБ на пользователя
3. Автоматические обновления приложений, позволяющие каждый месяц получать новые функции и возможности.
4. Круглосуточную службу поддержки Майкрософт по телефону или через Интернет.
5. Собрания и голосовая связь Teams
6. Социальные сети и интрасеть SharePoint, Yamer
7. Файлы и контент One Drive

А также Microsoft может оказать более расширенный пакет услуг в зависимости от требований разных клиентов.

Более подробно необходимо рассмотреть продукт SharePoint поскольку именно он будет выступать в роли будущего локального сервера. Здесь будут храниться общие данные. Microsoft выбрана не случайно, поскольку существует возможность переноса всей иерархии компании сохраняя уровни доступа сотрудников, организованные ранее на локальном сервере с помощью Active Dirrectory

Active Dirrectory позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager (ранее — Microsoft Systems Management Server), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя службу обновления Windows Server. хранит данные и настройки среды в централизованной базе данных. Сети Active Directory могут быть различного размера: от нескольких десятков до нескольких миллионов объектов.

Microsoft SharePoint — это облачная служба, которая помогает организациям обмениваться контентом, знаниями и приложениями и управлять ими для:

1. Расширения возможностей работы в команде.
2. Быстрого поиска информации в корпоративных данных.
3. Бесперебойной работы организации.

В зависимости от предпочтений компании, существует огромное количество предложений на рынке облачных технологий. На примере Microsoft рассмотрим процесс перехода из локального сервера на облачный.

Для начала необходимо произвести подсчет объёма необходимого будущего общего хранилища, количество пользователей. Объём необходимо брать с запасом, в зависимости от количества пользователей, объёма информации выгружаеваемого за промежуток времени. Желательно брать статистику за наибольший промежуток, поскольку в таком случае данные будут максимально приближены к реальным. К значению в пиковом периоде необходимо прибавить 20% для исключения форс мажорных обстоятельств. Например, резервной копирование баз данных бухгалтерии не удаляет старые резервные копии, в итоге мы получаем перегруженное хранилище. Если же объём памяти превышает пиковые значения на 20% системный администратор имеет большее количество времени для устранения неполадок, повышается отказоустойчивость всей системы. Далее необходимо произвести закупку учётных записей Microsoft 365(ранее office 365) в соответствии с рассчитанными ранее данными. Количество дополнительных услуг каждая компания выбирает в соответствии со своими возможностями и предпочтениями. Мы затронем только основную структуру.

На стороне локального сервера необходимо произвести обновление операционной системы не ранее Microsoft windows server 2016. поскольку миграция на облачный сервис сохраняя все настройки пользователей, групповых политик Active Dirrectory возможна только начиная с этой версии. Иначе необходимо будет назначать каждого пользователя в Microsoft share point вручную, что понесёт за собой затраты как материальные, так и временные. Обновление должен производить опытный системный администратор, поскольку при этом процессе также возможен сброс настроек групповых политик.

Переходя на облачные технологии, компания получает ряд преимуществ.

1. Высокая безопасность данных, обеспечивающаяся компанией, предоставляющей услуги облачных сервисов
2. Отсутствует необходимость установления стороннего ПО, для удалённого подключения.
3. Отсутствует необходимость в постоянном интернет соединении, поскольку облачный провайдер предоставляет возможность работы с данными на стороне пользователя в режиме, а при подключении к интернету внесённые пользователем изменения в данные переносятся в облако. Что в свою очередь даёт сотрудникам вести работу offline
4. Отсутствует необходимость в самом локальном сервере и его поддержке.

Список использованных источников:

1. Майкл Ноэл, Колин Спенс Microsoft SharePoint 2010. Полное руководство 2012г.-880с.
2. Рэнд Моримото "Microsoft Windows Server 2012. Полное руководство 2013г. -1456с.

УДК 654.16

МИКРОВОЛНОВЫЙ СЛУХОВОЙ ЭФФЕКТ ФРЕЯ

Калита С.О., студентка гр. 763101

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Аксёнов В.А. – ст. преподаватель

Аннотация. Описывается эффект возбуждения слуховых ощущений при облучении человека радиоволнами СВЧ. Эффект представляет интерес с точки зрения изучения возможного вредного влияния устройств сотовой связи на организм человека.

Ключевые слова: Фрей, сотовая связь, радиоволны СВЧ

Введение.СВЧ слуховой эффект, также известный как микроволновый слуховой эффект или эффект Фрея, состоит в восприятии человеком слышимых щелчков или даже речи, вызванных импульсными или модулированными радиочастотами. Коммуникации генерируются непосредственно внутри головы человека без необходимости использования каких-либо приемных электронных устройств.

Открытие микроволнового слухового эффекта.В 1956 г. было замечено, что люди, которые оказывались в зоне действия радиолокатора, начинали ощущать звуковые галлюцинации. Такой же эффект был, даже если уши были защищены подавляющими шум фильтрами. Испытуемые поочерёдно находились за экраном с отверстием диаметром в четверть длины волны на расстоянии 1,5…2,0 м от рупора антенны. Передатчик мощностью 500 КВт работал на частоте 1,3 ГГц, длительность импульса 2 мкс и частота следования 600 Гц (мощность приводится для радиоимпульса).

Результатом систематических наблюдений и первых исследований была работа Аллана Х. Фрея – «Реакция слуховой системы человека на модулированную электромагнитную энергию», которая была опубликована в Журнале прикладной физиологии в 1961 году.

Как утверждал Фрей, индуцированные звуки были описаны испытуемыми как «гудение, щелчки, шипение или стук, в зависимости от нескольких параметров передатчика, то есть ширины импульса и частоты повторения импульсов». Изменяя параметры передатчика, Фрей смог вызвать «ощущение сильного сотрясения головы без таких явных вестибулярных симптомов, как головокружение или тошнота». Другие же параметры передатчика вызывали парестезию. Парестезия – это ненормальное ощущение кожи без видимой физической причины. Парестезии обычно безболезненны и могут возникать на любом участке тела, но чаще всего возникают на руках и ногах. Самый известный вид парестезии – это ощущение, известное как «иголки». Менее известная и редкая, но важная парестезия – это ощущение ползания мурашек, ощущение, как насекомые ползают под кожей.

Гипотеза Аллана Фрея

Аланом Фреем была предложена гипотеза, что причиной является термоупругое расширение частей слухового аппарата, и общепринятым механизмом является быстрое (но незначительное, в диапазоне 10 °C) нагревание мозга каждым импульсом, и возникающая в результате волна давления, проходящая через череп, улитку. То есть, на участках внутреннего уха (рис. 1) происходит взаимодействие излучения с термоупругими тканями, сопровождающееся, возможно, их периодической деформацией. В ходе этого процесса при амплитудно-импульсной манипуляции возникают как бы механические ударные волны, воспринимаемые человеком в виде внутреннего звука, который никак не связан с колебанием барабанной перепонки. Этот сенсорно-акустический эффект представляет собой физическое явление, связанное с преобразованием электромагнитной энергии в низкочастотные механические колебания на пути к рецепторному аппарату путем костной звукопроводимости.

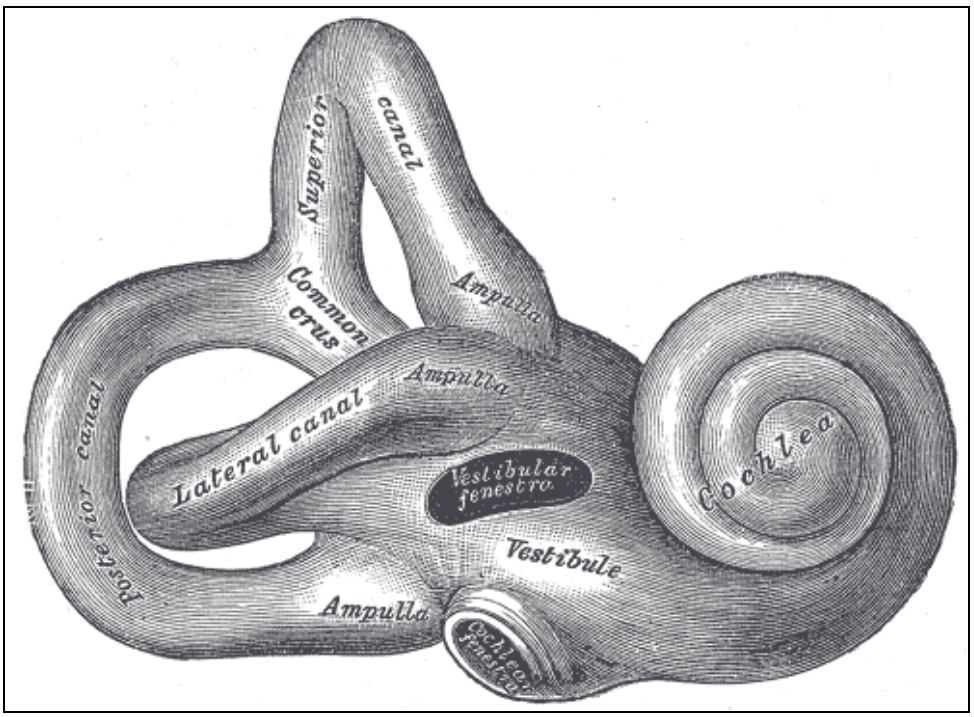


Рис. 1. Внутреннее ухо человека

Также было обнаружено, что при соответствующем выборе амплитудно-модулированного сигнала существует возможность передавать человеку информацию в виде отдельных слов, фраз и других звуков. Громкость воспринимаемого звука можно увеличить, но акустическую травму нанести невозможно, поскольку барабанная перепонка в процессе не участвует. Формирование же спектра, воспринимаемого человеком в виде слухового ощущения, определяется взаимодействием анатомических структур, представляющих как бы систему акустических резонаторов с динамической связью, выше критической.

В 1975 году в статье нейропсихолога Дона Юстесена, в которой обсуждается влияние радиации на человеческое восприятие, упоминается эксперимент Джозефа К. Шарпа и Марка Гроува из Армейского института Уолтера Рида. Проводилось исследования, в ходе которого Шарп и Гроув, как сообщается, смогли распознать девять из десяти слов, передаваемых «микроволнами с голосовой модуляцией». Поскольку уровни излучения приблизились к пределу безопасного воздействия по имевшимся тогда представлениям в 10 мВт/см², критики заметили, что в таких условиях может произойти повреждение мозга в результате теплового воздействия мощного микроволнового излучения. К тому же, не было «убедительных доказательств наличия слухового микроволнового эффекта при более низких температурах плотности энергии».

Заключение

К сожалению, микроволновый слуховой эффект до конца не изучен, однако он имеет потенциальное применение в слуховых аппаратах, в задачах беспроводной передачи информации, а также при создании нелетального оружия. Исследования и возможность применения ограничены потенциальной вредностью микроволнового излучения. Среди использующихся применений – устройства отпугивания птиц и термоакустическая томография, основанная на исследовании акустических волн, возникающих в результате локального теплового расширения тканей человеческого тела под действием микроволн.

Список литературы

1. Frey, Allan H. (July 1962). "Human auditory system response to modulated electromagnetic energy" [Электронный ресурс]. URL: https://mriquestions.com/uploads/
3/4/5/7/34572113/auditory_frey_rf_hearing_jappl.1962.17.4.689.pdf.

2. Frey A. H. (1961) Auditory system response to radio frequency energy. [Электронный ресурс]. URL: https://drive.google.com/file/d/0B3V8FIUj7brsYjg4ZGJiMTQtZjg1MC00Mz
U0LTg3ZWItOTQ4NzliYzVlYjQ3/view?hl=en&authkey=CKCPo7EK.

3. В. К. Баранов, Д. А. Кыдырбаева, Д. К. Тамбовцев. Механизм воздействия модулированного высокочастотного сигнала на неидеальный диэлектрик. Радиозвук. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/mehanizm-vozdeystviya-modulirovannogo-vysokochastotnogo-signala-na-neidealnyy-dielektrik-radiozvuk/viewer.

INFLUENCE OF MAN-MADE RADIO NOISE ON A RANGE OF A CELL, WHICH USES THE NARROW-BAND INTERNET OF THINGS

S.O. KALITA

Abstract. The analysis of the effect of excitation of auditory sensations when a person is exposed to microwave radiation. The effect is of interest from the point of view of studying the possible harmful effects of cellular communication devices on the human body.

Keywords: Frey, cellular communication, radio microwaves.

УДК 621.391

СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ IPS/IDS

Каплич А.А., магистрант гр. 967001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шевчук О.Г.. – канд. тех. наук, доцент

Аннотация. *Описаны системы обнаружения и предотвращения вторжений в сетевую инфраструктуру.*

Ключевые слова. Система обнаружения вторжений, система предотвращения вторжений, IPS, IDS.

Рассмотрим такой класс решений, как системы обнаружения вторжений и системы предотвращения вторжений. Данный класс средств защиты нацелен на выявление и регистрацию недостатков в безопасности внутренней инфраструктуры – сетевые атаки, попытки несанкционированного доступа, повышения привилегий, работа вредоносного ПО и т.д.

IDS состоит из сенсоров, которые просматривают сетевой трафик или журналы и передают анализаторам, анализаторы ищут в полученных данных вредоносный характер и в случае успешного обнаружения – отправляет результаты в административный интерфейс [1]. В зависимости от места расположения IDS делятся на сетевые (network-based IDS, NIDS) и хостовые (host-based, HIDS). В свою очередь IPS это программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них. Методы ее работы относятся к своевременным (превентивным) и проактивным, в отличие от IDS, выполняющей детективные функции. Возможность предотвращения атак реализована за счет того, что сетевая IPS, как правило, встраивается «в разрыв» сети и пропускает через себя весь трафик, а также имеет внешний интерфейс, на который приходит трафик и внутренний интерфейс, который пропускает трафик далее, если он признается безопасным [2]. Структурна схема IPS/IDS представлена на рисунке 1.

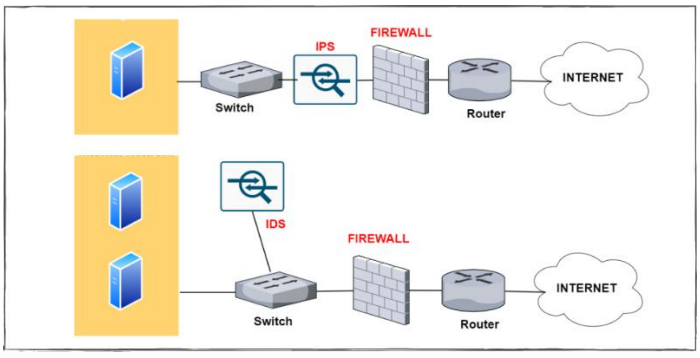


Рисунок 1 - Структурна схема IPS/IDS

Наиболее эффективной защиты инфраструктуры является совместное использование средств IDS и IPS в одном продукте – межсетевом экране, который с помощью глубокого анализа сетевых пакетов, обнаруживает атаки и блокирует их. Стоит отметить, что речь идет только об одном рубеже защиты, который, как правило, расположен за межсетевым экраном. И чтобы добиться комплексной защиты сети, необходимо использовать весь арсенал средств защиты, например,

UTM (Unified Threat Management) – совместно работающие межсетевой экран, VPN, IPS, антивирус, средства фильтрации и средства антиспама [3].

Список использованных источников:

1. Kruegel Christopher, Valeur Fredrik, Vigna Giovanni // Intrusion Detection and Correlation: Challenges and Solutions. 2005. P. 43–55.

2. Лукацкий А.В. // Обнаружение атак. 2001. P. 247–286.

3. Норткат С., Новак Д. // Обнаружение нарушений безопасности в сетях. 2003. P. 161–185.

INTRUSION DETECTION, PREVENTION SYSTEM

Kaplich A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Shevchuk O. G. – PhD in Technical, docent

Annotation. The systems for detecting and preventing intrusions into the network infrastructure are described.

Keywords. Intrusion detection system, intrusion prevention system, IPS, IDS.

ПРОГРАММНО-КОНФИГУРИРУЕМАЯ СЕТЬ SDN

Ковятинец И.П., Михнюк Д.Г., магистранты гр.967041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бобов М.Н. – доктор техн. наук., профессор

Аннотация. В данной работе представлены принципы работы и особенности функционирования программно-конфигурируемых сетей.

Ключевые слова. Программно-конфигурируемая сеть, SDN, виртуализация, OpenFlow.

В современном мире предъявляются большие требования к гибкости и масштабируемости компьютерных сетей. Новым подходом к построению информационных сетей является технология программно-конфигурируемых сетей (SDN).

Сеть SDN – это сеть передачи данных, в которой уровень управления и передачи разделяются за счет переноса функций на отдельное центральное устройство, называемое контроллером. За счет такого разделения управление и контроль состояния сети логически централизован. Такой подход позволяет уровню управления абстрагироваться от уровня передачи данных.

Архитектура сети SDN представлена на рисунке 1.

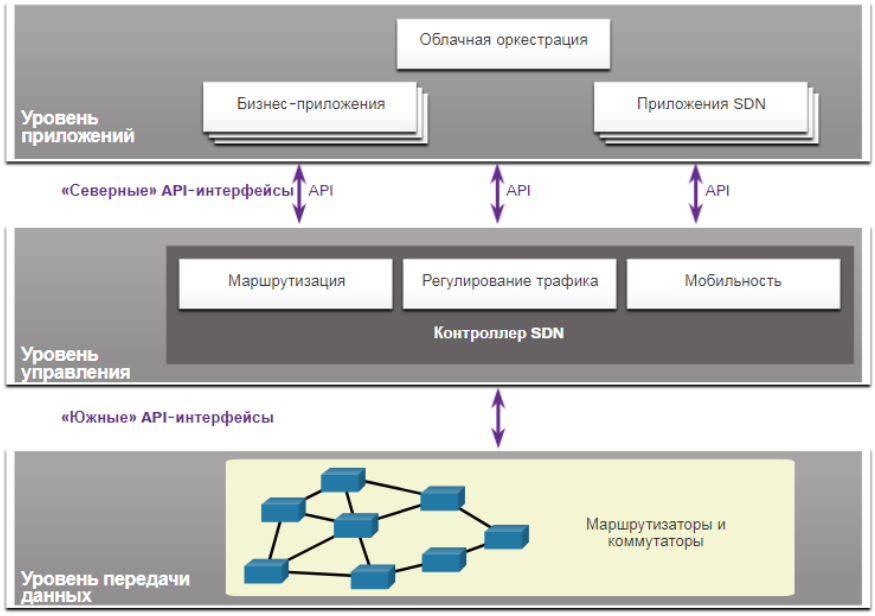


Рисунок 1 – Архитектура сети SDN

Архитектура сети SDN имеет три уровня. Уровень передачи данных включает в себя набор сетевых устройств и каналов передачи данных. На уровне управления отслеживается и поддерживается глобальное представление сети, работает программный интерфейс (API) для сетевых приложений. На уровне приложений реализуются различные функции управления сетью: управление потоками данных в сети, управление безопасностью, мониторинг трафика и управление качеством сервиса.

Наиболее перспективным и активно развивающимся стандартом для сетей SDN является OpenFlow. Данный протокол используется для управления сетевыми коммутаторами и маршрутизаторами с центрального устройства — контроллера сети. Это управление заменяет или дополняет работающую на коммутаторе либо маршрутизаторе встроенную программу, осуществляющую построение маршрута, создание карты коммутации и т. д. Контроллер используется для управления таблицами потоков, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами.

Принцип функционирования сети SDN на базе протокола OpenFlow представлен на рисунке 2.

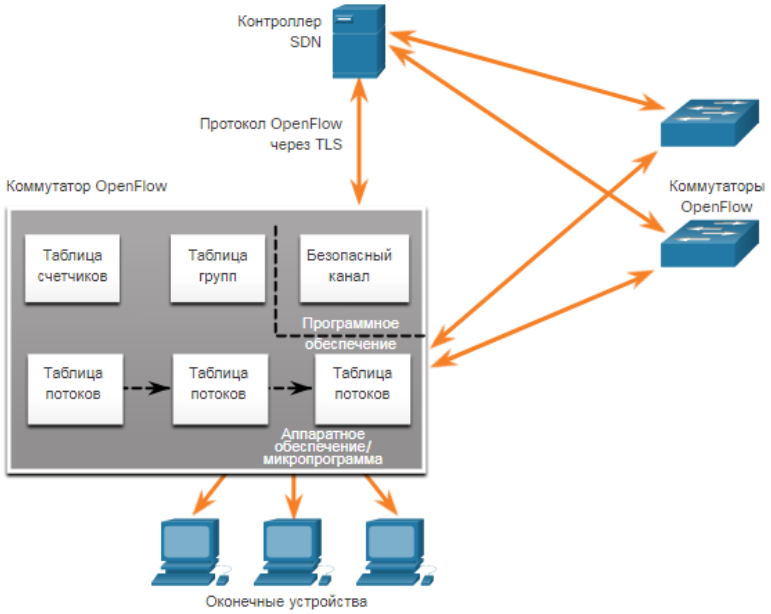


Рисунок 2 – Принцип функционирования сети SDN на базе протокола OpenFlow

Каждый коммутатор должен содержать одну или более таблиц потоков, групповую таблицу и поддерживать канал связи с удаленным контроллером-сервером. Каждая таблица потоков в коммутаторе содержит набор записей о потоках или правилах. Каждая такая запись состоит из полей-признаков, счетчиков и набора инструкций. Управление данными осуществляется не на уровне отдельных пакетов, а на уровне их потоков. Правило в коммутаторе OpenFlow устанавливается с участием контроллера только для первого пакета, а затем все остальные пакеты потока его используют. Имеющиеся на сегодняшний день физические коммутаторы SDN соответствуют спецификации OpenFlow 1.0 и содержат только одну таблицу потоков.

Преимуществами использования SDN являются гибкость и адаптивность управления сетью, возможность независимого развертывания и масштабирования, повышение надежности, упрощение структуры и логики сетевых устройств, а также снижение стоимости сетевой инфраструктуры.

Однако в архитектуре SDN существуют определенные недостатки: проблема надежности и проблема производительности, т.к. эти параметры напрямую зависят от самого контроллера.

Список использованных источников:

1. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 6-ое издание. - СПб.: Питер. 2020. — 1008с.

2. 2. Таненбаум, Э., Уэзеролл Д. Компьютерные сети : учеб. пособие / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер, 2013. – 960 с.

3. CCNA Routing and Switching // Cisco Network Academy [Электронный ресурс]. – 2021. – Режим доступа: https://netacad.com. – 31.03.2021.

Определение метрологических характеристик анализатора систем передачи и кабелей связи AnCom A-7

Кураш О.А., магистрантка гр.967041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белошицкий А.П. – канд. техн. наук, доцент

Аннотация. В докладе рассмотрены результаты экспериментальных исследований метрологических характеристик анализатора систем передачи и кабелей связи AnCom A-7.

Ключевые слова. Анализатор, системы передачи, кабели связи, метрологические характеристики, методика поверки.

Введение

Анализаторы систем передачи и кабелей связи AnCom A-7 (далее - анализаторы) предназначены для формирования одночастотных, двухчастотных, многочастотных, псевдослучайных, шумовых измерительных сигналов и измерений в диапазоне частот от 0,04 до 4096 кГц следующих параметров и характеристик:

– частота и уровень сигнала селективно, широкополосно, взвешенно, включая псофометрическое взвешивание, построение фазограмм и хронограмм уровня;

– затухание и защищенность сигнала от сопровождающих помех;

– паразитные составляющие и нелинейные искажения;

– анализ спектра и регистрация всплесков помех и перерывов;

– измерение частотных характеристик (ЧХ) затухания (АЧХ - рабочего, переходного, несогласованности, асимметрии, защищенности от помех), группового времени прохождения (ГВП), полного сопротивления (импеданса), включая модуль, фазу, активную и реактивную составляющие;

– сопротивление, емкость и тангенс угла диэлектрических потерь, индуктивность и добротность 2-полюсников;

– характеристики 4-полюсников и кабелей методом ХХ-КЗ;

– рефлектометрические измерения, включая измерение расстояния до места неоднородности и задержки распространения;

– измерение задержки между сигналами разной природы на входах.

Анализаторы состоят из генератора нормированных электрических испытательных воздействий измерительных сигналов и измерительного устройства. Внешний вид анализаторов представлен на рисунке 1.

Рисунок 1 - Анализаторы систем передачи и кабелей связи AnCom A-7

Функционирование анализаторов, а также обработка, накопление и представление результатов измерений обеспечивается встроенными вычислительными средствами и внешним универсальным персональным компьютером. Встроенный адаптер подключения позволяет реализовать различные схемы подключения анализатора к измеряемым объектам, выполняемые посредством симметричных трехполюсных розеток или коаксиальных разъемов, расположенных на панели подключения анализатора[1].

Для практического использования анализаторов, как и других средств измерений (далее - СИ) необходимо периодически проверять их метрологические характеристики (далее - МХ). Эти характеристики определяются при периодической поверке или калибровке СИ. Поверка (или

калибровка) проводятся с использованием специально разработанных методик. Для определения МХ анализатора была разработана методика поверки. Результаты экспериментального определения МХ анализатора, полученные при опробовании методики поверки приводятся ниже.

Экспериментальная часть

Поверка анализаторов производится в соответствии с следующим перечнем операций: внешний осмотр, проверка комплектности, маркировки и упаковки; опробование (контроль уровня собственных шумов генератора; измерение затухания и защищенности формируемого гармонического сигнала); определение погрешности установки и измерения частоты; определение погрешности установки и измерения уровня на частоте 100 кГц; определение погрешности измерения ЧХ асимметрии; определение погрешности измерения АЧХ и ГВП; определение погрешности измерения ЧХ импеданса.

Результаты измерений контроля уровня собственных шумов генератора на выходном коаксиальном разъеме и выходном симметричном разъеме представлены в таблице 1.

Таблица 1 – Контроль уровня собственных шумов генератора

Максимальная частота установленного диапазона частот, кГц	ровень собственного шума на выходном коаксиальном разъёме, дБм0	
	Требуемый уровень шума	Измерено при Rген=Rизм=75 Ом
256	<-87	-93,04
1024	<-82	-86,87
4096	<-76	-81,39
Максимальная частота установленного диапазона частот, кГц	Уровень собственного шума на выходном симметричном разъёме, дБм0	
	Требуемый уровень шума	Измерено при Rген=Rизм=150 Ом
4	<-94	-104,37
128	<-86	-91,43
4096	<-73	-77,15
-	Требуемый уровень шума	Измерено при Rген=Rизм=600 Ом
4	<-100	-110,54
128	<-85	-89,86
256	<-82	-86,79

Результаты измерений затухания и защищенности формируемого гармонического сигнала представлены в таблице 2 .

Таблица 2 – Измерение затухания и защищенности формируемого гармонического сигнала

Максимальная частота диапазона частот, кГц	Настройки генератора			Настройки измерителя		Измеряемые величины		
	Опорный уровень, дБмо	SIN-сигнал		Опорный уровень, дБм0	Максимальный измеряемый уровень, дБм	Параметр, дБ	Измеренно, дБ	Допускаемые значения, дБ
		Уровень, дБм0	Частота, кГц					
Rген=Rизм=600 Ом. Подключение: симметрично								
4	4	0	1,02	4	Макс. из трех возможных	Затухание	0,01	± 0,3
						Сигнал/шум	71,13	> 60
Rген=Rизм=150 Ом. Подключение: симметрично								
128	10	-50	10	10	Мин. из трех возможных	Затухание	50,11	50 ±1,5
512	10	-30	100	10	Макс. из трех возможных	Затухание	29,98	30±0,3
2048	0	0	100	0	Сред. из трех возможных	Затухание	0,08	± 0,3
						Сигнал/шум	63,51	> 60
Rген=Rизм=75 Ом. Подключение: коаксиально								
256	7	-50	100	7	Мин. из трех возможных	Затухание	50,18	50 ±1,5

1024	7	-40	100	7	Макс. из трех возможных	Затухание	40,02	40±0,6
4096	0	0	1000	0	Сред. из трех возможных	Затухание	0,05	± 0,3
						Сигнал/шум	59,07	> 56

Для определения погрешности установки и измерения частоты гармонического сигнала поверяемым анализатором, устанавливается уровень гармонического сигнала равный 6 дБм0. К коаксиальному выходу подключается согласованная нагрузка и частотомер. Результаты определения значений погрешности установки и измерения частоты гармонического сигнала представлены в таблице 3.

Таблица 3 – Определение погрешности установки и измерения частоты гармонического сигнала

Частота гармонического сигнала, кГц			Погрешность, кГц		
Номинальная частота, формируемая анализатором, $F_{ген}$	Показания частотомера, $F_{чм}$	Показания анализатора, $F_{изм}$	При формировании частоты, $F_{ген} - F_{чм}$	При измерении частоты, $F_{изм} - F_{чм}$	Допускаемое значение
100,0	99,9999	100,000053	0,00010	0,000053	± 0,00105

Определение погрешностей установки и измерения уровня гармонического сигнала на частоте 100 кГц производится с применением вольтметра В3-63. Результаты проверки представлены в таблице 4.

Таблица 4 – Определение погрешностей установки и измерения уровня на частоте 100 кГц

Максимальная частота установленного диапазона частот, кГц	Уровень, измеренный вольтметром, дБ	Уровень, измеренный вольтметром с учетом коррекции, дБм0, $P_{вм}$	Уровень, измеренный анализатором, дБм0, $P_{изм}$	Погрешность, дБ		
				При установке уровня, $P_{ген} - P_{вм}$	При измерении уровня, $P_{изм} - P_{вм}$	Допускамые значения
Подключение: коаксиально. Rген=Rизм=75 Ом. Коррекция: Рвм[дБм0]=Рвм[дБ]-1,761						
128	1,794	0,033	-0,053	-0,03	-0,09	± 0,2
256	1,804	0,043	-0,009	-0,04	-0,05	± 0,2
512	1,804	0,043	0,012	-0,04	-0,03	± 0,2
1024	1,804	0,020	0,007	-0,02	-0,01	± 0,2
2048	1,804	0,043	0,015	-0,04	-0,03	± 0,2
4096	1,807	0,046	0,019	-0,05	-0,03	± 0,2
Подключение: симметрично. Rген=Rизм=150 Ом. Коррекция: Рвм[дБм0]=Рвм[дБ]-4,771						
128	4,736	-0,035	-0,067	0,04	-0,03	± 0,2
256	4,751	-0,020	-0,058	0,02	-0,04	± 0,2
512	4,751	-0,020	-0,056	0,02	-0,04	± 0,2
1024	4,758	-0,013	-0,043	0,01	-0,03	± 0,2
2048	4,763	-0,008	-0,039	0,01	-0,03	± 0,2
4096	4,760	-0,011	-0,035	0,01	-0,02	± 0,2

Определение погрешности измерения ЧХ затухания асимметрии производится при использовании резистивного делителя Д62/63.19 (62,00 Ом и 63,19 Ом), обеспечивающего воспроизведение затухания асимметрии равное 50,0 дБ и подключаемого к симметричному входу поверяемого анализатора [3]. Результаты проверки определения погрешности измерения частотной характеристики затухания асимметрии приведены в таблице 5.

Таблица 5 – Определение погрешности измерения частотной характеристики затухания асимметрии

Максимальная частота установленного диапазона частот и параметры МЧС	Затухание асимметрии резистивного делителя, дБ	Максимальное по абсолютному значению отклонение частотной характеристики затухания асимметрии от заданной		
		Частота макс. отклонения затухания (по графику), кГц	Затухание асимметрии, дБ	
			Измеренное значение затухания асимметрии с максимальным отклонением	Допуск
128 кГц, F1=7,5 кГц, N=17, DF=7,5 кГц	50	82,5	50,41710	50 ± 5

1024 кГц, F1=60 кГц, N=17, DF=60 кГц	50	420,0	50,31818	50 ± 5
4096 кГц, F1=240 кГц, N=17, DF=240 кГц	50	3840,0	48,71079	50 ± 5

Результаты определения погрешностей измерения поверяемым анализатором частотных характеристик (ЧХ) затухания (АЧХ) и относительного группового времени прохождения (ГВП) приведены в таблице 6.

Таблица 6 – Определение погрешностей измерения частотных характеристик затухания и времени прохождения

Максимальная частота установленного диапазона частот и параметры МЧС	Проверяемый параметр	Максимальное по абсолютному значению отклонение частотной характеристики поверяемого параметра (затухания или времени прохождения) от заданной		
		Частота макс. отклонения (по графику), кГц	Значение поверяемого параметра	
			Измеренное значение с максимальным отклонением от заданного	Допускаемое значение
Подключение: коаксиально. Rген=Rизм=75 Ом				
128 кГц, F1=30 кГц, N=79, DF=1,25 кГц	АЧХ, дБ	33,75	0,25696	± 0,3
	ГВП, мкс	30,00	1,16878	± 10
1024 кГц, F1=30 кГц, N=100, DF=10 кГц	АЧХ, дБ	30,00	0,19142	± 0,3
	ГВП, мкс	30,00	0,88545	± 1,2
4096 кГц, F1=60 кГц, N=68, DF=60 кГц	АЧХ, дБ	4080,0	0,21583	± 0,3
	ГВП, мкс	30,00	0,16307	± 0,3
Подключение: симметрично. Rген=Rизм=150 Ом				
128 кГц, F1=0,625 кГц, N=204, DF=0,625 кГц	АЧХ, дБ	97,5000	0,13134	± 0,3
	ГВП, мкс	44,3750	0,57448	± 10
1024 кГц, F1=5 кГц, N=204, DF=5 кГц	АЧХ, дБ	675,00	0,05898	± 0,3
	ГВП, мкс	560,00	0,10171	± 1,2
4096 кГц, F1=20 кГц, N=204, DF=20 кГц	АЧХ, дБ	2200,00	0,07251	± 0,3
	ГВП, мкс	4020,00	0,04814	± 0,3

Погрешность измерения ЧХ импеданса приведены в таблице 7.

Таблица 7 – Определение погрешности измерения частотной характеристики импеданса

Максимальная частота установленного диапазона частот и параметры МЧС	Сопротивление генератора, Ом	Максимальное по абсолютному значению отклонение частотной характеристики импеданса от заданного образцового значения			
		Величина сопротивления нагрузочного резистора, Ом	Частота макс. отклонения импеданса (по графику), кГц	Затухание асимметрии, дБ	
				Измеренное значение импеданса с максимальным отклонением от заданного	Допускаемое значение
128 кГц, F1=7,5 кГц, N=17, DF=7,5 кГц	600	600	3,75	586,63	600 ± 18
1024 кГц, F1=60 кГц, N=17, DF=60 кГц	150	150	1560	146,69	150 ± 4,5
	135	150	1800	146,55	150 ± 4,5
	120	150	1560	146,60	150 ± 4,5
4096 кГц, F1=240 кГц, N=17, DF=240 кГц	100	150	3840	142,35	150 ± 9

Выводы

Приведенные выше результаты экспериментальных исследований МХ анализатора AnCom A-7 показывают, что прибор соответствует техническим характеристикам, заявленным производителем и может применяться для контроля параметров в сетях и системах инфокоммуникаций.

Список использованных источников:

1. Кабельный xDSL анализатор AnCom A-7 [Электронный ресурс]. URL: http://www.analytic.ru/products/8/soft

2. Хамадулин, Э. Ф. Методы и средства измерений в телекоммуникационных системах : учебное пособие для академического бакалавриата / Э. Ф. Хамадулин. — Москва : Издательство Юрайт, 2019. — 365 с.

3. AnCom A-7 руководство по эксплуатации [Электронный ресурс]. https://skomplekt.com/mag/1/files/A7_rukov_part1.pdf

УДК 004.738.2

ТЕХНОЛОГИИ VPN ДЛЯ КОРПОРАТИВНЫХ СЕТЕЙ

Кучинский П.С., студент гр.763102

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Давыдова Н.С. – канд. тех. наук., доцент

Аннотация. В работе представлен анализ возможных реализаций сети предприятия на базе технологий VPN.

Ключевые слова. Виртуальная частная сеть, VPN, VPN-шлюз, VPN-клиент, VPN-сервер, Site-to-Site VPN, Remote Access VPN.

VPN (Virtual Private Network) – это логическая сеть на базе виртуальных туннелей, создаваемая поверх другой коммуникационной сети. При этом, даже если коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, то за счёт шифрования создаются закрытые от посторонних каналы обмена информации и обеспечивается конфиденциальность и целостность данных. Доступ к такому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. VPN позволяет объединить, например, несколько офисов организации в единую сеть с безопасной передачей информации через Интернет [1].

Для создания виртуальной частной сети крупного предприятия нужны VPN-шлюзы, VPN-серверы и VPN-клиенты. VPN-шлюзы целесообразно использовать для защиты локальных сетей предприятия, VPN-серверы и VPN-клиенты используют для организации защищенных соединений удаленных и мобильных пользователей с корпоративной сетью через Интернет.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое программное обеспечение модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, выполняющий функции сервера. VPN-сервер обеспечивает защиту серверов от несанкционированного доступа из внешних сетей, а также организацию защищенных соединений с отдельными компьютерами и с компьютерами из сегментов локальных сетей, защищенных соответствующими VPN-продуктами.

Шлюз безопасности VPN – это сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Шлюз безопасности VPN должен быть размещен так, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети.

Классифицировать VPN решения можно по нескольким основным параметрам [2]:

– по типу используемой среды:

1 Защищённые VPN сети. Наиболее распространённый вариант приватных частных сетей. С его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

2 Доверительные VPN сети. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решении являются: MPLS и L2TP. Эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, который как правило, используется в паре с IPSec.

– по способу реализации:

1 VPN сети в виде специального программно-аппаратного обеспечения. Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

2 VPN сети в виде программного решения. Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

3 VPN сети с интегрированным решением. Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

– по назначению: Site-to-Site VPN, Remote Access VPN

Соединение «точка-точка» (Site-to-Site) применяется для подключения всей локальной сети в одной локации к локальной сети в другой. Стандартный сценарий – подключение удаленных филиалов к центральному офису или дата-центру компании. При этом не требуется установка VPN-клиентов на устройства пользователей, так как соединение обрабатывает VPN-шлюз, и передача данных между устройствами в разных сетях происходит прозрачно. При использовании VPN типа Site-to-Site шлюз VPN одной удаленной локальной сети взаимодействует со шлюзом другой локальной сети для создания безопасного туннеля. Удаленным устройствам не нужен VPN-клиент, они отправляют обычный трафик через шлюзы VPN. Схема VPN-соединения Site-to-Site представлена на рисунке 1.

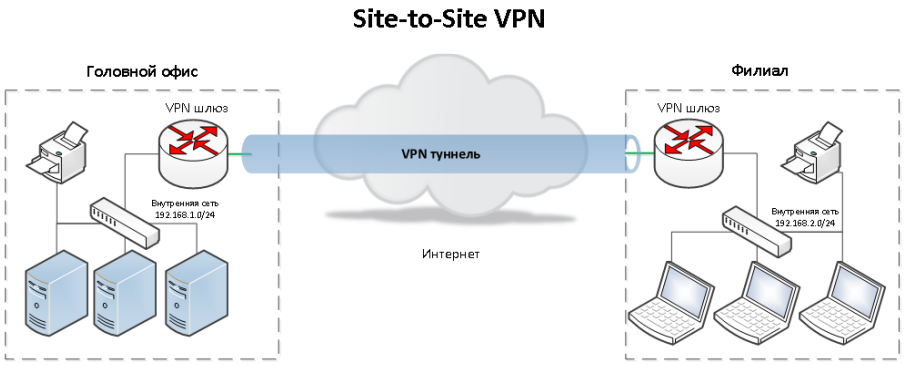


Рисунок 1 – Схема VPN-соединения Site-to-Site

VPN удаленного доступа (Remote access VPN) используется для предоставления сотрудникам компании безопасного доступа к корпоративной сети и ее ресурсам через публичную сеть Интернет. Это особенно актуально, когда для подключения к Интернету используется общественная точка доступа Wi-Fi или другие небезопасные способы подключения. Для Remote access VPN также необходимо, чтобы на устройстве было установлено клиентское программное обеспечение. Это программное обеспечение VPN-клиента взаимодействует со шлюзом VPN, на котором производится аутентификация и авторизация пользователя и создает защищенный «виртуальный» туннель между локальной сетью и шлюзом. После успешного прохождения этой процедуры пользователь получает доступ к внутренним сетевым ресурсам (файловый сервер, базы данных, принтеры и другие) так, будто он подключен к локальной сети. Схема VPN-соединения Remote access представлена на рисунке 2.

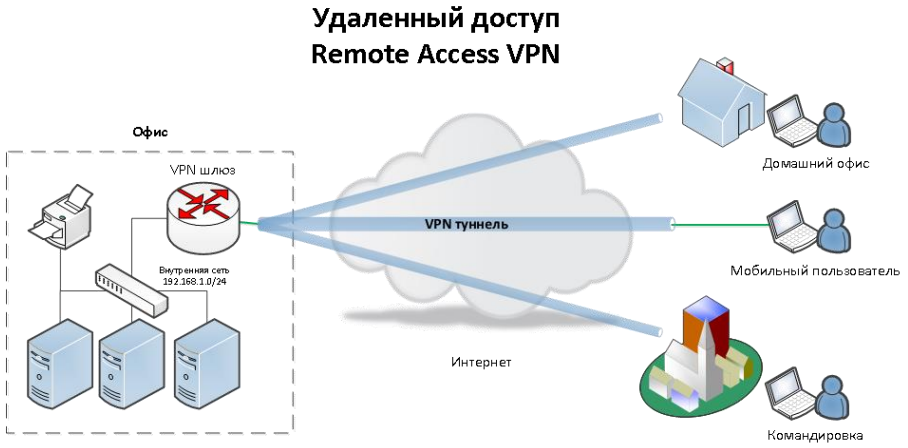


Рисунок 2 – Схема VPN-соединения Remote access

Стоит так же учитывать, что VPN можно различать по средствам реализации:

– VPN на базе сетевой ОС;

– VPN на базе программного обеспечения;

– VPN на базе маршрутизаторов;

– VPN на базе брандмауэров;

- VPN на базе аппаратных средств.

К средствам VPN, выполненным в виде автономного ПО относятся и VPN-шлюзы, и VPN-клиенты. Многие компании-производители аппаратных шлюзов дополняют линейку своих продуктов чисто программной реализацией VPN-клиента, который рассчитан на работу в среде стандартной ОС. Что касается программных шлюзов (иногда они называются также «сервера защищенных каналов»), то производители как правило нагружают их некоторыми

дополнительными функциями по защите данных, например: функциями по фильтрации траффика и контролю доступа, свойственными брандмауэру. Поэтому граница между брандмауэрами со встроенными функциями VPN и программными VPN-шлюзами очень размыта. Например, таким продуктом является RRAS (Routing and Remote Access Service). RRAS включает в себя усовершенствованный программный многопротокольный маршрутизатор, который поддерживает протоколы маршрутизации RIP и OSPF из TCP/IP. RRAS может быть использован как VPN-шлюз при взаимодействии «сеть-сеть» [3].

VPN на базе сетевой ОС. Примером являются системы Windows. Для создания VPN используется протокол PPTP, который интегрирован в систему Windows [4]. Данное решение очень привлекательно для организаций, использующих Windows в качестве корпоративной операционной системы. Необходимо отметить, что стоимость такого решения значительно ниже стоимости прочих решений. В работе VPN на базе Windows используется база пользователей NT, хранящаяся на Primary Domain Controller (главный контроллер домена) (PDC). При подключении к PPTP-серверу пользователь аутентифицируется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40 или 128 битным ключом, получаемым в момент установки соединения. Недостатками данной системы являются отсутствие проверки целостности данных и невозможность смены ключей во время соединения. Положительными моментами являются легкость интеграции с Windows и низкая стоимость.

VPN на базе маршрутизаторов применяется для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящая из локальной сети, проходит через маршрутизатор, то на маршрутизатор можно возложить и задачи шифрования. Примером оборудования для построения VPN на маршрутизаторах является оборудование компании «Cisco». Начиная с версии программного обеспечения IOS 11.3, маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования проходящей информации Cisco поддерживает и другие функции VPN, такие как идентификация при установлении туннельного соединения и обмен ключами.

VPN на базе брандмауэров. Брандмауэры большинства производителей поддерживают туннелирование и шифрование данных. К программному обеспечению брандмауэра добавляется модуль шифрования. Недостатком этого метода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает брандмауэр. При использовании брандмауэров на базе ПК надо помнить, что подобное решение можно применять только для небольших сетей с небольшим объемом передаваемой информации.

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Выделенные аппаратные шлюзы реализованы в виде отдельного аппаратного устройства, основная функция которого – высокопроизводительное шифрование траффика. VPN-устройства являются фактическими лидерами практически по всем показателям, кроме одного – стоимости. Аппаратные шлюзы высшего класса обязательно поддерживают IPsec, причем со многими расширениями в виде новых и мощных в криптографическом отношении алгоритмов. Обладают высокой производительностью за счет аппаратной поддержки операций шифрования. По удобству и простоте инсталляции, аппаратные шлюзы обычно намного превосходят программные шлюзы и такие комбинированные решения, как шлюзы на основе брандмауэров и маршрутизаторов. Аппаратное устройство уже при включении готово работать, ему не надо проходить громоздкий процесс инсталляции в среде какой-либо ОС, как это требуется для большинства программных или комбинированных продуктов, а для работы необходимо только задать значения конкретных адресов и, может быть, ключей для установления тоннелей.

Описанная выше классификация позволяет реализовывать VPN сети различными способами, каждый из которых имеет свои преимущества и недостатки в зависимости от требований к сети. При выборе решения требуется учитывать факторы производительности средств построения VPN. Для построения VPN лучше всего использовать специализированное оборудование, однако если имеется ограничение в средствах, то можно обратить внимание на чисто программное решение [5].

Таким образом, основными достоинствами использования VPN-технологий для защиты информации в распределенных корпоративных сетях являются:

1 Возможность защиты всей корпоративной сети.

2 Масштабируемость системы защиты.

3 Использование ресурсов открытых сетей в качестве отдельных коммуникационных звеньев корпоративной сети; все угрозы, возникающие при использовании сетей общего пользования, будут компенсироваться средствами защиты информации.

4 Обеспечение подконтрольности работы сети и достоверная идентификация всех источников информации.

5 Сегментация информационных систем и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.

Список использованных источников:

1. Scott C., Wolfe P., Erwin M. Virtual private networks. – O'Reilly Media Inc., 1999. P. – 225.

2. Николахин А. Ю., Использование технологии vpn для обеспечения информационной безопасности //Экономика и качество систем связи. – 2018. – №. 3.

3. Казиева Г. С., Мухамеджанова А. Д. НЕКОТОРЫЕ АСПЕКТЫ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ VPN //Научно-Технического Общества «КАХАК». – 1998. – С. 88.

4. VPN на базе аппаратных средств [Электронный ресурс]. – Режим доступа: https://helpiks.org/4-69912.html.

5. Березин А., Петренко С. Построение корпоративных защищенных виртуальных частных сетей //Сетевой журнал. – 2001. – №. 1.

УДОСТОВЕРЯЮЩИЙ ЦЕНТР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СЕТИ ПРЕДПРИЯТИЯ

Лодис А.В., магистрант гр. 067041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саломатин С.Б. – кандидат технических наук, доцент

Распространение и внедрение информационных технологий привело к тому, что применение электронных документов вместо печатных является наиболее удобным способом документооборота, поэтому для организации его на предприятии необходимо создание защищенной сети передачи данных, а также регистрационного центра предприятия для создания и выдачи электронной цифровой подписи сотрудникам.

Целью работы является создание облика защищенной сети передачи данных и регистрационного центра предприятия, повышение защиты сети передачи данных, тем самым обеспечение информационной безопасности при издании, распространении и хранении сертификатов открытых ключей проверки электронной цифровой подписи, присоединение к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

При внедрении систем электронного документооборота на предприятии необходимо организовать и четко отладить функционирование сети передачи данных с обязательным применением основных требований по информационной безопасности, а именно обеспечить конфиденциальность, целостность и доступность информации.

Как правило у самого предприятия нет собственных ресурсов сети связи и необходимые канальные ресурсы арендуются из сети связи общего пользования у региональных и национальных операторов связи.

Используемые структурно-технологические решения по сопряжению транспортных сетей из состава собственных сетей связи с сетями в составе сетей связи общего пользования операторов связи обеспечивают связность на сетевом уровне, за счет использования единых протокольных решений на основе протоколов IPv4 и IPv6. В целях обеспечения безопасности при сопряжении собственных сетей связи с сетями связи общего пользования должны быть использованы решения, обеспечивающие изоляцию адресных пространств отдельных сетей в составе собственных сетей связи и передаваемых потоков трафика от тех сегментов и потоков, которые обслуживаются в сетях связи общего пользования оператором связи.

С учетом развития угроз безопасности информации, а также способов реализации данных угроз за последнее время базовые принципы построения информационной сети претерпели существенные изменения. На рисунке 1 представлена схема взаимодействия в ведомственной информационной сети удаленных постов регистрации в региональных подразделениях с регистрационным центром в центральном узле предприятия и Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь в Национальном центре электронных услуг с применением средств межсетевого экранирования и программно-аппаратных комплексов шифрования передаваемого трафика (информации).

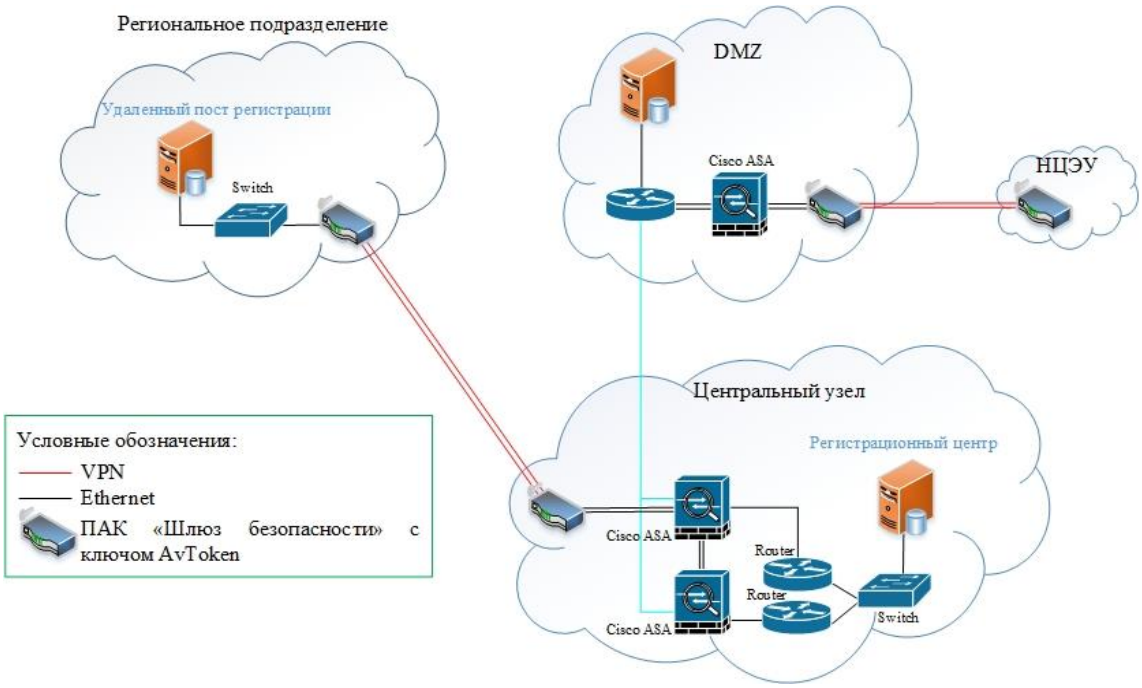


Рисунок 1. Схема сети передачи данных регистрационного центра предприятия

Для объединения локальных сетей удаленных узлов применяют технологию виртуальных частных сетей – VPN (Virtual Private Network). Данная технология предназначена для криптографической защиты данных, передаваемых по компьютерным сетям. Виртуальная частная сеть представляет собой совокупность сетевых соединений между несколькими VPN-шлюзами, на которых производится шифрование сетевого трафика.

В систему информационной сети предприятия входят программные, технические и программно-технические средства, обеспечивающие взаимодействие регистрационных центров как внутри предприятия, так и межведомственного обмена информацией.

Достоинства использования технологий виртуальных частных сетей для защиты информации в распределенных информационных сетях предприятий:

1. Сегментация информационной сети и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.
2. Использование ресурсов открытых сетей в качестве отдельных коммуникационных звеньев сети.
3. Обеспечение подконтрольности работы информационной сети и достоверная идентификация всех источников информации. При необходимости может быть обеспечена аутентификация трафика на уровне отдельных пользователей.
4. Возможность защиты всей информационной сети от крупных локальных сетей офисов до отдельных рабочих мест.
5. Масштабируемость системы защиты.

Основное предназначение регистрационного центра предприятия — это решение задач по обеспечению должностных лиц, сотрудников предприятия средствами электронной цифровой подписи Республиканского удостоверяющего центра национального центра электронных услуг.

Регистрационный центр предприятия является элементом Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг и осуществляет взаимодействие между Республиканским удостоверяющим центром и потребителями (сотрудниками предприятия, являющимися владельцами личных ключей, использующихся при выработке электронной цифровой подписи и получившими полномочия ее применять).

Основными функциями регистрационного центра предприятия являются:

проверка полноты и достоверности информации, представляемой заявителями в Республиканский удостоверяющий центр;

регистрация потребителей;

изготовление ключей электронной цифровой подписи;

запись на носители ключевой информации личных ключей;

формирование запросов в Республиканский удостоверяющий центр на выпуск сертификатов открытого ключа;

изготовление карточек открытых ключей;

изготовление учетных карточек;

формирование запросов в Республиканский удостоверяющий центр на прекращение действия (отзыв), приостановление действия сертификатов открытого ключа;

формирование запросов в Республиканский удостоверяющий центр на возобновление действия сертификатов открытого ключа;

изготовление, учет, накопление и хранение первого экземпляра карточек открытых ключей, одного экземпляра учетных карточек;

протоколирование работы регистрационного центра предприятия;

консультация потребителей по вопросам применения средств электронной цифровой подписи и др.

Таким образом с учетом функций, выполняемых регистрационным центром предприятия выдвигаемые требования по обеспечение требуемой высокой степени защиты сети передачи данных предприятия и использования оборудования межсетевого экранирования, шифрования передаваемого трафика, технологии виртуальных частных сетей являются обоснованными и необходимым условием для применения. Дальнейшая работа по исследованию данной темы будет направлена на поиск уязвимостей VPN сетей передачи данных и программно-аппаратных средств защиты сети, повышения защиты функционирования регистрационного центра предприятия.

Список использованных источников:

1. Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи» от 28.12.2009 г. № 113-З.

2. Макаренко С. И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. URL: http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf;

3. Документация о программном комплексе «Шлюз безопасности виртуальный Bel VPN Gate» [Электронный ресурс]. – Режим доступа: http://s-terra.by/products/bel-vpn-gate-v.19.

АВТОМАТИЗАЦИЯ РАЗВЕРТЫВАНИЯ СЕРВИСОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ОРКЕСТРАТОРА NOMAD

Матлаш Т.С., студентка группы 763102

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саломатин С. Б.− к. т. н., доцент

В современных практиках разработки программного обеспечения используется множество инструментов для компилирования, тестирования и резвертывания кода [2]. Прежде чем продукт попадает к конечному пользователю, он должен пройти множество проверок на дефекты в различных средах. Этот факт приводит к сложной конфигурации систем, в которых производится тестирование продукта, увеличению временных и денежных затрат на их поддержку, а также могут возникать ошибки и конфликты из-за различных настроек систем той или иной среды. Для автоматизации этих процессов используются оркестраторы. Оркестратор позволяет автоматизировать создание, мониторинг и развертывание ресурсов в среде разработки.

Ранее повсеместно для развертывания использовались виртуальные машины. Технически было организовано так, что весь код приложений собирался за счет средств автоматической сборки [2]. При помощи конфигурационного менеджера код из системы контроля версий доставлялся на виртуальные сервера. Но в этом способе есть несколько недостатков:

- для каждого сервиса необходимо поддерживать актуальную для него версию виртуальной машины (обновление библиотек и зависимостей);
- для каждого нового сервиса необходимо создавать отдельную новую виртуальную машину, которую также нужно обслуживать.

Nomad - это простой в использовании, гибкий и производительный оркестратор, который позволяет управлять контейнерами, в которых находятся сервисы. Nomad позволяет разработчикам использовать декларативную инфраструктуру как код для развертывания сервисов. Для развертывания сервиса необходим конфигурационный файл. В качестве формата конфигурационного файла используется язык HCL, что расшифровывается как HashiCorp Configuration Language (см. рисунок 1).

```
job "service-job" {
        region = "global"
        type = "service"
        group "service-group" {
                task "service-task" {
                        driver = "docker"

                        config {
                                image = "myimage:1.2.3"
                        }

                        service {
                                name = "my-service"
                                tags = [ "1.2.3" ]
                        }
```

Рисунок 1 – Пример конфигурационного файла

Все конфигурационные файлы хранятся в одном репозитории. Таким образом, конфигурации становятся обозреваемы: их легко поддерживать и можно увидеть, какие сервисы есть в данный момент. В случае необходимости несложно обновить или поменять конфигурации сервиса. Для добавления новой системы необходимо создать конфигурационный файл внутри новой директории (см. рисунок 2).

Рисунок 2 – Структура репозитория конфигурационных файлов

Nomad предоставляет удобный графический интерфейс. На рисунке 3 можно увидеть список развернутых сервисов, а также их состояние, что решает задачу мониторинга сервисов.

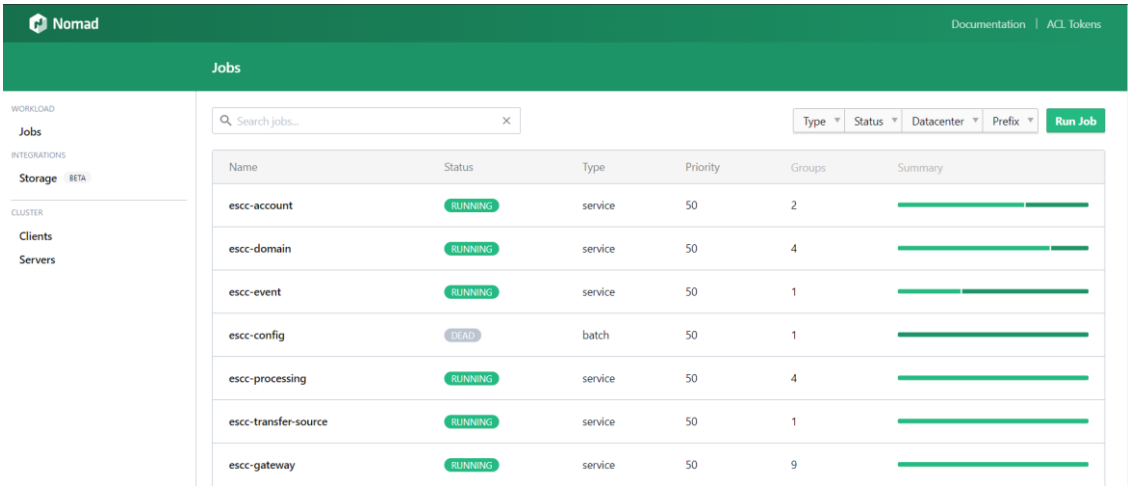


Рисунок 3 – Графический интерфейс оркестратора Nomad

Применение оркестратора Nomad позволяет решить задачу конфигурирования и поддержания систем для развертывания сервисов. Также его использование значительно ускоряет разработку программного обеспечения за счет использования декларативной инфраструктуры.

Список использованных источников:

1. Непрерывная интеграция программного обеспечения [Электронный ресурс]. - https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B5%D1%80%D1%8B%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D1%82%D0%B5%D0%B3%D1%80%D0%B0%D1%86%D0%B8%D1%8F
2. Деплой приложений [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/lamoda/blog/451644/

МОДЕЛИРОВАНИЕ ЗАЩИЩЕННОЙ МАРШРУТИЗАЦИИ МЕЖДУ VLAN

Михнюк Д.Г., Ковятинец И.П., магистранты гр.967041
Мамуду Сиссе, магистрант гр.067001

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Астровский И.И. - канд. техн. наук, доцент

Аннотация. В этой статье приведено решение для обучения персонала и студентов в сфере инфокоммуникационных технологий. Предлагается модель маршрутизации между VLAN с коммутатором уровня 3, которая может быть использована при проектировании сети VLAN.

Ключевые слова: проектирование модели, маршрутизация между VLAN, обучение.

Введение

Компьютерная сеть - это система, которая делает информацию доступной для многих людей и между несколькими машинами. Таким образом, сеть может соединять с помощью соответствующего коммуникационного оборудования компьютеры, терминалы и различные периферийные устройства, такие как принтеры и файловые серверы.

Соединение между этими различными элементами может быть выполнено с использованием постоянных соединений, таких как кабели, а также с использованием общедоступных телекоммуникационных сетей, таких как телефонная сеть. Фактически, размеры этих компьютерных сетей очень разнообразны, самые распространенные сети: глобальные (WAN), городские (MAN), локальные (LAN) и персональные (PAN) сети. Но особую роль в этом играют VLAN.

VLAN (виртуальная локальная сеть) - это локальная сеть, объединяющая набор машин логическим, а не физическим образом.

VLAN логически сегментируют коммутируемые сети на основе бизнес-функций, команд, проектов или приложений, независимо от их физического местоположения или сетевых подключений. Все рабочие станции и серверы, используемые рабочей группой, используют одну и ту же VLAN, независимо от местоположения или физического соединения. Всякий раз, когда узлам в одной VLAN необходимо взаимодействовать с узлами в другой VLAN, трафик должен маршрутизироваться между ними. Это называется «маршрутизацией между VLAN». Для связи между различными VLAN требуется маршрутизатор или какой-либо вид маршрутизации. Маршрутизация между виртуальными локальными сетями может выполняться с использованием коммутатора уровня 3 или более распространенной формы маршрутизации между виртуальными локальными сетями.

Изучение, внедрение сетевых технологий и настройка сетей VLAN с использованием только реальных устройств оказываются невозможными из-за высокой стоимости. Cisco разработала и поддерживает Cisco Packet Tracer, сложный симулятор, позволяющий моделировать и оценивать компьютерную сеть, используя модели устройств Cisco в качестве коммуникационного оборудования, например GNS3, VIRL ...

Цель работы: показать модель маршрутизации между Vlan с коммутатором уровня 3, которая может быть использована для разработки программ обучения персонала и студентов в области инфокоммуникационных технологий,.

Решения для обучения персонала и студентов в области инфокоммуникационных технологий с помощью Cisco.

Многолетним лидером в области сетевых технологий является Cisco Systems, одна из крупнейших мировых компаний, специализирующаяся на разработке и продаже сетевого оборудования. Именно ее продукты активно используются при построении локальных и глобальных компьютерных сетей, поэтому будущим сетевым инженерам стоит начинать обучение работе с оборудованием Cisco. Большой проблемой в данном случае является невозможность изучения сетевых технологий на примере реальных устройств из-за их дороговизны. Чтобы решить эту проблему, Cisco разработала и поддерживает Cisco Packet Tracer, сложный симулятор, который позволяет моделировать и оценивать компьютерную сеть, используя устройства Cisco в качестве коммуникационного оборудования.

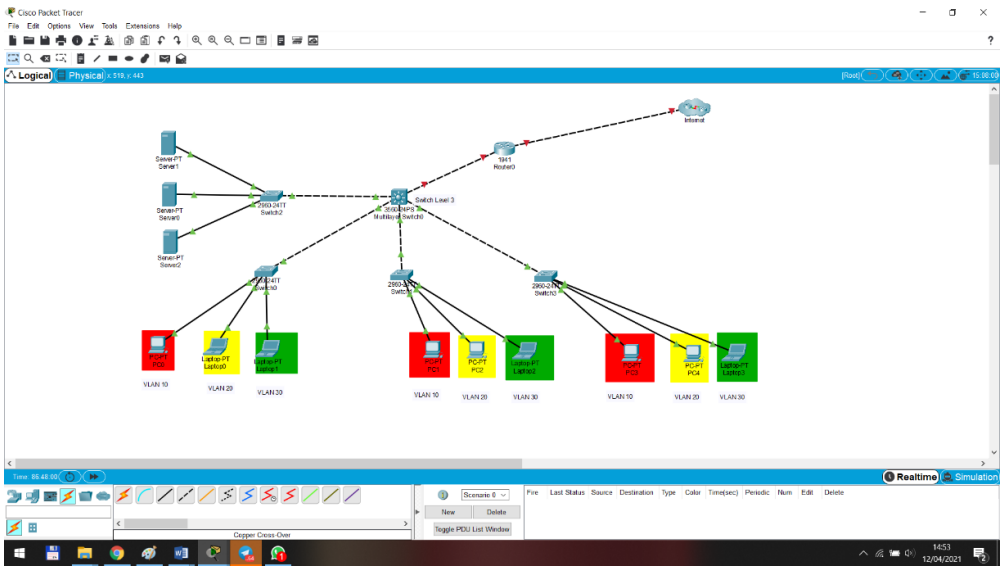
Cisco (или Cisco Systems) - американская фирма, изначально специализирующаяся на сетевом оборудовании, а в последнее время позиционирующаяся на стороне серверов. Его

продукты охватывают множество технологий: маршрутизатор, коммутатор, видеоконференцсвязь, беспроводную передачу, передачу голоса по IP.

Сетевая академия Cisco меняет жизнь студентов, преподавателей и целых сообществ с помощью технологий, образования и возможностей карьерного роста. Доступно для всех, где бы вы ни находились.

1. Packet Tracer - это программное обеспечение от CISCO, позволяющее создавать виртуальную физическую сеть и моделировать поведение сетевых протоколов в этой сети. Пользователь строит свою сеть, используя такое оборудование, как маршрутизаторы, коммутаторы или компьютеры. Затем это оборудование должно быть подключено через соединения (различные кабели, оптоволокно). После подключения всех устройств для каждого из них можно настроить IP-адреса, доступные службы и т. д.
2. GNS3 - отличный дополнительный инструмент для реальной лаборатории, предназначенной для обучения сетевых профессионалов, администраторов и студентов. Его также можно использовать для изучения функциональности Cisco IOS, Juniper JUNOS и для моделирования конфигураций, которые должны быть развернуты позже на реальных маршрутизаторах.
3. Cisco Virtual Internet Routing Lab (VIRL) - это программный инструмент, разработанный Cisco для создания и запуска сетевых симуляций без использования физического оборудования. Под аббревиатурой VIRL - понимают платформу на основе OpenStack, которая запускает образы программного обеспечения IOSv, IOSvL2, IOS XRv, NX-OSv, CSR1000v и ASAv на интегрированном гипервизоре. VIRL обеспечивает масштабируемую и расширяемую среду проектирования и моделирования сети с использованием интерфейса VM Maestro.

Модель маршрутизации между VLAN с коммутатором уровня 3.



Используя эту модель, можно установить связь между виртуальными локальными сетями с помощью переключателя уровня 3 и разрабатывать специальные обучающие и тестирующие программы.

Заключение

Показана модель, которая может быть взята за основу при разработке программ обучения персонала и настройки сетей VLAN. Эта модель может использоваться для маршрутизации между VLAN с оборудованием Cisco в области инфокоммуникаций.

БЕСПРОВОДНЫЕ СЕТИ ZIGBEE

Мялик А. И., студентка группы 763101

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Давыдова Н. С. − к.т.н., доцент

Беспроводные сети являются элементами информационных технологий, которые предназначены для передачи данных между приемником и отправителем на большие или малые расстояния без использования проводов. Беспроводные сети обеспечивают мобильность портативных и ручных компьютерных устройств. В настоящее время беспроводные технологии стали более надежными и в некоторых ситуациях их развертывание обходится дешевле, чем создание кабельных сетей. Примерами беспроводных технологий являются: Wi-Fi, Bluetooth, Thread, ZigBee.

ZigBee – это открытый стандарт беспроводной связи для систем сбора данных и управления. Технология ZigBee позволяет создавать самоорганизующиеся и самовосстанавливающиеся беспроводные сети с автоматической ретрансляцией сообщений, с поддержкой батарейных и мобильных узлов.

Технология ZigBee продвигается организацией ZigBee Alliance, ставящей своей целью обеспечение верхних слоев семиуровневой модели стеком протоколов (от сетевого уровня до уровня приложений), включая профили приложений и инженерную реализацию компонентов данной технологии. К разработке соответствующего стандарта низкоскоростной передачи данных подключился комитет IEEE 802.15.4 [1]. На рисунках 1 и 2 изображено распределение «зон ответственности» разработчиков и потребителей технологии, а также позиционирование в ряду беспроводной передачи данных:

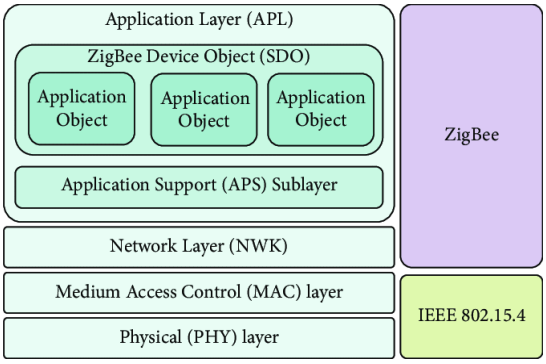


Рис. 1 – ZigBee protocol stack

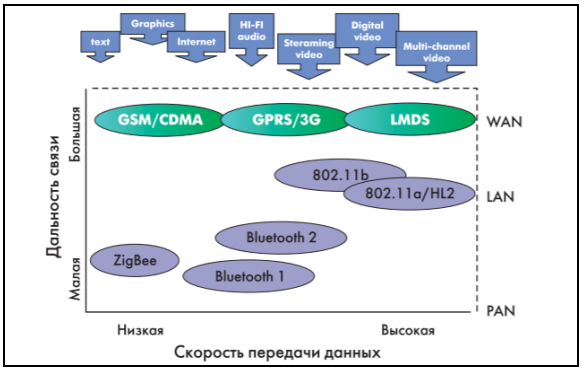


Рис. 2 – Позиционирование в ряду беспроводной передачи данных

Спецификация ZigBee регламентирует стек протоколов взаимодействия узлов сети, в котором протоколы верхних уровней используют сервисы, предоставляемые протоколами нижележащих уровней.

В качестве двух нижних уровней (физического и уровня доступа к среде MAC) используется стандарт IEEE 802.15.4. MAC-уровень в сети ZigBee реализует механизм CSMA/CA (прослушивания несущей и устранения коллизий), сетевой уровень NWK отвечает за маршрутизацию сообщений, а уровень поддержки приложений APS обеспечивает интерфейс с уровнем приложения.

Сектор ZDO (ZigBee Device Object), связывающий три верхних уровня, отвечает за определение роли устройства в сети (будет оно являться координатором или конечным устройством), инициализацию и реакцию на запросы соединения и обнаружения, за установление надежного и безопасного соединения между устройствами сети [3].

Стандарт ZigBee ориентирован, главным образом, на использование в качестве средства связи между автономными приборами и оборудованием управления.

Предъявляемые к технологии ZigBee требования, которые были реализованы ZigBee Alliance: поддержка сетей с несколькими сотнями функционирующих устройств (до 255 подключенных устройств); обеспечение в реальных домашних условиях среднего радиуса действия сетей порядка 30 метров; простота инсталляции и применения [2].

В основе сети ZigBee могут лежать топологии кластерное дерево, топология звезда и ячеистая топология (рисунок 3). Самой эффективной является ячеистая топология (mesh-топология). В такой сети, каждое устройство может связываться с любым другим устройством как напрямую, так и через промежуточные узлы сети. Ячеистая топология предлагает альтернативные варианты выбора маршрута между узлами. Сообщения поступают от узла к узлу, пока не достигнут конечного получателя. Возможны различные пути прохождения сообщений, что повышает доступность сети в случае выхода из строя того или иного звена.

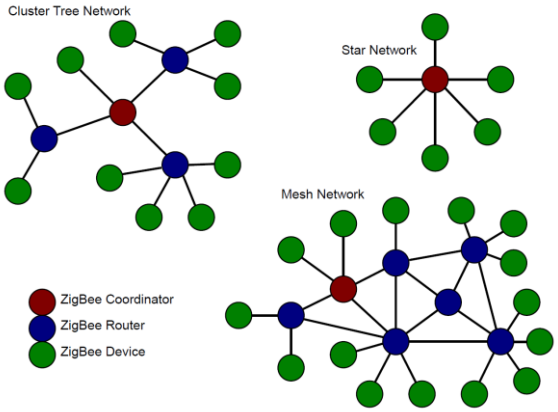


Рис. 3 – Виды топологий

В соответствии с технологией Zigbee сети беспроводной передачи включают в свой состав устройства двух классов – полнофункциональные (Full function device – FFD) и устройства с ограниченной функциональностью (Reduced function device – RFD). Устройства первого типа обеспечивают расширенные возможности по построению топологии сети, могут выполнять роль координатора работы сети (главной станции радиосети) и могут обмениваться сообщениями с любой другой станцией сети. Устройства второго типа могут работать только в сети звездообразной формы, не могут выполнять функции координации работы сети обмена данными и имеют упрощенную конструкцию.

Кроме деления устройств на RFD и FFD, альянсом ZigBee определены три типа логических устройств: ZigBee-координатор (согласующее устройство), ZigBee-маршрутизатор и оконечное устройство ZigBee. Координатор осуществляет инициализацию сети, управление узлами, а также хранит информацию о настройках каждого узла, подсоединенного к сети. ZigBee-маршрутизатор отвечает за маршрутизацию сообщений, передаваемых по сети от одного узла к другому. Под оконечным устройством понимают любое оконечное устройство, подсоединенное к сети. Устройства RFD и FFD так же являются оконечными устройствами.

Одна из основных идей разработки стандарта ZigBee состояла в том, чтобы обеспечить возможность совместной работы в одной беспроводной сети устройств различных производителей. Очевидно, что для обеспечения совместимости на уровне приложения устройствам ZigBee требуется некий стандартный язык общения. Для реализации этой задачи была разработана библиотека ZigBee-кластеров ZCL (ZigBee Cluster Library) [3]. Кластер похож на класс в объектно-ориентированном программировании и представляет собой слудующую совокупность: описание стандартного устройства ZigBee (например, осветительное устройство, диммер, выключатель, счетчик); описание стандартных атрибутов для этого устройства (например, вкл./выкл., яркость, показания счетчика); описание стандартных команд для этого устройства (например, установить уровень яркости, считать показания, включить/выключить). При этом, кластеры имеют клиент-серверную природу, т.е. ZigBee-сервер - это устройство, которое хранит значение атрибута, в то время, как ZigBee-клиент дистанционно считывает или записывает значение этого атрибута.

Таким образом, технология ZigBee разрабатывалась для создания надёжных сетей датчиков и управляющих устройств с невысокими скоростями передачи данных. В данной технологии реализована поддержка спящих и мобильных узлов, а также узлов, которые обеспечивают работу алгоритмов ретрансляции и самовосстановления. Технология ZigBee подойдёт для построения беспроводной малопотребляющей системы, которая будет охватывать несколько комнат или даже зданий, так как данная технология поддерживает ячеистую топологию, которой свойственна избыточность связей между соседними узлами, что даёт преимущество в случае возникновения помехи, так как будет найден альтернативный маршрут. Данная особенность делает сеть надёжнее. Сетевой стек протоколов позволяет устройствам работать в одной сети и обмениваться между собой сообщениями, а стандартные профили позволяют беспроводным узлам разных производителей понимать друг друга на прикладном уровне.

Список использованных источников:

1. Gislason D. Zigbee wireless networking. – Newnes, 2008.
2. Зуб М. А., Красичков А. А. Методика построения динамических сетей на базе технологии ZigBee стандарта 802.15. 4 //Сборник международной конференции «Информатика и компьютерные технологии. – 2009.
3. Беспроводные сети ZigBee и Thread // [Электронный ресурс]. – Режим доступа: https://wless.ru/technology/?tech=1.

МОДУЛЬ ВЕДЕНИЯ ОТЧЕТНОСТИ ЗА ОБРАБОТАННЫМИ ДОКУМЕНТАМИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ МЕНЕДЖМЕНТА ПРАВОВЫХ АКТОВ

Резниченко А. В., студент гр.763101

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Шевчук О. Г. − к. т. н., доцент

Аннотация. Работа представляет собой описание разработки одного из модулей распределенной системы, описание и обоснование выбранных инструментов для разработки, описание самой распределенной системы в целом и описание непосредственно разработанного для нее модуля. Представлены внешний вид разработок, а также описание решаемых ею задач и функций.

Ключевые слова. Распределенная система, модуль, клиент, сервер, база данных, архитектура «клиент-сервер», правовые акты, данные, формирование отчета, запрос, ответ.

В настоящее время наблюдается активное развитие индустрии современных информационных технологий. На рынке информационных технологий с каждым днём появляется всё больше новых востребованных разработок. Достижения современных технологий активно внедряются в повседневную жизнь любого человека и применяются они в различных сферах и областях общественной жизни.

Информационные технологии также нашли широкое использование в юридической и правовой деятельности. В данных сферах они позволяют решать определенные задачи, возникающие при исполнении профессиональных обязанностей и во время общественных отношений.

Распределенная система (приложение) – это программа, состоящая из нескольких взаимодействующих частей, каждая из которых, как правило, выполняется на отдельном компьютере (или другом устройстве) сети; приложение разработанное по архитектуре «клиент-сервер», использующее в качестве клиента веб-браузер и взаимодействует с сервером по средством запросов, а сервер отвечает на посылаемые клиентом запросы.

Логика распределенной системы распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети. Преимущество такого подхода заключается в том, что клиенты не зависят от операционной системы, поэтому распределенные системы являются кроссплатформенными.

В основе работы распределённой системы лежит модель взаимодействия клиент-сервер, которая позволяет разделять функционал и вычислительную нагрузку между клиентскими приложениями (заказчиками услуг) и серверными приложениями (поставщиками услуг) [1].

Система менеджмента правовых актов (СМПА) представляет собой многомодульную распределенную систему, общая схема которой представлена на рисунке 1, которая позволяет решать различные задачи, связанные с регистрацией, ведением правовых актов, ведением справочников, классификаторов банков данных и ведением статистики обработанных правовых актов. Внешний вид раздела ведения банков данных локальных правовых актов СМПА представлен на рисунке 2.

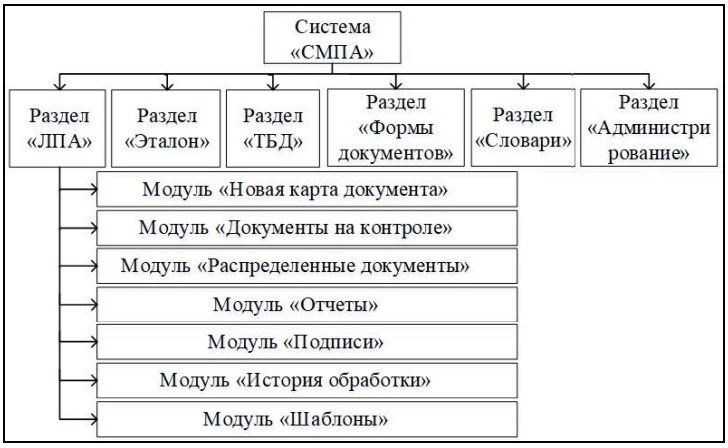


Рисунок 1 –Общая схема системы менеджмента правовых актов

Средство ведения банков данных локальных правовых актов «Система менеджмента правовых актов» позволяет:

– обеспечить ведение Национальным центром правовой информации Республики Беларусь банков данных локальных правовых актов для государственных органов и иных организаций, содержащих принимаемые государственными органами, иными организациями локальные правовые акты и документы, связанные с использованием и применением на практике принимаемых ими правовых актов, в составе информационно-поисковой системы «ЭТАЛОН»;

– осуществлять необходимое организационно-техническое взаимодействие между центром и его филиалами – региональными центрами правовой информации при формировании и ведении данных ресурсов с последующим развитием в направлении формирования единого информационно-правового пространства Республики Беларусь.

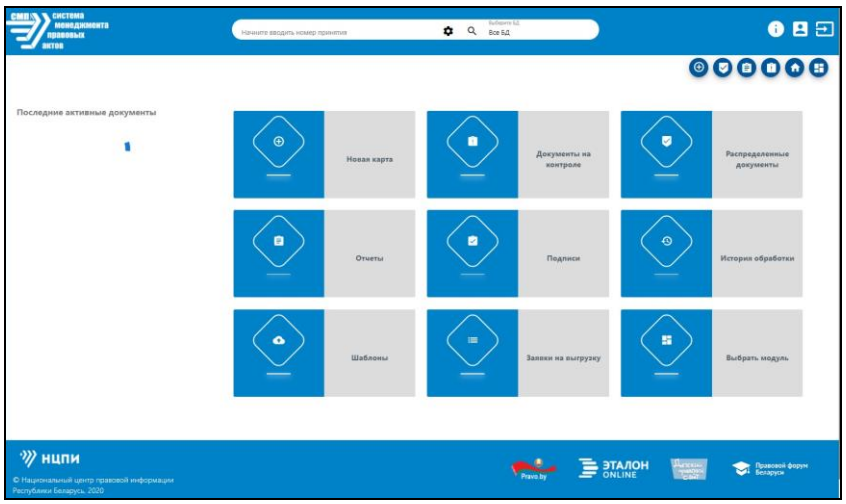


Рисунок 2 – Внешний вид раздела ведения банков данных локальных правовых актов СМПА

Разрабатываемый модуль ведения отчетности за обработанными документами, представленный на рисунке 3, позволяет пользователям вести статистику по обработанным документам по каждому локальному банку данных правовых актов и каждому отдельному пользователю с применением определенных фильтров, таких как: период выборки, формат документа, готовность локального правового акта, банк данных, сотрудник, поля для выгрузки в отчет. В данном модуле также предусмотрена функция выгрузки сформированного отчета в формат документа doc приложения «MS Word».

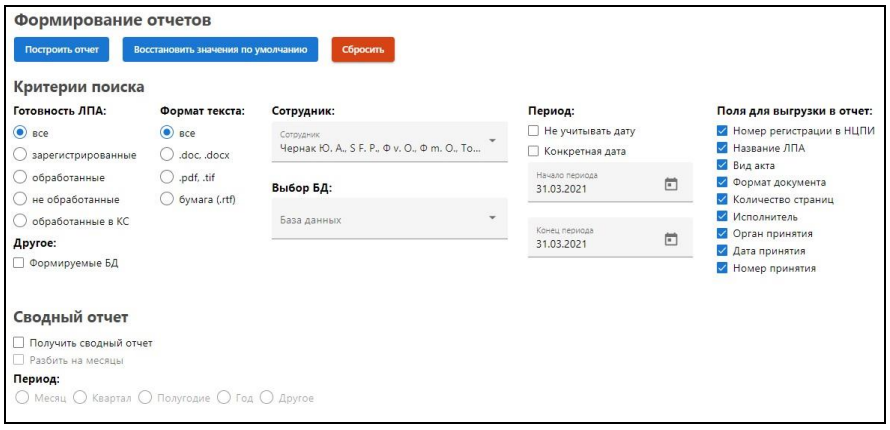


Рисунок 3 – Внешний вид модуля ведения отчетности СМПА

Данный модуль включает следующие возможности:

– построение отчета по отдельным критериям поиска (готовность ЛПА, формат текста, сотрудник, выбор БД, период и поля для выгрузки в отчет);

– построение сводного отчета по конкретному периоду (готовность ЛПА, выбор БД и выбор периодов).

Для написания клиентской стороны пользовательского интерфейса данного модуля была использована платформа Angular, которая представляет из себя фреймворк от компании Google

для создания клиентских приложений. Данная платформа предоставила возможность использовать такую функцию, как двустороннее связывание, которая позволяет динамически изменять данные в одном месте интерфейса при изменении данных модели в другом. Одной из ключевых особенностей Angular является то, что он использует в качестве языка программирования TypeScript [2].

Клиентская часть реализует пользовательский интерфейс, формирует запросы к серверу и обрабатывает ответы от него.

Для разработки программно-аппаратной (серверной) части модуля был использован объектно-ориентированный язык C Sharp, который имеет ряд преимуществ, использованных при разработке: имеет статическую типизацию, поддерживает полиморфизм, перегрузку операторов (в том числе операторов явного и неявного приведения типа), делегаты, атрибуты, события, свойства, обобщённые типы и методы, итераторы, анонимные функции с поддержкой замыканий, LINQ, исключения, комментарии в формате XML [3].

Разработанный модуль функционально выполняет следующие задачи:

- ввод критериев составления отчетов;
- вывод информации в соответствии с критериями;
- форматирование представленной информации;
- вывод представленной информации в формате документа doc.

Перейдя в модуль ведения отчетности, который в СМПА именуется как «Отчеты», пользователь инициирует следующий процесс – процесс получения сформированного отчета, который состоит из следующих этапов (см. рисунок 4):

Рисунок 4 – Диаграмма последовательности получения сформированного отчета

1 Пользователь, перейдя в модуль «Отчеты», запрашивает у сервера форму для заполнения критериев, по которым будет формироваться отчет.

2 Сервер, получив запрос от пользователя, отправляет страницу с формой для формирования критериев для построения отчета со всеми вложенными в нее значениями.

3 Клиент заполняет полученную с сервера форму определенными данными, которые необходимы для построения отчета согласно его запросам. После заполнения формы пользователь оправляет её на сервер.

4 Сервер, получив форму с введенными пользователем данными, производит валидацию данных введенных в данную форму.

5 Если валидация данных формы была произведена успешно, то сервер формирует запрос к базе данных с выделенными из данной формы параметрами и отправляет его базе данных.

6 База данных, получив запрос от сервера, начинает формировать массив документов из общего массива, хранящегося в базе данных, которые соответствуют полученным в запросе параметрам. После формирования данного массива документов база данных отправляет его в ответ на запрос назад на сервер.

7 Сервер, получив массив документов от базы данных, начинает формирование новых запросов по каждому документу для заполнения всех полей, запрошенных пользователем в форме, всей необходимой информацией. После формирования запроса сервер отправляет его базе

данных и повторяет данную процедуру для каждого документа из полученного массива.

8 База данных, получив запрос на предоставление дополнительной информации по каждому документу, начинает сбор соответствующей информации для каждого из документов. После формирования массива данных для документа база данных отправляет этот массив в ответ на запрос по определенному документу назад на сервер и повторяет данную процедуру для каждого полученного запроса по документам.

9 Сервер, получив от базы данных дополнительную информацию для определенного документа, дополняет ранее полученный массив документов дополнительной информацией по каждому из них. После формирования полного массива данных по каждому из документов сервер отправляет всю информацию пользователю.

10 На стороне пользователя происходит графическое формирование из полученного массива данных отчета, который будет понятен пользователю.

На рисунке 5 представлен внешний вид сформированного отчета:

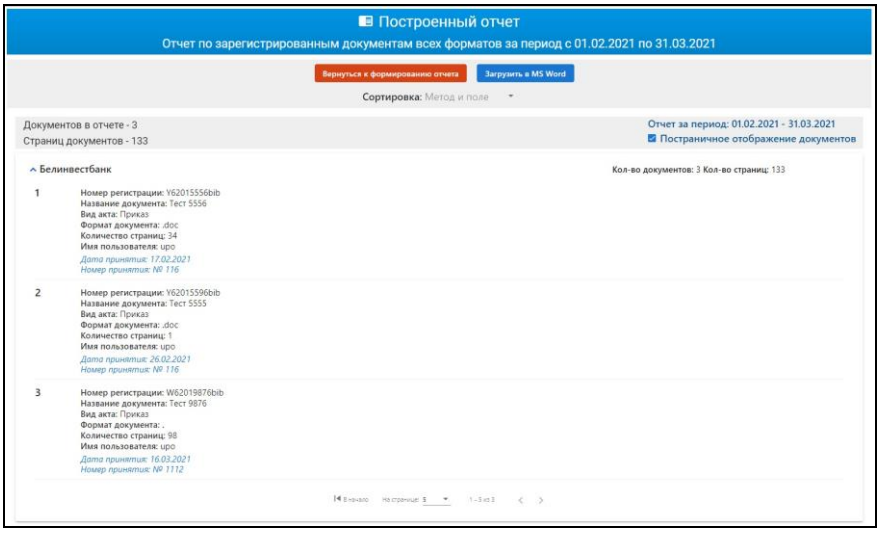


Рисунок 5 – Внешний вид сформированного отчета

Таким образом, был разработан модуль распределенной системы менеджмента правовых актов соответствующий всем поставленным перед ним функциональным требованиям и нормам, были проанализированы и выбраны основные технологии и средства для разработки его клиентской и серверной частей.

Список использованных источников:

3. Олищук, А. В. Разработка Web-приложений на PHP5. Профессиональная работа / А. В. Олищук, А. Н. Чаплыгин. – Москва, 2006. – 352 с.

4. The architecture of open source applications [Электронный ресурс]. – Режим доступа: http://www.aosabook.org/.

5. Скит, Джон. C# для профессионалов: тонкости программирования, 3-е изд. / Джон, Скит. – Москва, 2014. – 608 с.

ЗАЩИТА СЕТЕВОГО УРОВНЯ ПРИ ПОМОЩИ ПРОТОКОЛОВ GRE OVER IPSEC

Сакович Д.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шевчук О. Г. − к. т. н., доцент

В нынешнее время многие компании столкнулись с проблемой организации удалённого доступа между филиалами. Для этого многие из них прибегают к использованию инфраструктуры провайдера для соединения. Однако данная сеть небезопасна для использования в коммерческих целях. Для повышения защиты используется технология туннелирования при помощи протоколов GRE и IPSec.

Использование туннелей GRE вместе с IPSec дает несколько преимуществ, прежде всего потому, что IPSec не поддерживает трафик, отличный от одноадресной. Это может привести к проблемам, если планируется использоваться службы, требующие такого типа трафика, например, протоколы динамической маршрутизации, такие как OSPF или EIGRP, что можно увидеть на рисунке 1.

Благодаря процессу инкапсуляции GRE широковещательный и многоадресный трафик инкапсулируется в одноадресный пакет, который может обрабатываться IPSec, что делает возможной динамическую маршрутизацию между одноранговыми узлами, разделенными небезопасной сетевой областью.

Кроме того, туннели GRE обеспечивают более высокий уровень отказоустойчивости, чем на самом деле пакеты поддержки активности IKE.

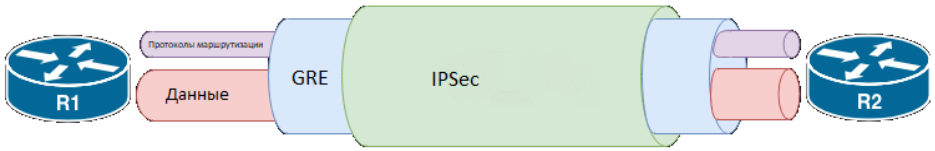


Рисунок 1 – Структура GRE over IPSec туннеля

Для развертывания на сетях был выработан алгоритм, по которому будет организовываться защита сетевого уровня. Данный алгоритм можно увидеть на рисунке 2.

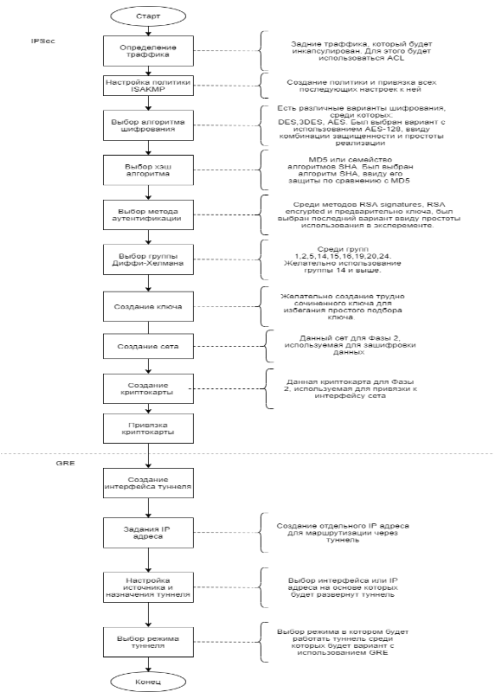


Рисунок 2 – Алгоритм установления защиты при помощи GRE over IPSec

По каждому шагу можно понять какие методы были использованы для инициализации туннелирования.

Данный алгоритм был использован и протестирован смоделированной сети при помощи перехвата пакетов для оценки его. Для моделирования сети был использован программа для эмуляции Cisco Packet Tracer. Результат перехвата одного из пакетов представлен на рисунке 3.

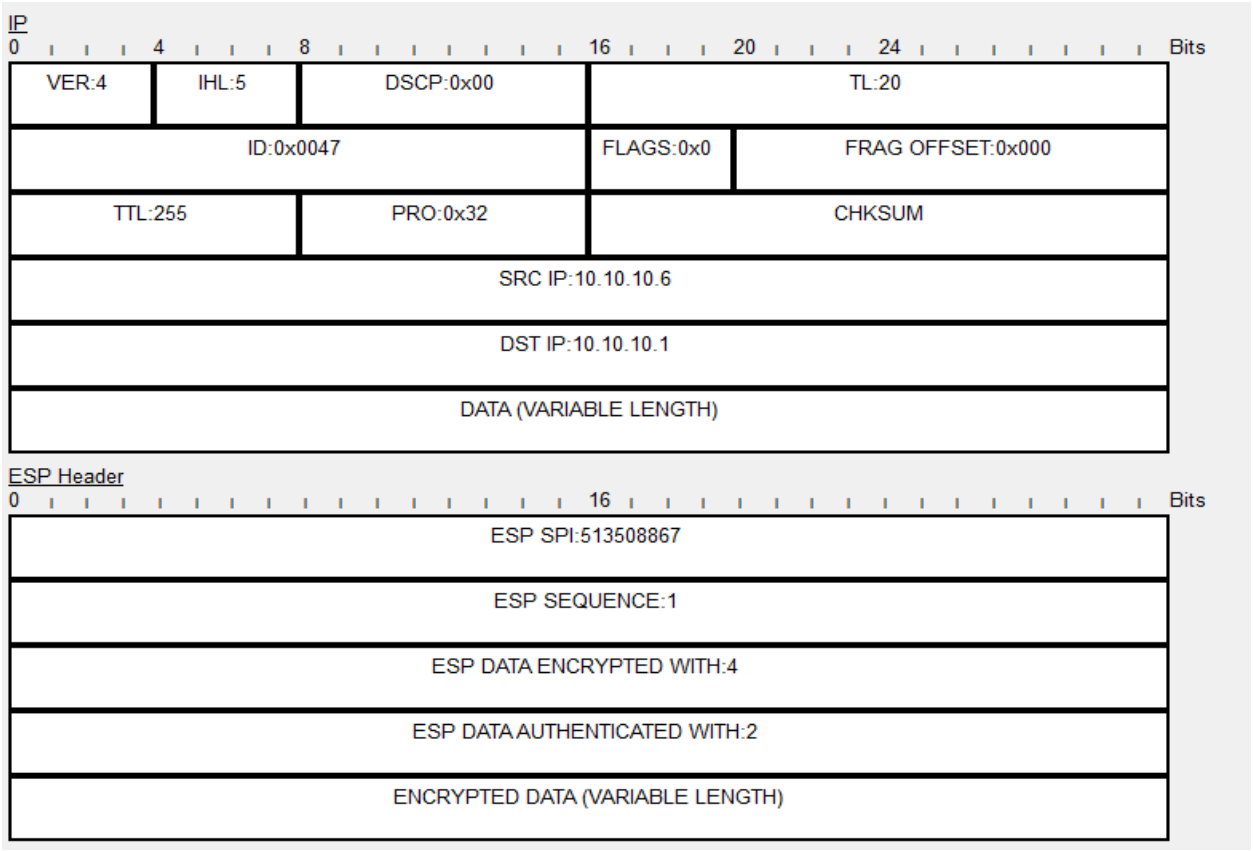


Рисунок 3 - Перехваченный инкапсулированный пакет

При перехвате пакета был получен результат, что данные находятся в зашифрованном и инкапсулированном состояние.

Таким образом, данный метод защиты не даёт возможность злоумышленнику узнать данные передаваемые по сетевому уровню IP.

Список использованных источников:

1. RFC 4301 Security Architecture for the Internet Protocol / S. Kent, K. Seo, december 2005.
2. RFC 1701 – Generic Routing Encapsulation (GRE) / Stan Hanks, october 1994

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ БЛОКЧЕЙН СЕТЕЙ

Яковчик Н.В., студент гр.967041 магистрант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич И.А. – к.т.н., доцент

Аннотация. В данной работе рассматриваются факторы, оказывающие влияние на производительность блокчейн сети, в частности на величину Transactions Per Second (TPS).

Ключевые слова. блокчейн, производительность, tps.

При подсчете TPS время обработки транзакций собирается с узлов сети [1], что не совсем корректно, так как на практике клиентское приложение не может получить указанный результат. Более наглядным является подсчет времени с момента начала формирования транзакции до момента получения достоверной информации о включении данной транзакции в блокчейн. Но при данном подходе на разных клиентских приложениях результат может отличаться в несколько раз, даже при отправке идентичной транзакции. Далее будут рассмотрены этапы обработки транзакций, которые могут повлиять на производительность всей сети.

В блокчейн сетях транзакция формируется и подписывается клиентским приложением. Например, блокчейн, использующий доказательство принадлежности к списку на основе merkle-tree, не требует много ресурсов для верификации в цепочке, но ресурсозатратен при подготовке транзакции [2]. Это означает, что производительность клиентского устройства прямо влияет на скорость обработки транзакций.

Прежде чем приступить к отправке транзакции, клиентское приложение должно запросить состояние блокчейна. Когда сеть имеет мало узлов, это не оказывает существенного влияния, но когда сеть разрастается, таких запросов становится довольно много и они могут повлиять на загруженность сети. Из-за чего такие запросы будут обрабатываться медленнее.

На следующем шаге клиентское приложение должно отправить транзакцию в один из узлов блокчейна. Этот узел начинает распространять информацию о транзакции через peer-to-peer (p2p) сеть до тех пор, пока транзакцию не увидит узел, формирующий блоки, и не добавит ее в один из блоков. Так как клиентское приложение знает хеш транзакции – ему нужно дождаться изменения состояния блокчейна и проверить, есть ли нужный хеш в новых блоках цепочки.

В большинстве современных p2p сетей используются разные модификации протокола Kademila [3]. В целом, этот вид сетей сложен и менее предсказуем, чем привычные сети централизованных сервисов. Анализ затрудняется воздействием таких факторов, как количество активных нод, расположеных рядом, размер блоков и транзакции.

Добавление транзакций в блоки и включение их в блокчейн должно происходить максимально быстро, но могут возникать случаи, когда две длинные конкурирующие цепочки, переключаясь между собой, производят изменения метаданных тысяч транзакций [4]. Главным фактором воздействия на данном этапе является выбранный алгоритм консенсуса. К тому же, смарт-конракты являются программами, которые требуют определенных ресурсов для исполнения [5]. А если смарт-контракт генерирует большой массив данных – клиенту потребуется больше времени на прием информации при медленном интернет-соединении.

В итоге, можно выделить следующие категории операций, производимых в блокчейн сетях и влияющих на производительность:

1. криптографические преобразования;
2. передача данных в p2p сети;
3. выполнение смарт-контрактов;
4. фиксация изменений в блокчейне;
5. получение клиентом обновления состояния.

Список использованных источников:

1. Australasian Telecommunication Networks and Applications Conference., Melbourne, 22-24 Nov. 2017 / Rendezvous Hotel ; ed.: A.E. Krzesinski [et al.]. – IEEE Explore, Melbourne 2017. – 96p.

2. Hackernoon [Electronic resource] : Evolution of Airdrop: from Common Spam to the Merkle Tree. – Mode of access: https://hackernoon.com/evolution-of-airdrop-from-common-spam-to-the-merkle-tree-30caa2344170. – Date of access: 15.03.2021.

3. IMC '18: Proceedings of the Internet Measurement Conference., Boston, Oct. 31 – Nov. 02 2018 / Northeastern University ; ed.: S. Zannettou [et al.]. – Boston : The Association for Computing Machinery, 2018. – 202 p.

4. Performance Evaluation of Blockchain Systems: A Systematic Survey ; Fan C. [et al.] . – Edmonton : IEEE Acces 2020. – 24p.

5. 17th International Conference, Held as Part of the Services Conference Federation, SCF 2020., Honolulu, 18-20 Sep. / IEEE Computer Society ; ed.: W. Qingyang [et al.] – Honolulu : Springer, 2020. – 155p.

UDC 004.72

DESIGN OF IOT NETWORK

Usama H.M.[1] master student gr. 967011

Belarusian State University of Informatics and Radioelectronics[1]
Minsk, the Republic of Belarus

Vishnyakou U.A. – doctor of techn. science, professor

Annotation. The design of IoT network structure on Google Cloud IoT platform are given. GPRS-A LTE as controller is discussed.

Key words. IoT design, Google Cloud IoT platform, GPRS-A LTE module.

Solutions for the Internet of Things (IoT) network - this is a set of resources and components divided by IoT devices, IoT platform and IOT applications. Events, analytical information and actions are data streams and processing conveyors that are performed in these structural parts.

Consider the process of building the Internet of Things (IoT) network to control the temperature and energy in the building, including the device (sensors), a microcontroller, a network gateway, the Google Cloud IoT cloud platform (CP), a mobile device. The controller, depending on its configuration, performs the functions of collecting information from the accounting device, its accumulation and subsequent transfer to the server, from where it becomes available to the end user.

The gateway is required to convert and transmit data to a cloud platform (OP). In the cloud environment, the server is involved. OP server contains measurement databases, site.

Cloud Internet of Things platform - placed in the cloud managed service, which acts as a message center for bilateral relations between the Internet application of things and devices that it controls. The functionality of the platform allows to create scalable, full-featured internet solutions, for example, to monitor the use of an office building. The platform provides sensors a secure communication channel to send data. Authentication for a separate sensor allows to safely connect to the platform and safely control each device. A wide range of device features supports multiple authentication types. SAS token-based authentication allows to quickly start working with the Internet solving things. Separate authentication based on X.509 certificate is used for secure authentication based on standards.

In the database, the received data from the device (serial number of the instrument, the network address of the device, the energy measurement unit, the measured heat value, the pressure indication, the type of inputs G3/G4, the type of temperature sensors, etc.) is stored.

The site serves as a means of displaying captured and obtained results. On each of the mobile devices, it can install an application that allows to display the information you are interested in the cloud database through the site. To ensure remote removal, the instruments can be equipped with an LTE interface.

The Google Cloud IoT platform includes a number of services with which you can create an IoT network. Cloud IoT Core is a fully managed service for easy and secure connection, as well as management and reception data from various devices. Cloud Pub/Sub is a service that processes information about events and provides real-time thread analytics. Cloud Machine Learning Engine, which allows to create learning models and use data obtained from IoT devices [1].

As a microcontroller and gateway, we will apply a GPRS-A LTE - a universal monitoring module that can work automatically or within the system of alarm system, as well as building automation systems [2]. The device is equipped with a module that supports data transmission in LTE technology.

Using a cellular network (TCP), the module can exchange data with devices in IoT). This allows you to integrate the module with automation and data collection systems. The module can send to the devices to IoT information about the status of inputs and outputs, as well as values from analog inputs and from the 1-Wire bus. In response, the module can finalize requests for blocking / canceling inputs and on / off the outputs of the module.

List of literature sources:

1. Google Cloud IoT solutions [Electronic resource]. – Access code : https://cloud.google.com/solutions/iot. – Data of access : 29.03.2021.

2. GPRS-A LTE [Electronic resource]. – Access code : https://www.satel.pl/ru/produktid/1200. – Data of access : 29.03.2021.

UDC 620.9

ORGANIZATION OF IOT NETWORK

Usama H.M.[1] master student gr. 967011

Belarusian State University of Informatics and Radioelectronics[1]
Minsk, the Republic of Belarus

Vishnyakou U.A. – doctor of techn. science, professor

Annotation. The analysis of structure and organization of network of UoT are given. Some elements of such structure are discussed.
Key words. IoT structure, four levels, sensors, gateway, network capabilities, applications.

The Internet of things belongs conceptually to the next generation of networks, so its structure is similar to the well-known four layer of NGN architecture, which includes smart sensors, transport environment, services and applications [1].

The lowest level of the IoT structure consists of smart objects integrated with sensors. Sensors connect the physical and virtual (digital) worlds, providing real-time data collection and processing. Miniaturization, which reduced the physical size of hardware sensors, made it possible to integrate them directly into objects in the physical world. There are different types of sensors for the relevant purposes, for example, for measuring temperature, pressure, speed, location, etc Most sensors require a connection to a sensor aggregator (gateway), which can be implemented using a local area network (LAN) such as Ethernet and Wi-Fi, or a personal network (PAN) such as ZigBee, Bluetooth, and ultra-wide-band wireless communication over short distances (UWB – Ultra-Wide Band). For sensors that do not require connection to the aggregator, their connection to servers/applications can be provided using global wireless WAN networks such as GSM, GPRS, and LTE.

The large amount of data generated at the first level of IoT by miniature sensors requires a reliable and high-performance wired or wireless network infrastructure as a transport environment (network level). To implement a wide range of services and applications in IoT, it is necessary to ensure that multiple networks of different technologies and access protocols work together in a heterogeneous configuration. These networks must provide the required values for the quality of information transmission, especially for latency, bandwidth, and security. This layer consists of a converged network infrastructure that is created by integrating heterogeneous networks into a single network platform.

There are four levels of management in the IoT network: the application level; the support level for applications and services; the network level; and the device level (sensor + handler) [1].

The application and service support layer includes capabilities for various IoT objectsThe service level contains a set of information services designed to automate technological and business operations in the IoT: support for operational and business activities (OSS/BSS – Operation Support System/Business Support System), various analytical information processing (statistical, data and text mining, predictive analytics, etc.), data storage, information security, Business Rule Management (BRM), BPM – Business Process Management, etc.

At the fourth level of the IoT architecture, there are different types of applications for the relevant industrial sectors and fields of activity (energy, transport, trade, medicine, education, etc.).

The network layer includes network capabilities (access and transport network resource management, mobility management, authorization, authentication, and billing functions, AAA) and transport capabilities (providing network connectivity for transmitting IoT application information and services). The device layer includes the device's capabilities for retrieving information, preprocessing it, and gateway capabilities.

The capabilities of the device include direct exchange with the communication network, exchange through the gateway, exchange through the wireless dynamic ad-hoc network, as well as temporary stop and resume operation of the device for energy saving. The gateway features support multiple interfaces for devices (CAN bus, ZigBee, Bluetooth, Wi-Fi, etc.) and for access/transport networks (3G, LTE, DSL, etc.). Another feature of the gateway is support for protocol conversion, if the protocols of the device and network interfaces differ from each other [1].

There are also two vertical levels, the management level and the security level, covering all four horizontal levels. Vertical operational management capabilities include managing the consequences of failures, network capabilities, configuration, security, and billing data.

List of literature sources:

1. Roslyakov, A.V. Internet of things: studies. manual /A.V. Roslyakov, S. V. Vanyashin, A. Yu. Grebeshkov. – Samara, Phuthi, 2015. − 115 p.

СЕКЦИЯ «СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ»

УДК 621.391

ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ОБУЧЕНИЯ С ОШИБКАМИ АЛГЕБРАИЧЕСКИХ РЕШЕТЧАТЫХ КОДОВ

Алисеенко М.А.[1], аспирант

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Саломатин С.Б. – канд. тех. наук, доцент

Аннотация. Показана временная сложность вычисления алгоритма LWE, реализованного на языке программирования Python, для различных длин открытого сообщения и наличия ошибок.

Ключевые слова. Алгоритм обучения с ошибками, LWE, алгебраические решетки.

Одной из задач разработки алгоритмов защиты данных является их потенциальная способность противостоять различного вида атакам, в том числе на основе пост-квантовых и параллельных вычислений. Применение алгоритмов теории многомерных алгебраических решеток предоставляют возможность формирования пространственно-временного многообразия кодовых криптографических структур [1–4].

Алгоритм алгоритма обучения с ошибками LWE [5] реализован на Python 3.8.7 с использованием модуля numpy. Среднее время вычислений рассчитано из 20 измерений на каждую длину открытого текста с использованием встроенного модуля time. При вычислениях использовались следующие параметры: n=3, m=3, t=10, r=9, q=23, длина сообщения l, состоящего из случайных целых чисел от 0 до r, варьировалась от 2^1 до 2^{20}.

Результаты вычислений представлены в таблице и на рисунке 1 (график построен использованием модуля matplotlib). Сложность вычислений растет экспоненциально.

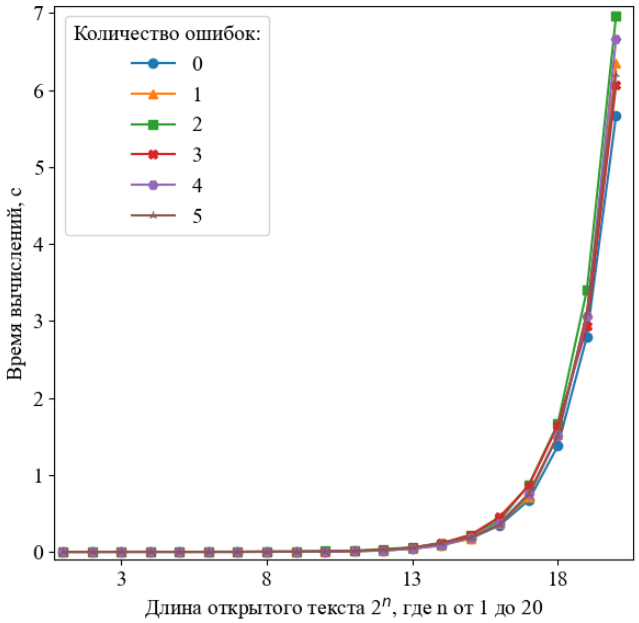


Рисунок 1 – График зависимости среднего времени вычислений в секундах от количества символов открытого текста и наличия ошибок

В настоящее время важность задачи разработки алгоритмов защиты данных определена их потенциальной способностью противостояния к разного рода атакам, таким как постквантовые и параллельные вычисления. Актуальной проблемой становится поиск быстрых алгоритмов шифрования с минимальной вычислительной сложностью для систем связи в сенсорных сетях. Временная сложность алгоритма обучения с ошибками LWE алгебраических

решетчатых кодов растет экспоненциально по мере увеличения длины открытого текста, что необходимо учитывать в аппаратном обеспечении устройств интернета вещей.

Список использованных источников:

1. Low complexity lattice codes for communication networks / Ferdinand N. S. // University of Oulu Graduate School, 2016. – P. 178.

2. The Geometry of Numbers / Olds C.D. // Mathematical Association of USA, 2012. – P. 192.

3. Quadratic integers and Coxeter groups / Johnson N. W., Weiss A. I. // Canadian Journal of Mathematics, 1999. – P. 192.

4. Stallings W. Cryptography and Network Security: Principles and Practice / Stallings W. – Prentice-Hall, Upper Saddle River, New-Jersey, fifth edition, 2006. – P 592.

5. Защита каналов передачи и хранения данных на основе алгебраических решетчатых кодов / М.А. Алисеенко, С.Б. Саломатин // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. науч.-техн. семинара (Республика Беларусь, Минск, ноябрь – декабрь 2020 г.). Минск : БГУИР, 2020. – С. 23-27.

СИСТЕМА АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ УСТРОЙСТВ ИНТЕГРИРОВАННОГО ДОСТУПА

Ипатович А.А., магистрант гр.067041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Давыдова Н.С.– к. т. н., доцент

В докладе рассмотрена разработанная система автоматизированного тестирования устройств интегрированного доступа, работающих по технологии ADSL. Приведены методы автоматизации процессов диагностики и длительного тестирования устройств при ремонте в производственных лабораториях. Описана аппаратная часть системы, структурная схема, а также алгоритм работы программного обеспечения.

Устройство интегрированного доступа (IAD - «Integrated Access Device) — телекоммуникационное оборудование, расположенное в помещении абонента (клиента), может принадлежать клиенту или быть взято в аренду или в наем. Оборудование используется для соединения абонента с сетью оператора (провайдера) для предоставления услуг VoIP, IPTV, доступа в сеть Интернет и др. Среди преимуществ устройств интегрированного доступа можно отметить возможность добавлять новые услуги, не ухудшая уже предоставляемые, а также возможность использования устройств для функций мониторинга локальных сетей, выявления нарушений эксплуатации и управления доступом в сеть. [1].

Основные функциональные возможности устройств интегрированного доступа, работающих по технологии ADSL:

- высокоскоростной доступ к сети Интернет,
- предоставление услуг интерактивного цифрового телевидения по технологии IPTV,
- предоставление услуг телефонной связи по IP (VoIP),
- точка доступа Wi-Fi.

Процесс ремонта абонентских устройств интегрированного доступа в производственных лабораториях включает в себя следующие этапы: диагностика, устранения неисправностей и тестирование, при котором производится проверка работоспособности всех узлов и контроль основных параметров. С течением времени растет как количество выходящих из строя устройств, так и разнообразие возникающих неисправностей. Некоторые из таких неисправностей проявляются лишь при длительной эксплуатации абонентских устройств, что значительно усложняет процессы диагностики и тестирования на рабочем месте по ремонту. В связи с этим возникла необходимость в усовершенствовании и автоматизации процессов диагностики и тестирования ремонтируемых устройств интегрированного доступа.

Основные задачи, решаемые при разработке и внедрении автоматизированной системы тестирования:

1. Повышение качества ремонта абонентских устройств интегрированного доступа. Это достигается путем более длительного тестирования устройств, позволяющего выявить неявные неисправности, которые не проявляются при кратковременной проверке работоспособности.

2. Снижение трудозатрат на операцию длительного тестирования устройств интегрированного доступа. Это достигается максимальной степенью автоматизации системы. Все этапы тестирования проходят без участия оператора: конфигурация SIP-аккаунта, задание локального IP-адреса, мониторинг параметров ADSL соединения, контроль качества канала тональной частоты, фиксирование разрывов Ethernet и ADSL соединений, сброс на заводские настройки устройства.

Система также обладает следующими характеристиками:

1. Универсальность. Система поддерживает все модели абонентских устройств интегрированного доступа, эксплуатируемых на предприятии и работающих по технологии ADSL. Устройства разных производителей и моделей имеют разный интерфейс взаимодействия.

2. Масштабируемость — возможность добавления новых моделей устройств, когда они будут введены в эксплуатацию.

На рисунке 1 приведена структурная схема разработанной автоматизированной системы тестирования устройств интегрированного доступа, содержащая следующие элементы аппаратной части:

- мультисервисный модуль доступа Huawei SmartAX MA5600 с платами услуг ADEE, ADBF для подключения устройств интегрированного доступа по ADSL [2],
- сетевой коммутатор Cisco Catalyst 3560 с 24 интерфейсами Ethernet,
- сервер IP-телефонии на основе свободного программного обеспечения Asterisk,
- ПЭВМ оператора,
- Dial-Up модем Zyxel Omni 2 в качестве телефонного аппарата выполняет функции автоматического телефонного соединения, определителя номера, контроля качества канала тональной частоты,
- коммутатор телефонных каналов — специально разработанное устройство для мультиплексирования телефонных каналов всех тестируемых устройств на стенде с одним телефонным аппаратом,
- источник вторичного питания для устройств интегрированного доступа.

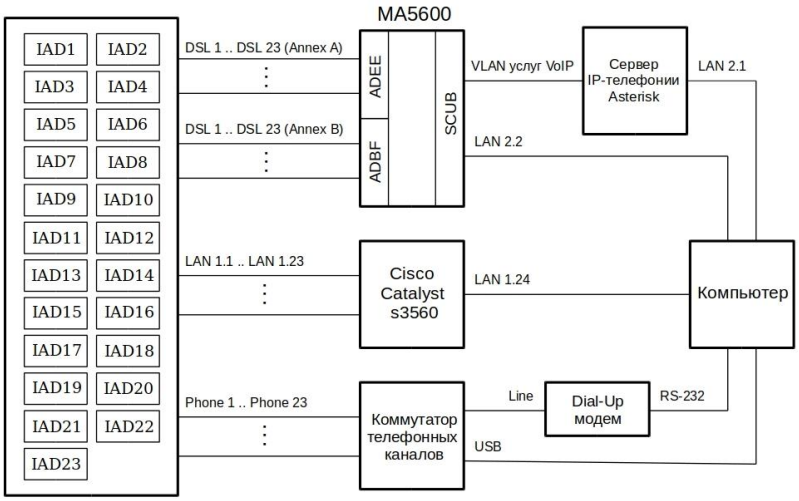


Рисунок 1 – Структурная схема автоматизированной системы тестирования устройств интегрированного доступа, работающих по технологии ADSL

В левой части рисунка схематично показан стенд с установленными на нем 23 абонентскими терминалами, что соответствует максимальной нагрузке системы. Порт 24 сетевого коммутатора выделен для подключения ПЭВМ. К каждому месту тестирования на стенде подведено 2 ADSL линии (Annex A, Annex B) от плат ADEE, ADBF, кабель Ethernet локальной сети от коммутатора Cisco, кабель телефонного интерфейса от коммутатора телефонных линий абонентских устройств. Плата управления SCUB MA5600 имеет два Ethernet подключения: первое — с сервером IP-телефонии, второе — с ПЭВМ системы тестирования и технологической сетью лаборатории. ПЭВМ имеет два сетевых интерфейса. Один используется для доступа в технологическую локальную сеть, модулю MA5600 и серверу IP-телефонии, второй — для подключения к тестируемым абонентским устройствам через сетевой коммутатор. Dial-Up модем подключен к ПЭВМ по интерфейсу RS-232. Коммутатор телефонных каналов абонентских устройств подключен к ПЭВМ по интерфейсу USB 2.0.

Алгоритм тестирования одного устройства интегрированного доступа описывается следующими этапами:

1. Ожидание системой подключения тестируемого устройства с заводскими настройками.
2. Определение модели устройства и его конфигурация: настройка VoIP, локального IP адреса.
3. Отображение информации по устройству в таблице системы и начало автоматизированного тестирования.
4. Периодический контроль ADSL параметров линии, мониторинг статуса регистрации на сервере IP телефонии, совершение автоматических вызовов с проверкой определителя номера и качества канала тональной частоты, контроль соединения по протоколу IP.
5. Завершение тестирования по команде оператора и сброс на заводские настройки, получение отчета о тестировании.

Для реализации работы системы по описанному алгоритму было разработано программное обеспечение на языке программирования Python с использованием таких инструментов, как Selenium, PyQT5, PjSIP и др.

Таким образом, разработанная система позволяет значительно повысить качество ремонта абонентских устройств интегрированного доступа за счет максимальной автоматизации процесса тестирования и более глубокой диагностики неисправностей.

Список использованных источников:

1. Ибе О. Компьютерные сети и службы удаленного доступа: пер с англ. - М.: ДМК Пресс. - 336с.
2. Мультисервисный модуль доступа SmartAX MA5600. Техническое описание. - Huawei, 85 с.

УДК 378.4(476)

ОСОБЕННОСТИ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ И ТЕСТИРОВАНИЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Михнюк Д.Г., Ковятинец И.П., магистранты гр.967041
Mamoudou Cisse, магистрант гр.067001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Астровский И.И. – канд. техн. наук, доцент

Аннотация. Предложены решения для повышения квалификации и тестирования специалистов. Приведен обзор компаний, ведущих подготовку специалистов в области инфокоммуникационных технологий. Показана методика тестирования обучающихся.

Ключевые слова. Повышение квалификации, тестирование специалистов.

Введение

Интернет с каждым днем играет все большую роль в повседневной жизни. Он есть везде, начиная с крупных городов и заканчивая деревнями.

Передача информации не могла бы осуществляться, если бы компьютеры не были объединены в сеть. Наиболее распространены такие сети как глобальные (WAN), городские (MAN), локальные (LAN) и персональные (PAN). Но особую роль из вышеперечисленных играют локальные сети. Локальные сети используют сложное оборудование, которое требует обслуживания высококвалифицированными специалистами. Специалистов обучают в вузах, специализированных колледжах, курсах по подготовке сетевых специалистов. Прежде чем допустить обучающегося до реального оборудования, он проходит обучение на тренажерах. Поскольку происходит постоянная модернизация оборудования и выпускаются более новые версии программного обеспечения, требуется регулярное совершенствование обучающего материала.

Задачами системного администратора являются:

- проверка работоспособности баз данных;
- контроль над бесперебойной работой локальных сетей;
- защита данных и обеспечение их целостности;
- защита сети от незаконного доступа;
- регулировка прав доступа пользователей локальной сети к ресурсам сети;
- резервное копирование информации;
- использование оптимальных методов программирования с целью полного использования доступных средств и ресурсов сети;
- ведение специальных журналов по работе сети;
- осуществление обучения пользователей локальной сети;
- контроль над используемым программным обеспечением;
- контроль над совершенствованием локальной компьютерной сети;
- разработка права доступа к сети;
- приостановление незаконной модификации программного обеспечения для сети.

Цель работы: обзор существующих программ для обучения специалистов и разработка методики и программы тестирования знаний.

Решения для повышения квалификации и тестирования специалистов в области инфокоммуникационных технологий

На сегодняшний день существует большое количество решений для повышения квалификации и тестирования специалистов в области инфокоммуникационных технологий. Основными из которых являются:

1. CISCO SYSTEMS

Компания Cisco, являющаяся ведущим производителем активного сетевого оборудования, только за последний год удвоила свой оборот. Это сказалось на интересе клиентов к обучению по продуктам Cisco. Притом интерес настолько велик, что люди вынуждены записываться на курсы за несколько месяцев вперед.

Cisco разработала специальную программу Cisco Career Certifications для подготовки квалифицированных специалистов по своим продуктам. Согласно программе существуют несколько званий специалистов. Это так называемые карьерные треки (Career Track). В области обслуживания сетей (Network Support) Cisco различает сетевого специалиста (Cisco Certified Network Associate, CCNA), сетевого профессионала (Cisco Certified Network Professional, CCNP), эксперта по сетям (Cisco Certified Internetwork Expert, CCIE); в области проектирования сетей (Network Design) — специалиста по проектированию (Cisco Certified Design Associate, CCDA) и профессионала по проектированию (Cisco Certified Design Professional, CCDP).

С каждым годом поток желающих обучиться непрерывно возрастает. Очередь на курсы составляет около двух месяцев. Инструкторы ISL не только сертифицированы на право чтения курсов, но и являются CCIE. В центрах Cisco обучение проводится на русском языке российскими специалистами.

2. Компания 3COM

В общемировом масштабе 3Com предлагает стандартную двухуровневую схему подготовки специалистов: сначала обучение в авторизованных центрах (по желанию), а затем сертификация в центрах тестирования Sylvan Prometric. Однако в России до недавнего времени специалисты могли лишь пройти авторизованное обучение. Тем не менее сейчас в России стало доступно и тестирование (сертификация) – для этого уже не надо ехать за границу.

По окончании каждого курса слушателям выдается сертификат 3Com международного образца о прохождении курса. Особенно большой интерес слушатели проявляют к курсам по коммутаторам/концентраторам и маршрутизатору NETBuilder. "Микроинформ" организует расписание курсов так, чтобы за один цикл обучения слушатель мог пройти несколько курсов, двигаясь от простого к сложному.

3. BAY NETWORKS

Оборудование Bay Networks в России достаточно популярно. Особенно большой всплеск интереса наблюдался, когда Bay Networks выпустила дешевые и в то же время мощные коммутаторы для Fast Ethernet. Компания Bay Networks недавно объединилась с телекоммуникационным гигантом Nortel, но функционирует в рамках объединенной компании в достаточной степени автономно.

Bay Networks предлагает стандартную двухуровневую схему подготовки специалистов: обучение по желанию в авторизованных центрах и сертификацию (тестирование) в центрах Sylvan Prometric (с некоторыми особенностями). У Bay имеются две квалификации: специалиста (Specialist) и эксперта (Expert). Для получения звания специалиста кандидату необходимо сдать компьютерный тест в Sylvan Prometric. В то же время, чтобы стать экспертом, кандидат должен сначала получить звание специалиста, далее пройти еще один компьютерный тест (эксперта) в Sylvan Prometric и затем сдать практический экзамен в одном из специализированных центров Bay Networks (за границей).

Наиболее востребованным и доступным из представленных решений является компания CISCO SYSTEMS, так как данная компания является ведущим производителем активного сетевого оборудования, разработала специальную программу по подготовке специалистов с нуля, разработала инструмент для моделирования сетей.

Методика тестирования обучающихся

На основе возможностей, предоставленных компанией CISCO SYSTEMS реализован лабораторный стенд изображенный на рисунке 1 и методика для тестирования обучающихся.

Данная методика позволяет поставить перед учащимися целый ряд задач, которые могут быть модифицированы в зависимости от рассматриваемой темы. Решение задач и ответы на поставленные вопросы осуществляются по следующей методике.

Методика тестирования обучающихся на разработанном решении состоит (реализована) из следующих шагов:

1. включить питание. Устройство выполняет Power-On-Self-Test (POST);
2. убедиться в том, что коммутатор действительно сброшен к заводским настройкам;
3. задать имя устройству;
4. задать пароль на привилегированный EXEC режим;
5. запретить нежелательный поиск в DNS;

6. задать баннерное сообщение MOTD, которое будет выводиться перед входом в систему;

7. обеспечить возможность удаленного управления коммутатором, путем настройки IP-адреса на Switch Virtual Interface (SVI);

8. ограничить доступ к консольному порту;

9. настроить линии Virtual Teletype (VTY) для коммутатора, чтобы разрешить удаленный доступ по протоколу Telnet;

10. сохранить настройки коммутатора.

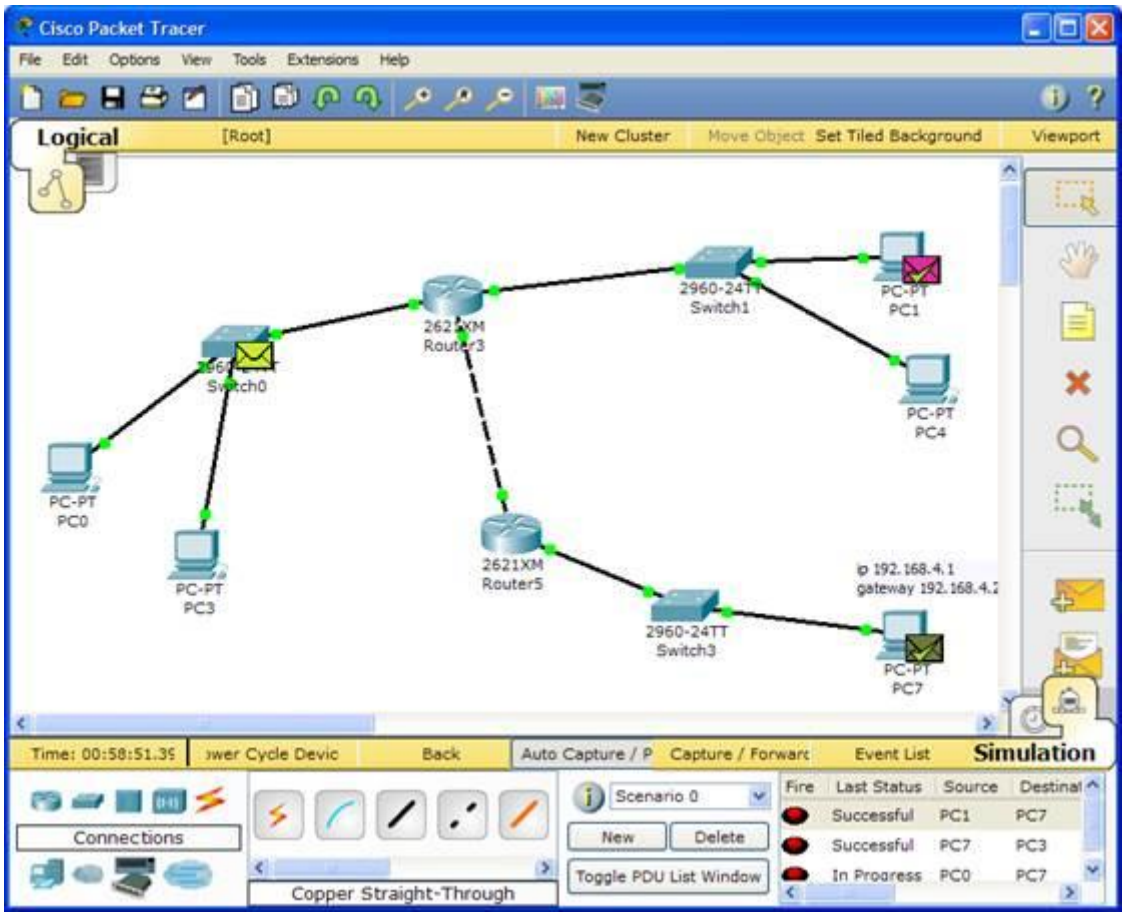


Рисунок 1 – Лабораторный стенд

Используя данную методику можно протестировать знания обучающегося и выявить у обучающегося слабые места при настройке коммутаторов.

Выводы

Предложены решения для подготовки и тестирования специалистов, обслуживающих сети телекоммуникаций. Разработана программа, позволяющая осуществлять проверку знаний специалистов в области инфокоммуникаций. Разработанная программа может быть модифицирована в зависимости от целей обучения.

УДК 621.391.83:681.5

МОДЕЛИРОВАНИЕ СОСТАВНЫХ ИНФОКОММУНИКАЦИОННЫХ СИГНАЛОВ НА КОМПЛЕКСНОЙ ПЛОСКОСТИ И ВО ВРЕМЕННОЙ ОБЛАСТИ

Мойсиевич Ю.С.[1], аспирант

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Ильинков В.А. – канд.тех. наук

Аннотация. Предложены удобные для моделирования способы задания составных инфокоммуникационных сигналов во временной области. Построена математическая модель составных сигналов на комплексной плоскости, основанная на кусочно-линейной аппроксимации.

Ключевые слова. Сигнал, задание, модель, временная область, комплексная плоскость, математическое моделирование

Учитывая стремительное развитие современных систем инфокоммуникаций и радиоэлектроники (СИР), математическое моделирование является основным методом их проектирования и разработки. В связи с этим все более актуальной является задача анализа прохождения различных по свойствам сигналов через реальные каналы (функциональные звенья) СИР.

Эффективная система моделирования должна базироваться на удобных моделях описания простых и составных сигналов, функциональных звеньев, обладать математическими моделями и алгоритмами расчета временных, частотных и энергетических характеристик сигналов и реакций [1, 2]. Упомянутым выше требованиям полностью отвечает моделирование сигналов и звеньев на комплексной плоскости с помощью преобразования Лапласа, которое переносит описание и расчет сигналов из области функций действительного переменного *t* в область комплексного переменного *p* [3]. Преобразование Лапласа удобно как для теоретических методов исследования, так и для реализации математического моделирования на ПЭВМ [3].

Основной задачей любой системы моделирования является нахождение реакции звена (канала) на входное воздействие φ(t). В случае периодического сигнала $\varphi(t) = \varphi(t+T), t \in (-\infty, +\infty)$ Поэтому до начала моделирования необходимо задать отсчетные значения $\varphi_n = \varphi(n\Delta t), (n = \overline{0, N-1}; N = T / \Delta t)$.

Анализ разновидностей решаемых задач, технологии и практики математического моделирования показывает, что эффективная система моделирования должна обеспечивать следующие способы задания входного воздействия во временной области: 1) табличный; 2) файловый; 3) аналитический.

В первом способе задается количество отсчетных значений *N* и формируется таблица (массив) значений сигнала (воздействия) φ_n в точках *n*, полученных экспериментальным или расчетным путем.

Во втором способе используется набор готовых отсчетных значений сигналов, заданных в виде массива отсчетных значений $D_n = \varphi_0, \varphi_1, ..., \varphi_n, \varphi_{n+1}, ..., \varphi_{N-1}$. В общем случае это встроенная в программный комплекс библиотека сигналов.

Аналитический способ предлагает расширенные возможности моделирования. В этом случае предусматривается возможность задания составного сигнала $\varphi(t) = \sum_{m=1}^{M} \varphi_m(t) = \varphi_1(t) + \varphi_2(t) + \varphi_3(t)$ в виде линейной суперпозиции *M* сигналов, описываемых сложными функциями. В результате воздействие задается в виде

$$\varphi(t) = \sum_{m=1}^{M} \varphi_m^{III}\left(\varphi_{m1}^{II}\left(\varphi_{m1}^{I}(t)\right) + \varphi_{m2}^{II}\left(\varphi_{m2}^{I}(t)\right) + \varphi_{m3}^{II}\left(\varphi_{m3}^{I}(t)\right)\right), \quad (1)$$

где φ_m^{III} – функции третьего (высшего) порядка; $\varphi_{m1}^{II},\varphi_{m2}^{II},\varphi_{m3}^{II}$ – функции второго порядка; $\varphi_{m1}^{I},\varphi_{m2}^{I},\varphi_{m3}^{I}$ – функции первого (низшего) порядка.

Последующий анализ показывает, что для описания практически любого составного сигнала достаточно располагать следующим набором так называемых базовых функций:

$$\begin{gathered} f_1(t)=a_1t^3+a_2t^2+a_3t+d+a_4\sqrt{t}+a_5\sqrt[3]{t},\ f_2(t)=at^{-1}+d,\ f_3(t)=ae^{ct}+d,\ f_4(t)=a^{ct}+d, \\ f_5(t)=a\ln(bt+c)+d,\ f_6(t)=a\lg(bt+c)+d, \\ f_7(t)=a\sin(bt+c)+d,\ f_8(t)=a\cos(bt+c)+d,\ f_9(t)=a\,\mathrm{tg}(bt+c)+d,\ f_{10}(t)=a\,\mathrm{ctg}(bt+c)+d, \\ f_{11}(t)=a\arcsin(bt)+c,\ f_{12}(t)=a\arccos(bt)+c,\ f_{13}(t)=a\,\mathrm{arctg}(bt)+c,\ f_{14}(t)=a\,\mathrm{arcctg}(bt)+c, \\ f_{15}(t)=a\int_0^t f(t)dt\equiv a\sum_{k=0}^{N-1}f(k\Delta t)\Delta t,\ f_{16}(t)=0,\ f_{17}(t)=\varnothing, \end{gathered} \tag{2}$$

где a_1, a_2, a_3, a_4, a_5, a, b, c, d – постоянные коэффициенты; $f_{17}(t)$ – пустое множество, функция, которая используется в качестве функции II или III уровня и возвращает значение внутренней функции низшего порядка.

Например, необходимо рассчитать реакцию канала на радиосигнал с периодическим изменением частоты по закону линейной частотной модуляции, который описывается выражением

$$\varphi(t)=U_m\cos\left(2\pi f_ct+2\pi\int_0^t\Delta f_1(t)dt+2\pi\int_0^t\Delta f_2(t)dt+\Phi_0\right), \tag{3}$$

где f_c – исходная частота сигнала; $\Delta f(t)$ – приращение частоты под действие модулирующего сигнала.

Тогда, чтобы привезти функцию $\varphi(t)$ к виду (1) достаточно принять (при $M = 1$):

$$\begin{gathered} \varphi_{11}^{I}(t)=f_1(t)=2\pi f_ct,\ \varphi_{11}^{II}(t)=f_{17}(t)=\varnothing,\ \varphi_{12}^{I}(t)=f_{15}(t)=2\pi\int_0^t\Delta f_1(t)dt, \\ \varphi_{12}^{II}(t)=f_{17}(t)=\varnothing,\ \varphi_{13}^{I}(t)=f_{15}(t)=2\pi\int_0^t\Delta f_2(t)dt,\ \varphi_{13}^{II}(t)=f_{17}(t)=\varnothing, \\ \varphi_{13}^{I}(t)=f_8(t)=\cos\left(\varphi_{11}^{II}(\varphi_{11}^{I})+\varphi_{12}^{II}(\varphi_{12}^{I})+\varphi_{13}^{II}(\varphi_{13}^{I})+\Phi_0\right). \end{gathered} \tag{4}$$

Такая форма представления составного сигнала достаточно проста для понимания и удобна в программировании. При необходимости библиотека базовых сигналов (2) может расширяться и дополняться.

В результате задания входного воздействия получены N отчётных значений $D_n=\varphi_0,\varphi_1,\ldots,\varphi_n,\varphi_{n+1},\ldots,\varphi_{N-1},(n=\overline{0,N-1};N=T/\Delta t)$. С помощью этих отчётных значений можно выполнить аппроксимацию исходного воздействия.

Существует различные способы аппроксимации. Применительно к данной задаче при одновременном учете сложности и точности представления предпочтительна аппроксимация по способу трапеций, при которой воздействие представляется суммой трапецеидальных элементов, как показано на рисунке 1.

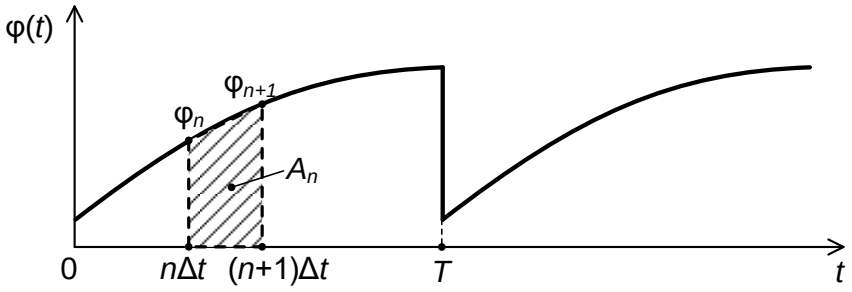


Рисунок 1 – Аппроксимация входного воздействия методом трапеций

В результате исходное воздействие на интервале [0, *T*) описывается в виде

$$\underset{[0,T)}{\varphi(t)} = \sum_{n=0}^{N-1} A_n^T(t), \tag{5}$$

где $A_n^T(t)$ – *n*-ый трапецеидальный элемент, соответствующий отсчётным значениям φ_n, φ_{n+1}.

Чтобы получить представление исходного воздействия (5) на комплексной плоскости, для начала необходимо рассмотреть простые сигналы и их лапласовские изображения.

В задачах моделирования СИК удобно применять следующие простые сигналы (непериодические финитные (рисунок 2, а), периодические (рисунок 2, б), непериодические бесконечно протяженные ((рисунок 2, в)) [4]. Математическое описание этих сигналов во временной области при $0 < t_1 < t_2 < T$ имеет вид:

$$\begin{gathered}
\varphi_{1T}(t) = \begin{cases} \varphi(t), [0, t_1) \\ 0, \quad (-\infty, 0) \cup [t_1, \infty) \end{cases}, \varphi_{2T}(t) = \begin{cases} \varphi(t), [0, t_2) \\ 0, \quad (-\infty, 0) \cup [t_2, \infty) \end{cases}, \varphi_{0T}(t) = \begin{cases} \varphi(t), [t_1, t_2) \\ 0, \quad (-\infty, t_1) \cup [t_2, \infty) \end{cases}, \\
\varphi_1(t) = \begin{cases} \varphi_{1T}(t), \quad [0, T) \\ \varphi_1(t+T), (-\infty, \infty) \end{cases} \varphi_2(t) = \begin{cases} \varphi_{2T}(t), \quad [0, T) \\ \varphi_2(t+T), (-\infty, \infty) \end{cases} \varphi_0(t) = \begin{cases} \varphi_{0T}(t), \quad [t_1, t_2) \\ \varphi_0(t+T), (-\infty, \infty) \end{cases} \\
\alpha_1(t) = \begin{cases} \varphi(t), [t_1, \infty) \\ 0, \quad (-\infty, t_1) \end{cases}, \alpha_2(t) = \begin{cases} \varphi(t), [t_2, \infty) \\ 0, \quad (-\infty, t_2) \end{cases}, \alpha_0(t) = \begin{cases} \varphi(t), [0, \infty) \\ 0, \quad (-\infty, 0) \end{cases},
\end{gathered} \tag{6}$$

где $\varphi_{1T}(t)$, $\varphi_{2T}(t)$, $\varphi_{0T}(t)$ – простые непериодические финитные сигналы; $\varphi_1(t)$, $\varphi_2(t)$, $\varphi_0(t)$ – простые периодические сигналы, $\alpha_1(t)$, $\alpha_2(t)$, $\alpha_0(t)$ – простые бесконечно протяженные сигналы; $\varphi(t)$ – образующая аналитическая функция.

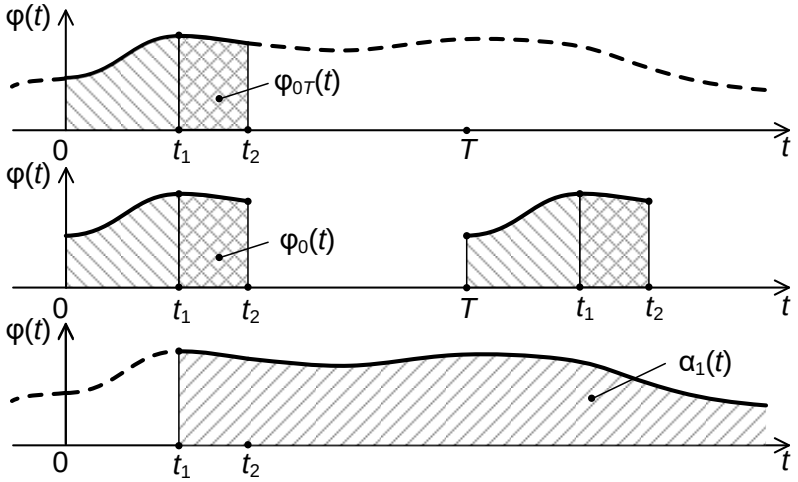


Рисунок 2 – Разновидности простых сигналов

Для сигналов (6) лапласовские изображения представляются в виде [5]:

$$\begin{gathered}
\varphi_{1T}(t) \leftrightarrow \overline{\varphi_{1T}}(p) = S_1(p)e^{-pt_1} - S_0(p), \\
\varphi_{2T}(t) \leftrightarrow \overline{\varphi_{2T}}(p) = S_2(p)e^{-pt_2} - S_0(p), \\
\varphi_{0T}(t) = \varphi_{2T}(t) - \varphi_{1T}(t) \leftrightarrow \overline{\varphi_{0T}}(p) = S_2(p)e^{-pt_2} - S_1(p)e^{-pt_1}, \\
\varphi_1(t) \leftrightarrow \overline{\varphi_1}(p) = \frac{\overline{\varphi_{1T}}(p)}{(1-e^{-pT})}, \\
\varphi_2(t) \leftrightarrow \overline{\varphi_2}(p) = \frac{\overline{\varphi_{2T}}(p)}{(1-e^{-pT})}, \\
\varphi_0(t) \leftrightarrow \overline{\varphi_0}(p) = \frac{\overline{\varphi_{0T}}(p)}{(1-e^{-pT})},
\end{gathered} \tag{7}$$

$$\alpha_0(t) = \lim_{t_1\to\infty} \varphi_{1T}(t) = \lim_{t_2\to\infty} \varphi_{2T}(t) = \lim_{\substack{t_1\to 0\\ t_2\to\infty}} \varphi_{2T}(t) \leftrightarrow \overline{\alpha_0}(p) = -S_0(p) = -\lim_{t_1\to 0} S_1(p) = -\lim_{t_2\to 0} S_2(p),$$

$$\alpha_1(t) = \alpha_0(t) - \varphi_{1T}(t) \leftrightarrow \overline{\alpha_1}(p) = \overline{\alpha_0}(p) - \overline{\varphi_{1T}}(p) = -S_0(p) - \left(S_1(p)e^{-pt_1} - S_0(p)\right) = -S_1(p)e^{-pt_1},$$

$$\alpha_2(t) = \alpha_0(t) - \varphi_{2T}(t) \leftrightarrow \overline{\alpha_2}(p) = \overline{\alpha_0}(p) - \overline{\varphi_{2T}}(p) = -S_0(p) - \left(S_2(p)e^{-pt_2} - S_0(p)\right) = -S_1(p)e^{-pt_2},$$

где $\overline{\varphi_{1T}}(p)$, $\overline{\varphi_{2T}}(p)$, $\overline{\varphi_{0T}}(p)$ – изображения простых непериодических финитных сигналов $\varphi_{1T}(t)$, $\varphi_{2T}(t)$, $\varphi_{0T}(t)$; $\overline{\varphi_1}(p)$, $\overline{\varphi_2}(p)$, $\overline{\varphi_0}(p)$ – изображения простых периодических сигналов $\varphi_1(t)$, $\varphi_2(t)$, $\varphi_0(t)$; $\overline{\alpha_1}(p)$, $\overline{\alpha_2}(p)$, $\overline{\alpha_0}(p)$ – изображения простых бесконечно протяженных сигналов $\alpha_1(t)$, $\alpha_2(t)$, $\alpha_0(t)$;

Таким образом, согласно выражениям (7), изображение элемента $A_n^T(t)$ представляется в виде

$$A_n^T(t) \leftrightarrow \overline{A_n^T}(p) = \int_{n\Delta t}^{(n+1)\Delta t} A_n^T(t)e^{-pt}dt = S_{n2}(p)e^{-pt_2} - S_{n1}(p)e^{-pt_1}, \tag{8}$$

где $t_2 = (n + 1)\Delta t$; $t_1 = n\Delta t$.

Выполняя необходимые преобразования можно получить следующее выражение для $S_{n2}(p)$, $S_{n1}(p)$ и $S_{n0}(p)$:

$$S_{n2}(p) = \frac{(p + a_{n2})}{C_{n2}p^2}, S_{n1}(p) = \frac{(p + a_{n1})}{C_{n1}p^2}, S_{n0}(p) = \frac{(p + a_{n0})}{C_{n0}p^2}, \tag{9}$$

где

$$a_{n2} = \frac{\varphi_{n+1} - \varphi_n}{\Delta t\varphi_{n+1}}; a_{n1} = \frac{\varphi_{n+1} - \varphi_n}{\Delta t\varphi_n}; a_{n0} = \frac{\varphi_{n+1} - \varphi_n}{\Delta t(\varphi_n - n(\varphi_{n+1} - \varphi_n))}; C_{n2} = -\frac{1}{\varphi_{n+1}}; C_{n1} = -\frac{1}{\varphi_n}; C_{n0} = -\frac{1}{\varphi_n - n(\varphi_{n+1} - \varphi_n)}.$$

Зная изображение $\overline{A_n^T(p)}$ одиночного элемента $A_n^T(t)$, согласно (7) находим лапласовское изображение $\overline{A_n}(p)$ периодической последовательности $A_n(t)$ этих элементов:

$$\overline{A_n}(p) = \frac{\overline{A_n^T}(p)}{1 - e^{-pT}}. \tag{10}$$

Тогда изображение всего периодического входного воздействия $\overline{\varphi}(p)$ определяется выражением:

$$\overline{\varphi}(p) = \frac{\sum_{n=0}^{N-1}(S_{n2}(p)e^{-pt_2} - S_{n1}(p)e^{-pt_1})}{1 - e^{-pT}}. \tag{11}$$

Зная изображение исходного воздействия, можно найти реакцию линейного звена (канала), описываемого операторной передаточной функцией $K_z(p)$ [4], на данное воздействие:

$$\overline{\psi}(p) = \overline{\varphi}(p)K_z(p). \tag{12}$$

Таким образом, с помощью преобразования Лапласа получена модель описания составных сигналов на комплексной плоскости. Наиболее важным преимуществом использования преобразований Лапласа является то, что сложные операции дифференцирования и интегрирования сигналов во временной области для их изображений на комплексной плоскости заменяются простыми алгебраическими действиями (умножением и делением), что существенно упрощает моделирование и с легкостью реализуется на ПЭВМ.

Список использованных источников:

1. Трухин, М. П. Основы компьютерного проектирования и моделирования радиоэлектронных средств : учеб. пособие для вузов / М. П. Трухин. – М.: Горячая линия-Телеком, 2015. – 440 с.

2. Баскаков, С. И. Радиотехнические цепи и сигналы : учеб. для вузов/ С. И. Баскаков. – 4-е изд., испр. и доп. – М.: Ленанд, 2016. – 528 с.

3. Лаврентьев М.А., Шабат Б.В. Методы теории функций комплексного переменного: учеб. для вузов. Изд. 6-е, стереотип. СПб.: Лань, 2002. 688 с.

4. Беленкевич, Н. И. Совместное математическое описание сигналов, линейных звеньев и реакций систем телекоммуникаций и радиоэлектроники / Н. И. Беленкевич, В. А. Ильинков // Вес. Нац. акад. навук Беларуси. Сер. физ.-тэхн. навук. – 2017. – № 4. – С. 93–104.

5. Ильинков, В. А. Метод расчета реакции линейной системы на периодическое и непериодическое воздействие / В. А. Ильинков, Н. И. Ильинкова // Вестник БГУ. Сер. 1: Физика, математика, информатика. – 1999. – № 3. – С. 33–38.

UDC 621.391.83:681.5

SIMULATION OF COMPOSITE INFOCOMMUNICATION SIGNALS ON THE COMPLEX PLANE AND IN THE TIME DOMAIN

Maisiyevich Y.S.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Ilyinkov V.A. – PhD in Technology

Annotation. Convenient for modeling methods of specifying composite infocommunication signals in the time domain are proposed. A mathematical model of composite signals on a complex plane based on piecewise-linear approximation is built.

Keywords. Signal, assignment, model, time domain, complex plane, mathematical modeling.

УДК 004.934.1

Статистический анализ в задачах распознавания речи

Новицкая К.А., студент гр. 920605, Нехлебова О.Ю., магистрант гр. 017141

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Печень Т. М. – старший преподаватель каф. ИКТ

Аннотация. В работе обобщается опыт теоретических и прикладных исследований, проводимых на кафедре ИТСиТ Института инженерных технологий и естественных наук.

Ключевые слова. Евклидово расстояние, расстояние Махаланобиса, корреляционная функция, речевой сигнал.

В настоящее время система распознавания речевых сигналов при общении человека с компьютером развивается огромными темпами. Растет важность массового внедрения новых интерфейсов для такого рода взаимодействия, поскольку традиционные интерфейсы уже в скором времени могут достигнуть предела в своём развитии. Также это связано с тем, что около 85% данных мы получаем через органы зрительного восприятия. Таким образом данный канал сейчас становится все более перегруженным. Первоочередной альтернативой является использование акустического канала. Таким образом эта технология становится актуальна не только для людей с ограниченными возможностями, но и для всех людей, активно пользующихся техникой.

Программы обработки в частотно-временной области представляют собой методы, содержащие все преимущества временного и частотного анализов с минимальными проявлениями их недостатков. В зависимости от выбранного метода обработки программы можно разделить на несколько видов. В данной работе были проанализированы виды анализа: с использованием линейных преобразований; с использованием корреляционной функции и евклидовых преобразований.

Применение методов Евклидова расстояния.

Евклидова метрика — наиболее естественная функция расстояния, отражающая интуитивные свойства расстояния между точками. Чем меньше значение евклидова расстояния между речевыми сигналами, которые вычисляются по теореме Пифагора, тем они похожее. Евклидово расстояние между точками речевых сигналов вычисляется по следующей формуле (сноска):

$$d(x,y) = \sqrt{\sum_{i=0}^{N-1}(x_i - x_i)^2} \quad (1)$$

где N – количество точек входных речевых сигналов; i – индексы отсчётов речевых сигналов; x и y – входные речевых сигналы.

Евклидовы методы расчета широко используются в анализе данных в качестве критерия для объединения наблюдений в классы и кластеры, оценки ошибок в предсказательной аналитике, а также в инструментах визуализации.

Расстояние Махаланобиса.

Расстояние Махаланобиса является мерой расстояния между векторами случайных сигналов, обобщающая понятие Евклидова расстояния. Оно отличается от Евклидова расстояния тем, что оно учитывает корреляции между сигналами и инвариантно к масштабу. Однако данная мера расстояния плохо работает в случаях, когда ковариационная матрица рассчитывается исходя из всего множества входных данных. В то же время, будучи сосредоточенной на определенной группе данных, данная метрика показывает хорошие результаты:

$$d(x,y) = (M(x) - M(y))^T \cdot \left(\frac{nx}{nx+ny} \cdot cov(x) + \frac{ny}{nx+ny} \cdot cov(y)\right)^{-1} \cdot \left(M(x) - M(y)\right) \quad (2)$$

где nx – длина речевого сигнала x; ny – длина речевого сигнала y; cov – ковариация речевого сигнала; M – математическое ожидание речевого сигнала; x и y – входные речевые сигналы.

Ковариация и корреляция.

Ковариация оценивает силу линейной зависимости между двумя сигналами, но в то же время не позволяет определить ее:

$$\mathrm{cov}(x,y) = M\left[\left(x_i - M(x)\right)\cdot\left(y_i - M(y)\right)\right] \quad (3)$$

где M - математическое ожидание речевого сигнала; x и y – входные речевые сигналы; i – индексы отсчётов речевого сигнала.

Для получения более точного значения силы зависимости нужно рассчитать коэффициент корреляции. Корреляционная функция является линейной, как и ковариация, и имеет выборку значений от -1 до +1. Линейность корреляции означает, что все точки будут лежать на одной прямой.

Таким образом ковариация - это ни что иное, как мера корреляции:

$$K(x,y) = \frac{\sum_{i=1}^{N}(x_i - M(x))\cdot(y_i - M(y))}{\sqrt{\sum_{i=0}^{N}(x_i M(x))\cdot\sum_{i=0}^{N}(y_i - M(y))}} = \frac{\mathrm{cov}(xy)}{\sigma_x\sigma_y} \quad (4)$$

где M (x) - среднее значение речевого сигнала (математическое ожидание); N – кол-во отсчётов речевого сигнала; i – индексы отсчётов речевого сигнала; x и y – входные речевые сигналы; cov – ковариация между речевыми сигналами; σ - среднеквадратическое отклонение речевого сигнала.

Корреляция относится к масштабированной форме ковариации. Значение корреляции имеет место между -1 и +1. А значение ковариации лежит между -∞ и + ∞. На ковариацию влияет изменение масштаба, т.е. если все значение одной переменной умножается на постоянную, а все значение другой переменной умножается на аналогичную или другую постоянную, то ковариация изменяется.

При выборе метода корреляция предпочтительнее ковариации, поскольку она не зависит от изменения местоположения и масштаба, а также может использоваться для сравнения между две пары переменных.

Среднеквадратическое отклонение (СКО).

СКО - распространённый показатель рассеивания значений случайной величины относительно её математического ожидания:

$$d(x,y) = \sqrt{\frac{\sum_{i=0}^{N-1}(x_i - y_i)^2}{\sum_{i=0}^{N-1}(x_i)^2}} \quad (5)$$

где x и y – входные речевые сигналы; i – индексы отсчётов речевого сигнала; N – кол-во отсчётов речевого сигнала.

Среднее квадратичное отклонение или СКО несет информацию о мощности отклонения сигнала от среднего значения. Также оно отражает шум и другие помехи. Среднеквадратическое отклонение находит отклонение речевых сигналов друг от друга. Поэтому чем меньше значение среднеквадратического отклонения между речевыми сигналами, тем они похожее друг на друга.

Оценка результатов вычислений на основе гипотез.

В данной работе рассматриваются гипотезы о виде и параметрах распределения некоторой генеральной совокупности, а также о сравнении выборок из различных генеральных совокупностей.

Допустим, что нам дана случайная выборка (x_1, x_2,…, x_n) объема n из некоторой генеральной совокупности (конечной или бесконечной). Каждое значение x_i в этой выборке само является случайной величиной, даже если генеральная совокупность состоит из конечного числа элементов. Необходимо также иметь в виду, что случайная выборка из какой-либо генеральной совокупности должна соответствовать некоторой схеме испытаний, при реализации которой выявляется искомая случайная величина X.

Располагая выборочными данными и руководствуясь конкретными условиями рассматриваемой задачи, формулируют гипотезу H_0, которую называют основной или нулевой, и гипотезу H_1, конкурирующую с гипотезой H_0. Гипотезу H_1 называют также альтернативной. H_0

и H_1 – две взаимно исключающие гипотезы. Отметим, что для одной основной гипотезы может быть выдвинуты несколько альтернативных.

Для проверки статистической гипотезы используется специально подобранная случайная величина с известным законом распределения, называемая статистическим критерием. Множество ее возможных значений разбивается на два непересекающихся подмножества: одно из них (критическая область) содержит значения критерия, при которых нулевая гипотеза отклоняется, второе (область принятия гипотезы) – значения, при которых она принимается.

Критерия, позволяющего точно (на 100%) узнать, верна гипотеза H_0 или нет, не существует в силу ограниченности и случайности выборки, так как выборка не содержит всей информации о генеральной совокупности. Отклоняя или принимая гипотезу H_0, можно допустить ошибку двух видов:

– ошибка первого рода совершается при отклонении гипотезы H_0 (т. е. принимается альтернативная H_1), тогда как на самом деле гипотеза H_0 верна; вероятность такой ошибки обозначим:

$$\alpha = P(H_1 / H_0) \quad (6)$$

– ошибка второго рода совершается при принятии гипотезы H0, тогда как на самом деле высказывание H_0 неверно и следовало бы принять гипотезу H_1; вероятность ошибки второго рода обозначим как:

$$\beta = P(H_0 / H_1) \quad (7)$$

Вероятность ошибки первого рода при проверке статистических гипотез называют уровнем значимости и обычно обозначают α. Вероятность ошибки второго рода обозначается β. Величина (1 − β) – мощность критерия. Чем выше мощность, тем меньше вероятность совершить ошибку второго рода.

Вероятность ошибки первого рода при проверке статистических гипотез называют уровнем значимости и обычно обозначают α. Вероятность ошибки второго рода обозначается β. Величина (1 − β) – мощность критерия. Чем выше мощность, тем меньше вероятность совершить ошибку второго рода.

Таким образом, можно сделать вывод, что построенные на основании этих методов закономерности относятся не к отдельным испытаниям, из повторения которых складывается данное массовое явление, а представляют утверждения об общих вероятностных характеристиках данного процесса. Такими характеристиками могут быть вероятности, плотности распределения вероятностей, математические ожидания, дисперсии и т. п.

Найденные характеристики позволяют построить вероятностно-статистическую модель изучающую вопрос о распознавании речи. Таким образом, теория вероятностей по вероятностной модели процесса предсказывает его поведение, а математическая статистика по результатам наблюдений за процессом строит его вероятностно-статистическую модель.

Список использованных источников:
1. Марей Раад Али Салех «Исследование признаков речевых сигналов для задач распознавания речи», 2017.
2. С. Е. Демин, Е. Л. Демина: «Математическая статистика»: учебно-методическое пособие.

UDC 004.934.1

STATISTICAL ANALYSIS IN SPEECH RECOGNITION PROBLEMS

Novitskaya K.A.,Niakhlebava V.Y.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Pechan T.M. – assistant professor of the academic department of ICT

Annotation. The work summarizes the experience of theoretical and applied research carried out at the Department of ITS&T of the Institute of Engineering Technologies and Natural Sciences.

Keywords. Euclidean distance, Mahalanobis distance, correlation function, speech signal.

УДК 004.5

ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ИНФОКОММУНИКАЦИЯХ

Потапова С.А., студент гр.920605, Нехлебова О.Ю., магистрант гр. 017141

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Печень Т.М. – магистр технических наук

Аннотация. Научно-исследовательская работа посвящена вопросу изучения теории принятия решений. На практическом примере рассмотрены вероятности появления рисков проекта, возможные последствия и способы их предотвращения. Расчеты выполнены следующим инструментарием сферы математической статистики и теории вероятности: функция нормального распределения, плотность вероятности, математическое ожидание и дисперсия.

Ключевые слова. Теория принятия решения, кафедра инфокоммуникаций, риск, вероятностная оценка, плотность вероятности, нормальное распределение, математическое ожидание, научно-исследовательская деятельность, кредит.

Анализируя и сравнивая варианты инвестиционных проектов, инвесторы и менеджеры часто действуют в рамках теории принятия решений (ТПР). Вероятностный инструментарий позволяет достаточно четко разграничить понятия риска и неопределённости. В соответствии с этим, в ТПР выделяются два типа моделей:

1) Принятие решений в условиях риска, когда лицо, принимающее решение, знает вероятности наступления исходов или последствий для каждого решения;

2) Принятие решения в условиях неопределённости, когда лицо, принимающее решение, не знает вероятности наступления исходов или последствий для каждого решения.

Под ситуацией риска в теории принятия решений понимается такая ситуация, когда можно указать не только возможные последствия каждого варианта принимаемого решения, но и вероятности их появления. Для выбора оптимального решения в данном случае предназначены критерий математического ожидания и критерий Лапласа.

Сама природа предпринимательского риска предполагает некоторую вероятность возникновения неблагоприятного события. Это означает, что, рассматривая его как вероятностную категорию, мы в полной мере можем применить математический инструментарий, использующий так называемые стохастические модели. Для наилучшего представления об уровне риска используется функция плотности распределения, связанная со стандартным нормальным законом распределения.

Разберем практический пример реализации вполне конкретного инвестиционного проекта. В результате выявления основных факторов риска и его идентификации установлены основные угрозы успеху проекта. Экспертный анализ рисков позволил установить, что опасность представляет несвоевременное погашение кредита банка, который кафедра инфокоммуникаций намерена получить под инвестиции для проведения научно-исследовательских работ. Среднее время реализации проекта – 3 года. Время реализации имеет вероятный разброс в полгода, поэтому с некоторым запасом ссудные средства привлекаются на срок – 4 года. Следует вопрос: есть ли риск того, что кафедра вовремя не вернет кредит? Как избежать дополнительных штрафных санкций от банка и не допустить нарушения кредитной истории?

Формула функции для оценки динамики исследуемого параметра учитывает вероятность рискового события и уровень его последствий:

$$R = f(x) = f(P, I) \quad (1)$$

где, R – значение оценки последствий рискового события;

$f(x)$ – функция параметра x (дохода, прибыли, ущерба, потерь, срока и т.п.)

P – вероятность наступления рискового события;

I – потенциальные последствия фактора риска.

Следует учитывать, что сами действия по формированию вероятностной модели оценки риска и его анализа достаточно трудоемки. Связано это с тем, что факторы риска субъективны и постоянно претерпевают изменения.

Случайная величина имеет нормальное распределение, если её плотность вероятности имеет вид:

$$f(x) = \frac{1}{\sigma_x\sqrt{2\pi}} e^{\frac{-(x-\bar{x})^2}{2\sigma_x^2}} \quad (2)$$

Функция распределения:

$$R = \frac{1}{\sigma_x\sqrt{2\pi}} \int_{x_1}^{x_2} e^{\frac{-(x-\bar{x})^2}{2\sigma_x^2}} dx \quad (3)$$

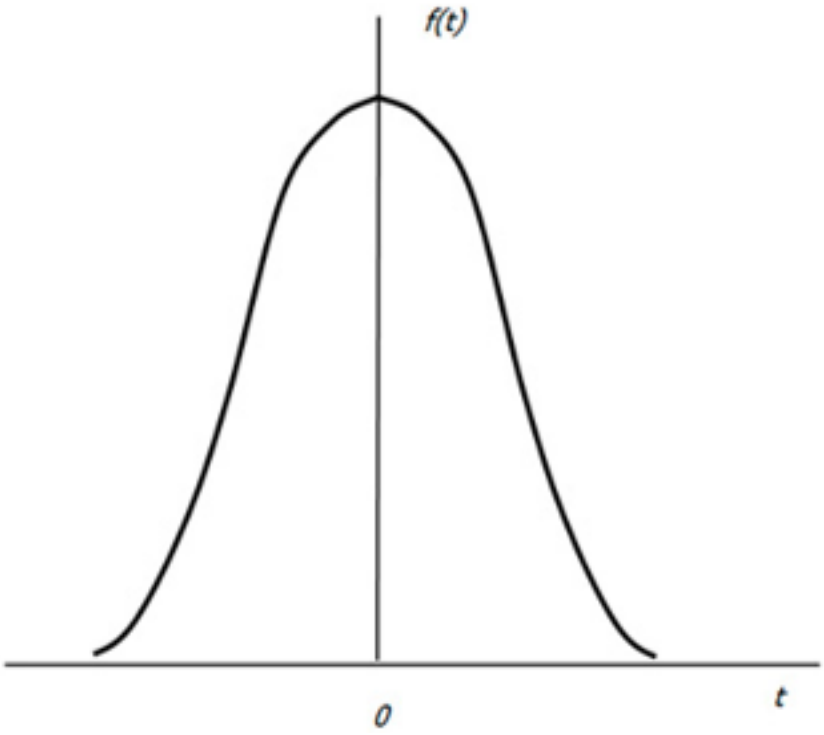


Рисунок 1 – График плотности вероятности случайной величины.

Предположим, мы от периода к периоду имеем определенное значение дохода и хотим на следующий год получить значение риска падения дохода ниже требуемого. Тогда мы должны допустить, что:

1. Статистика рассматриваемого параметра подчиняется нормальному закону распределения.
2. Нам удалось рассчитать среднее значение параметра.
3. Рассчитан разброс в виде среднеквадратического отклонения от среднего значения.

Риск рассматривается с позиции вероятности возникновения результата меньше требуемого размера заданного параметра. Само значение риска исчисляется как интеграл от -∞ до уровня требуемого значения (в нашем случае – дохода) плотности распределения по нормальному закону распределения. Если названные выше допущения соблюдены, тогда риск определяется как площадь, показанная на размещённой ниже диаграмме плотности нормального распределения.

$$R = p(x < Д_{тр}) \quad (4)$$

$$R = \int_{-\infty}^{Д_{тр}} f(x)\,dx = \frac{1}{\sigma_x\sqrt{2\pi}} \int_{-\infty}^{Д_{тр}} e^{\frac{-(x-\bar{x})^2}{2\sigma_x^2}} dx \quad (5)$$

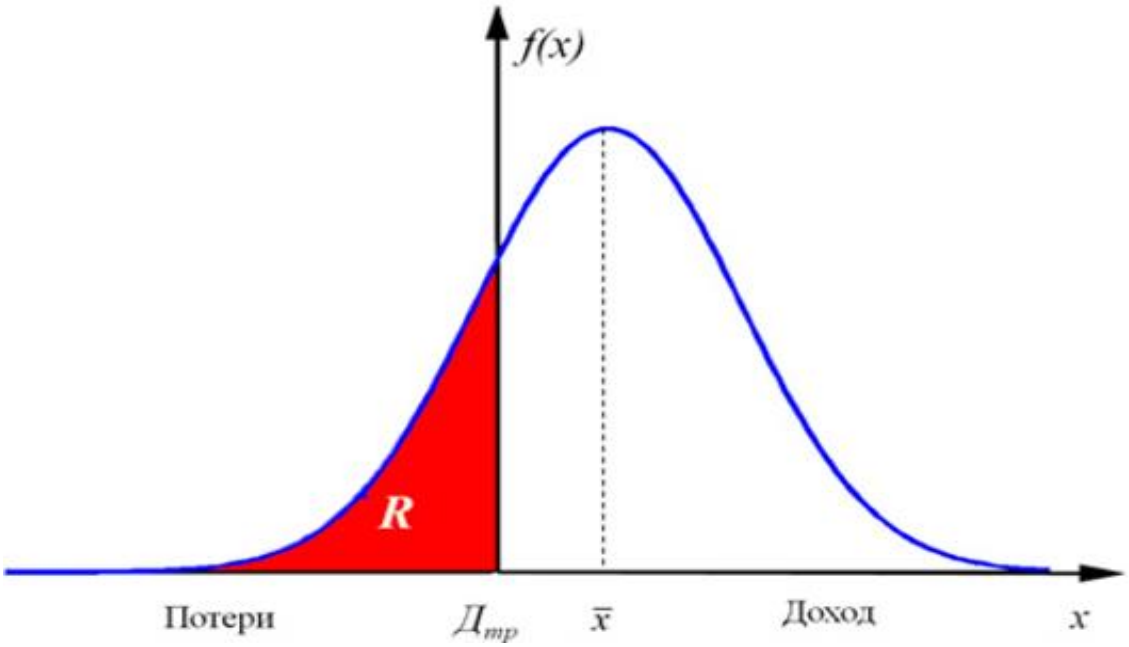


Рисунок 2 – Модель визуального определения риска на кривой плотности нормального распределения.

Для нашего примера имеем:

$X_{проекта} = 3$ года $= 36$ месяцев
$X_{кредита} = 3{,}5$ года $= 42$ месяца
$\sigma_{проекта} = 0{,}5$ года $= 6$ месецев

$$R = 1 - \int_{-\infty}^{X_{кредита}} f(x)dx = 1 - \frac{1}{\sigma_x\sqrt{2\pi}} \int_{-\infty}^{X_{кредита}} e^{\frac{-(x-\bar{x})^2}{2\sigma_x^2}} dx \quad (6)$$

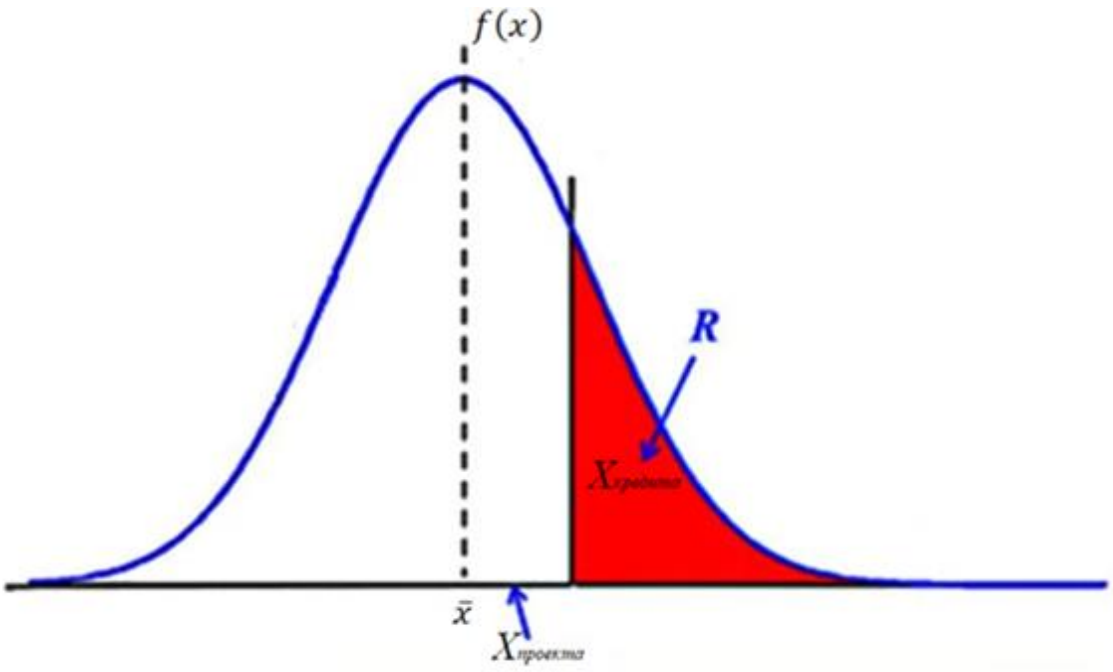


Рисунок 3 – Модель расчета риска для примера инвестиционного проекта

Поскольку мы предполагаем соблюдение типовых допущений вероятностного метода оценки, заданных трех условий достаточно, чтобы произвести надлежащие расчеты. Поскольку плотность распределения подчиняется нормальному закону распределения, нам нужно рассчитать значение риска по формуле (6).

$$R = 1 - \frac{1}{6\sqrt{2\pi}} \int_{-\infty}^{42} e^{\frac{-(x-36)^2}{2*6^2}} dx = 0{,}158655 \quad (7)$$

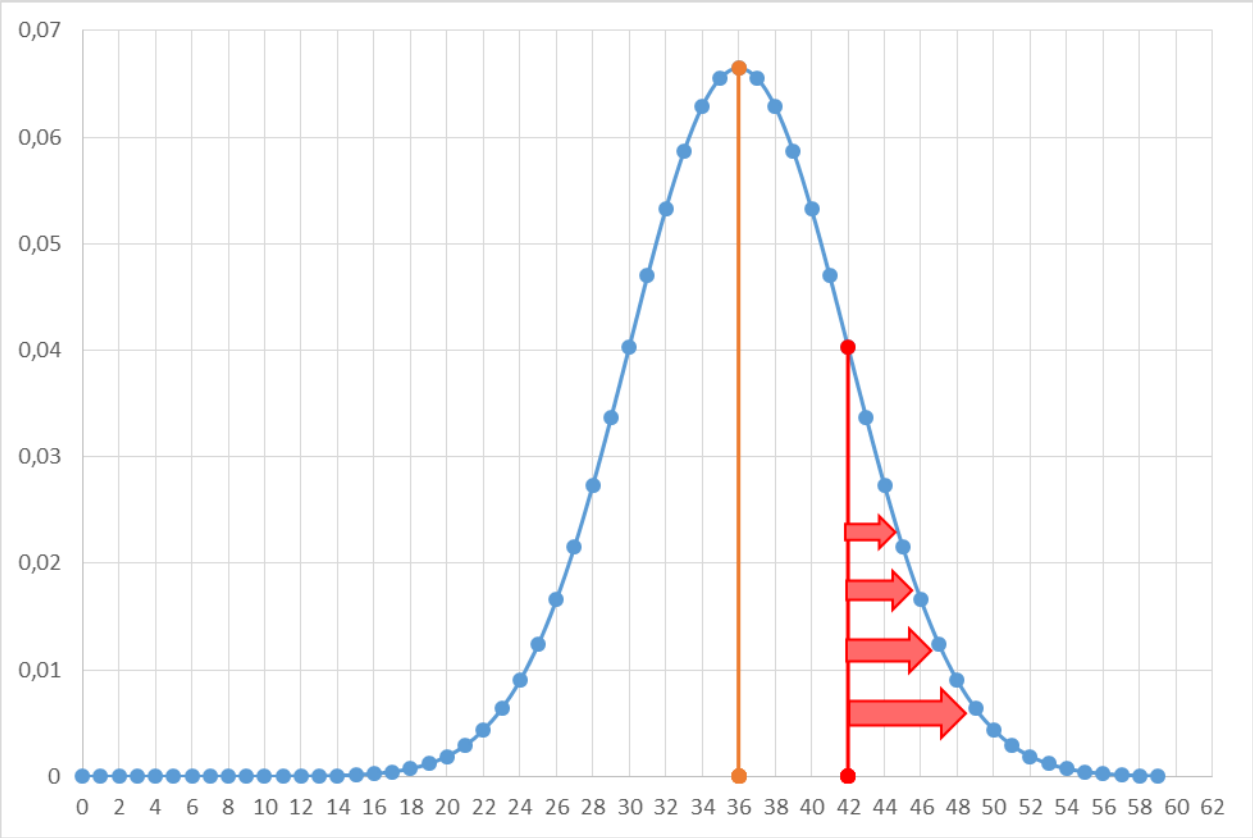


Рисунок 3 – Модель функции нормального распределения

Результаты определения риска по данному методу означают, что с вероятностью 16% при заданных условиях кредит не будет погашен в срок. Изменяя условия длительности кредита, увеличив его на 3 месяца, мы добиваемся того, что значение риска снижается до 6,6%. Зона риска отмечена на диаграмме в форме площади, обозначенной красными стрелками.

Таким образом, методология вероятностной оценки позволяет руководству научно-исследовательской деятельности кафедры просчитывать варианты решений, гипотетически выдвигаемых после выявления и идентификации рисков.

Список использованных источников:

1. Теория вероятностей и математическая статистика: Конспект лекций для студентов всех специальностей и форм обучения БГУИР / А.И. Волковец, А.Б. Гуринович. – Мн.:БГУИР,2003. – 84с.:ил.

2. Орлов А.И. Теория принятия решений. Учебное пособие. - М.: Издательство "Март", 2004. - 656 с.

UDC 004.5

THEORY OF DECISION-MAKING IN INFOCOMMUNICATIONS

Potapova S. A., Niakhlebava V.Y.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

PechenT.M. – Master of Technical Sciences

Annotation. The research work is devoted to the study of the theory of decision-making. The probabilities of project risks, possible consequences and ways to prevent them are considered on a practical example. The calculations are performed using the following tools of mathematical statistics and probability theory: normal distribution function, probability density, mathematical expectation, and variance.

Keywords. Decision theory, Department of Infocommunications, risk, probability estimation, probability density, normal distribution, mathematical expectation, research activity, credit

УДК 621.391.63

ОПРЕДЕЛЕНИЕ МАСКИ OOC-PSD В NG-PON2

Сергеев Н.Н., аспирант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бобов М.Н.. – доктор. техн. наук

Аннотация. Рассмотрено определение маски OOC-PSD. Проведен анализ вариантов размещения несущей в NG-PON2.

Ключевые слова. NG-PON2, ONU, сигнал, маска, помехи, волна, мощность, спектр, коэффициент затухания.

В NG-PON2 передатчик ONU подчиняется правилам вне канала (OOC). А именно, существует два уровня правил OOC. Рассмотрим первое, в нем OOC1 определяется некогерентными перекрестными помехами, которые возникают, когда мешающий свет выходит за пределы полосы пропускания канала-жертвы, и OOC2 определяется когерентными перекрестными помехами, которые будут возникать, когда мешающий свет находится внутри канала-жертвы [1]. Определение маски OOC показано на рисунке 1.

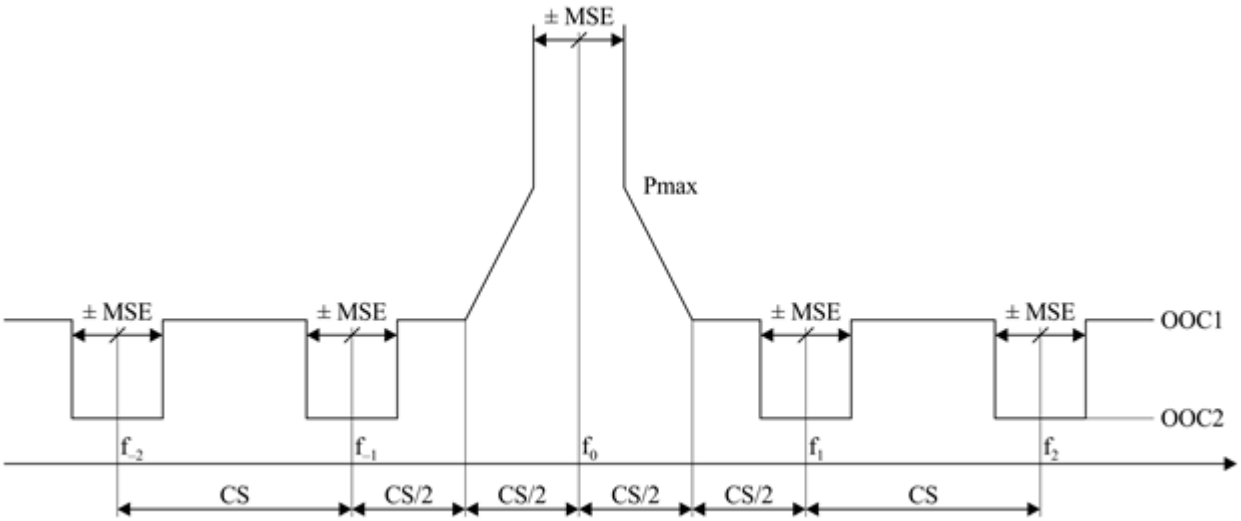


Рисунок 1 – Определение маски OOC-PSD

Переход от когерентных перекрестных помех к некогерентным будет резким только при наличии идеально монохроматического сигнала; сигналы модулируются, что приводит к расширению их спектра, следовательно к смягчению границ между ими [2].

Сигнал, которому подвергаются помехи, представляет собой сигнал NRZ, модулированный по интенсивности на оптической несущей. Форма волны NRZ классически является функцией sinc (f). Чтобы упростить расчет, необходимо моделировать спектр как функцию rect (f) с шириной 15 ГГц (для электрической полосы частот 7,5 ГГц). Предполагая, что коэффициент затухания близок к идеальному, половина мощности идет на модуляцию, а другая половина - на оптическую несущую, которая представлена дельта-функцией (f). Это можно записать:

$$PSD\ (f) = 1/2 * (f - f0) + 1/2\ 1/15\ ГГц\ rect\ ((f - f0) / 15\ ГГц). \quad (1)$$

Худший вариант размещения несущей - это когда f0 находится на расстоянии 7,5 ГГц (или более) от края полосы [3].

Допустимая мощность помех на любой частоте может быть вычислена путем интегрирования по каждой части PSD, которая находится в пределах 7,5 ГГц от частоты помех. Некогерентные перекрестные помехи всегда присутствуют, их количество линейно возрастает.

Список использованных источников:
1. ITU-T Recommendation G.989.2. NG-PON2: Physical media dependent layer specification. 2019. - P. 9 –11.
2.ITU-T Recommendation G.989.3. 40-Gigabit-capable passive optical networks NG-PON2. - P.21–28.
3. Nesset D. / NG-PON2 Technology and Standards / Journal of Lightwave Technology. London. 2015. Vol. 33. -. 1136–1143.

UDC 621.391.63

DEFINITION OF OOC-PSD MASK IN NG-PON2

Sergeev N.N.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Bobov M.N. – Holder of an Advanced Doctorate (Doctor of Science) in Engineering Sciences

Annotation. The definition of the OOS-PSD mask is considered. The analysis of carrier placement options in NG-PON2 is carried out.

Keywords. NG-PON2, ONU, signal, mask, interference, wave, power, spectrum, attenuation coefficient.

УДК 621.3.049.77–048.24:537.2

МОДЕЛИРОВАНИЕ ПРИЕМОПЕРЕДАЮЩЕГО ТРАКТА СИСТЕМЫ СВЯЗИ НА ОСНОВЕ АЛГОРИТМА БПФ-ОБПФ

Синицкий Р.С., студент группы 760802

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Печень Т.М. – ст. преподаватель кафедры ИКТ

Аннотация. Произведено математическое моделирование оценки спектральных характеристик телекоммуникационных сигналов на основе быстрого преобразования Фурье. Установлено, что этот быстрый и мощный инструмент, однако для него необходимо использовать сигналы определенной длины. Обоснованы основные схематические решения.

Ключевые слова: приемопередающий тракт, система связи, алгоритм БПФ-ОБПФ, спектральный анализ, модулятор, демодулятор.

Введение. В настоящее время очень актуальна задача быстрой обработки больших массивов данных, что влечет за собой значительное увеличение производительности обрабатывающих устройств. Интерес к цифровым методам спектрального анализа поддерживается тем улучшением характеристик, которое они обещают, а именно: высоким частотным разрешением, повышенной способностью к обнаружению слабых сигналов или же сохранением «достоверности» формы спектра при меньшем числе используемых параметров. Методы спектрального анализа, а именно с применением алгоритмов, основанных на быстром преобразовании Фурье, являются быстро действенными, несут высокую точность, а также имеют высокое разрешение спектральных оценок.

Основная часть. В основе моделирования приемопередающей части системы связи лежат алгоритмы «переноса спектра вверх» и «переноса спектра вниз». Алгоритм БПФ-ОБПФ позволяет выполнять операции в частотной области с переходом во временную, что сокращает вычислительные объемы, т.е. повышает эффективность обработки. На рисунке 1 представлена структурная схема приемопередающего тракта системы связи на основе алгоритма БПФ-ОБПФ.

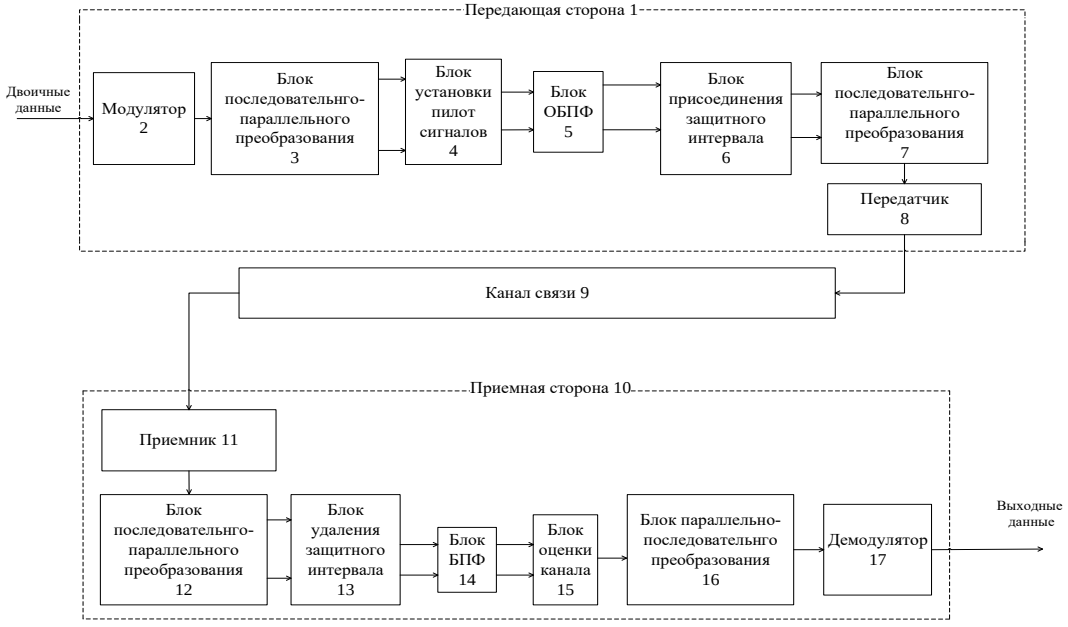


Рисунок 1 – Структурная схема приемопередающего тракта системы связи на основе алгоритма БПФ-ОБПФ

Устройство работает следующим образом. На передающую станцию 1 поступает последовательность двоичных символов. В модуляторе 2 последовательность двоичных

символов разбивают на слова, состоящие из d символов (d=1, 2, ..., D). Каждому слову присваивают модулированный символ данных в виде комплексного числа.

В блоке последовательно-параллельного преобразования 3 преобразуют последовательность модулированных символов данных в параллельные группы модулированных символов.

В блоке установки пилот-сигналов 4 в параллельных группах модулированных символов между модулированными символами данных располагают пилот-символы, формируя таким образом последовательность групп, каждая из которых состоит из N модулированных символов, N=Q+K, где Q – число модулированных символов данных в параллельной группе, K – число пилот-символов в параллельной группе.

В блоке ОБПФ 5 с каждой группой выполняют ОБПФ, формируя параллельные выходные группы значений ОБПФ.

В блоке присоединения защитного интервала 6 дополняют параллельные выходные группы значений ОБПФ защитным интервалом.

В блоке параллельно-последовательного преобразования 7 преобразуют параллельные выходные группы значений ОБПФ с защитным интервалом в последовательную форму, формируя таким образом последовательность ортогональных частотных мультиплексированных символов.

Передают последовательность ортогональных частотномультиплексированных символов с выхода передатчика 8 по каналу связи 9 на принимающую станцию 10.

На принимающей станции 10 через канал связи 9 в приемнике 11 принимают их и в блоке последовательно-параллельного преобразования 12 преобразуют принятые частотно-мультиплексированные символы в параллельные группы входных значений.

В блоке удаления защитного интервала 13 удаляют защитный интервал.

С каждой группой входных значений в блоке БПФ 14 выполняют БПФ, формируя таким образом N модулированных символов в каждом блоке.

В блоке оценки канала 15 в каждой группе по пилот-символам выполняют оценку канала связи. Используя полученные результаты оценки канала связи, выполняют оценку модулированных символов данных, формируя группы оценок модулированных символов данных.

В блоке параллельно-последовательно преобразования 16 преобразуют группы оценок модулированных символов данных в последовательную форму, формируя таким образом последовательность оценок модулированных символов данных.

В демодуляторе 17 выполняют демодуляцию полученных оценок модулированных символов данных, формируя таким образом последовательность двоичных данных, которые с выхода демодулятора 17 поступают на выход принимающего устройства 10.

Найдём импульсную характеристику k-го фильтра, обеспечивающего измерения спектра в точке $z_k = e^{j\left(\frac{2\pi}{N}\right)k}$ [1]. Она равна:

$$h(n) = e^{-j\left(\frac{2\pi}{N}\right)kn}, 0 \le n \le N-1 \quad (1)$$

Для моделирования необходимо использовать аппарат Z-преобразования, которое имеет вид:

$$H(z) = \sum_{n=0}^{N-1} e^{-j\left(\frac{2\pi}{N}\right)kn} z^{-n} = \frac{1-z^{-N}}{1-z^{-1}e^{-j\left(\frac{2\pi}{N}\right)k}} \quad (2)$$

С учетом того, что Z-преобразование и Фурье преобразование взаимосвязаны, перепишем выражение 2 следующим образом:

$$H(e^{j\omega}) = e^{-j\omega\frac{N-1}{2}} e^{j\frac{\pi k}{N}} \frac{\sin\left(\frac{N\omega}{2}\right)}{\sin\left(\frac{\omega}{2}+\frac{\pi k}{N}\right)} = e^{-j\omega\frac{N-1}{2}} e^{j\frac{\pi k}{N}} f_N(\omega,k) \quad (3)$$

Спектр сигнала на выходе блока 14 представлен на рисунке 2.

Метод выполнения анализа при числе отсчетов сигнала L = 2N становится очевидным, если обратиться к направленному графу БПФ. Видно, что выходные отсчеты с четными номерами располагаются в верхней половине графа. Это означает, что в алгоритме БПФ, предназначенном для получения только четных отсчетов спектра, достаточно лишь частично

обработать все L отсчетов, чтобы получить верхнюю половину выходных отсчетов первого этапа БПФ. Только эта половина отсчетов дает все четные коэффициенты ДПФ.

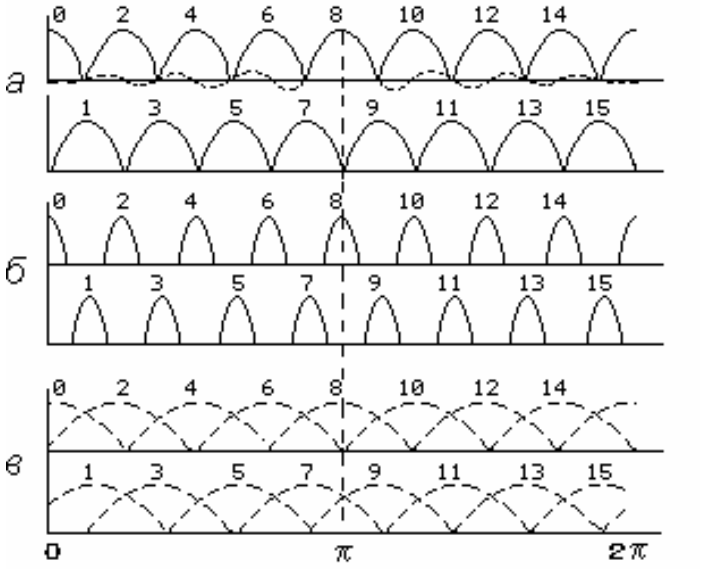


Рисунок 2 – Спектр сигнала на выходе блока 14

Этот подход можно развивать дальше, отметив, например, что восемь верхних выходных коэффициентов дают каждый четвертый коэффициент ДПФ, причем их можно определить, выполнив половину операций на первом этапе, половину – на втором, а также четырехточечное БПФ, полученных на втором этапе восьми отсчетов. Пусть в общем случае число отсчетов сигнала L равно MN, где N – требуемое число спектральных отсчетов, а M – целое число, большее единицы. Искомое преобразование равно:

$$X(k) = \sum_{n=0}^{N-1}[\sum_{m=0}^{M-1} x(n + mN)]e^{-j\left(\frac{2\pi}{N}\right)nk}, k = 0, 1, \dots, N-1 \quad (4)$$

На рисунке 1 в блоке ОБПФ выполняется процедура по следующему алгоритму:

$$x(n) = \sum_{n=0}^{N-1} X(k)W^{kn} \quad (5)$$

Это отображение $x(n) \rightarrow X(k)$ будем считать, как прямое ДПФ. Обратное преобразование $X(k) \rightarrow x(n)$ в случае ОДПФ:

$$X(k) = \sum_{k=0}^{N-1} x(n)W^{-kn}, k = 0, 1, \dots, N-1 \quad (6)$$

Выражение 6 отличается по форме только знаком степени W. Однако различие можно устранить если перейти к комплексно-сопряжённой форме:

$$x^*(n) = \sum_{k=0}^{N-1} X^*(k)W^{-kn}, k = 0, 1, \dots, N-1 \quad (7)$$

В обратном преобразовании (при восстановлении сигнала) для входа и выхода необходимо использовать подстановку:

$$\begin{aligned} x(n) &= \acute{U}^*(n) = \acute{U}(N-n), \\ X^*(k) &= \acute{S}(k), \; k, n = 0, 1, \dots, N-1 \end{aligned} \quad (8)$$

Наибольший выигрыш получается для длины временной последовательности $N = 2^k$, так как в этом случае процесс разбиения на две последовательности удается довести до 2-х точечного преобразования Фурье [2, 16]. При этом на каждом этапе объединения двух БПФ меньшего порядка требуется N/2 операций умножения. Общее количество операций комплексного умножения для вычисления БПФ потребуется:

$$N_{on} = \frac{N}{2} * \log_2 N \quad (9)$$

Теперь обратим внимание, что последовательность отсчетов сигнала на входе алгоритма быстрого преобразования Фурье не соответствует естественному течению времени. Ее следует переупорядочить. Для того, чтобы определить как следует переставить отсчеты воспользуемся двоичным представлением номера входного отсчета. При перестановке младшие и старшие биты номера отсчета меняются местами. В качестве примера рассмотрим перестановку входных отсчетов 8-ми точечного БПФ. Соответствие входных номеров отсчетов сигнала и номеров на входе алгоритма БПФ приведено в таблице 1.

Таблица 1 – Соответствие входных номеров отсчетов сигнала и номеров на входе алгоритма БПФ

Номер	Двоичное представление	Двоично-инверсная перестановка	Десятичное представление
0	000	000	0
1	001	100	4
2	010	010	2
3	011	110	6
4	100	001	1
5	101	101	5
6	110	011	3
7	111	111	7

Следует отметить, что в настоящее время быстрое преобразование Фурье обычно выполняется в сигнальных процессорах, а в них предусмотрен особый вид адресации — двоично-инверсный адрес. При этом старшие и младшие биты адреса меняются местами аппаратно, а реальная перестановка не производится. Это позволяет значительно сокращать время вычисления спектра входного сигнала. Не меньший выигрыш в быстродействии получается за счет применения умножителей-накопителей.

Заключение. Алгоритм БПФ-ОБПФ позволяет выполнять моделирование приемопередающей системы связи с высоким быстродействием и малыми затратами на вычисления, т.к. минимальный выигрыш эффективности обработки сигналов в цифровой системе составляет (после равно логарифм). Однако стоит отметить, что массив данных используется определенный и кратный степени двойки.

Список использованных источников:

1. Методы формирования и цифровой обработки сигналов: Учеб. пособие / Авсянников В.А. БГУИР Минск, 2010, 18 с.

2. Цифровой спектральный анализ: Учеб. пособие / А.Н. Кренёв, Т.К. Артёмова. Яросл. гос. ун-т. Ярославль, 2002. 114 с.

UDC 621.3.049.77–048.24:537.2

MODELING OF THE transceiver TRACT OF THE COMMUNICATION SYSTEM BASED ON THE FFT- IFFT ALGORITHM

Sinitski R.S., student group 760802

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Pechen T.M. – senior lecturer of the Department of ICT

Annotation. Mathematical modeling of the estimation of the spectral characteristics of telecommunications signals based on the fast Fourier transform is performed. It is established that this is a fast and powerful tool, but it needs to use signals of a certain length. Design and technology documentation were developed.

Keywords. transceiver tract, communication system, FFT-IFFT algorithm, spectral analysis, modulator, demodulator

СИСТЕМЫ ГЕТЕРОДИННОГО ПРИЕМА В РАДИО И ОПТИЧЕСКОМ ДИАПАЗОНАХ

Скороходов Р.В., студент гр.067001/магистрант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тарченко Н.В. – канд. технических наук

Аннотация. Тематика работы обусловлена повсеместным использованием волоконно-оптических систем передачи, в том числе и со спектральным уплотнением. При постоянном увеличении пропускной способности волоконно-оптических систем передачи (ВОСП) совершенствуются способы обработки оптического сигнала как в передающем и приемном оборудовании, так и в процессе передачи по оптическому волокну. Совершенствование оптических технологий расширяет возможности алгоритмов обработки сигналов на приемной стороне и требует оценки их эффективности.

Ключевые слова. Когерентный прием, цифровая обработка сигналов, оптическое гетеродинирование.

1 Введение

Многоуровневые форматы модуляции сочетают в себе высокую спектральную эффективность и устойчивость к воздействию дисперсии [1, 2]. Эти достоинства многоуровневых форматов модуляции делают их перспективными при необходимости увеличения скорости передачи в действующих системах связи со спектральным уплотнением. Сочетание когерентного детектирования с цифровой обработкой сигналов позволяет достигнуть еще более высоких значений количества передаваемой информации на один символ [3]. Когерентные оптические системы связи были предложены в 1970-е гг. [4] и в 1980-е начали интенсивно исследоваться, поскольку обеспечивают достижение квантового предела чувствительности приемников [5, 6]. Однако с появлением систем связи со спектральным уплотнением и оптическими усилителями научно-исследовательские работы в этом направлении были прерваны примерно на 20 лет.

После демонстрации в 2005 г. нового поколения приемников – цифровых когерентных приемников – повсеместный интерес к когерентным системам связи вновь возродился. Он обусловлен возможностями реализации в этих системах множества разнообразных многоуровневых форматов модуляции. Кроме того, цифровая обработка сигналов в электронной форме позволяет компенсировать искажения, связанные, например, с хроматической и поляризационно-модовой дисперсией. Существенным недостатком первых когерентных систем связи была их высокая поляризационная чувствительность. Однако проблема была решена благодаря изобретению поляризационной диверсификации (*polarization diversity*) [7]. Более того, современные цифровые когерентные приемники позволяют удвоить скорость передачи информации за счет поляризационного уплотнения информации.

В настоящей работе рассмотрены принципы работы когерентных систем связи и гетеродинного приема, сегодняшний уровень их развития и перспективы.

2 Гетеродинный фотоприём

Структурная схема гетеродинного фотоприёмника изображена на рисунке 1. В его состав входит гетеродин – источник монохроматического оптического излучения с частотой $\nu_г$, близкой к частоте принимаемого сигнала $\nu_с$. Оба сигнала – принимаемый и гетеродинный – одновременно поступают на фотодетектор, тип которого может быть любым, лишь бы время его инерции было меньше периода колебаний разностной частоты $T = \frac{1}{|\nu_г - \nu_с|}$. Роль гетеродина играет лазер [8] с непрерывным излучением высокой спектральной чистоты (монохроматичности).

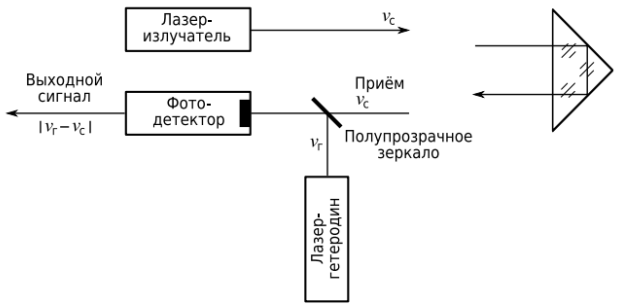


Рисунок 1 – Структурная схема гетеродинного фотоприёмника

В результате интерференции оптических полей гетеродинного и принимаемого сигналов (для чего необходима взаимная параллельность волновых фронтов и одинаковость поляризации обеих волн) на чувствительную площадку фотодетектора воздействует результирующее поле, амплитуда которого изменяется с разностной частотой $|\boldsymbol{\nu}_г - \boldsymbol{\nu}_c|$. В фототоке детектора также возникает составляющая разностной частоты, величина которой, как показывает анализ, определяется формулой:

$$I_P = \frac{e \cdot \eta_{кв}}{h\nu} \sqrt{2 P_г P_c}, \quad (1)$$

где $P_г$ и P_c – соответственно оптическая мощность гетеродина и сигнала;

e – заряд электрона;

h – постоянная Планка;

ν – частота колебаний сигнала или гетеродина (различием между $\boldsymbol{\nu}_г$ и $\boldsymbol{\nu}_c$, в данном случае можно пренебречь ввиду его малости);

$\eta_{кв}$ – квантовый выход фотодетектора.

В случае приёма слабых сигналов $P_г \gg P_c$, и, как видно из формулы (1), за счёт мощности гетеродина происходит как бы усиление сигнала в фотодетекторе. Величина этого усиления пропорциональна $\sqrt{P_г / P_c}$ и может быть весьма значительной. Предельно допустимая мощность гетеродина определяется угрозой перегрузки фотодетектора [8] из-за его нагрева гетеродинным излучением и других причин; типичные значения $P_г$ имеют порядок 10^{-3} Вт. Шумы гетеродинного приёмника при отсутствии фона и флуктуации мощности гетеродина определяются выражением:

$$P_ш = \frac{hc}{\lambda \eta_{кв}} \Delta f, \quad (2)$$

где c – скорость света;

λ – длина волны принимаемого излучения;

Δf – ширина частотного спектра электрического сигнала на выходе ФД (фотодетектора).

Напряжение с частотой $|\boldsymbol{\nu}_г - \boldsymbol{\nu}_c|$, возникающее на сопротивлении нагрузки фотодетектора при протекании по нему тока I_P, представляет собой сигнал промежуточной частоты. Этот сигнал обычно усиливается последующим усилителем промежуточной частоты, подвергается детектированию с помощью радиочастотного детектора (промежуточная частота $|\boldsymbol{\nu}_г - \boldsymbol{\nu}_c|$. обычно имеет порядок $10^7 - 10^9$ Гц, т.е. лежит в радиочастотном диапазоне) и превращается в сигнал переменного тока, форма которого отражает форму огибающей оптического сигнала.

В некоторых случаях частоту гетеродина выбирают равной частоте сигнала. Разностная (промежуточная) частота при этом равна нулю, а в токе фотодетектора непосредственно содержится составляющая, пропорциональная амплитуде, огибающей модулированного оптического сигнала. Такой фотоприёмник называется гомодинным; в нём сохраняются достоинства гетеродинного приёма (усиление сигнала в фотодетекторе за счёт мощности гетеродина и малый собственный шум) и отсутствует надобность в усилителе промежуточной частоты. Гомодинный приём рассматривается как частный случай гетеродинного приёма.

Недостатками гетеродинного приёма являются весьма жёсткие требования к точности совмещения фронтов гетеродинной и сигнальной волн, а также к относительной стабильности

их частот. Во многих практических случаях выполнение этих требований оказывается сложным делом, что требует дополнительных исследований в связи с развитием технологий.

3 Преимущества передачи информации с помощью когерентного приема

Максимальная скорость передачи информации в когерентных системах связи определяется возможностями современных аналого-цифровых преобразователей (АЦП), скорость работы которых достигла 56 Гбод. На их основе удалось увеличить скорость работы цифровых систем обработки сигналов и довести скорость работы когерентных приемников до 28 Гбод.

Когерентные приемники обеспечивают возможность внедрения различных типов многоуровневых форматов модуляции включая фазовые и квадратурные форматы. Наиболее перспективным форматом для скорости передачи информации 100 Гбит/с является формат *DP–QPSK* [9]. В каждом из двух ортогонально поляризованных потоков информация передается с использованием 4–х уровневой фазовой модуляции (*QPSK*). В результате в каждой поляризации передается по 2 бита на символ, всего 4 бит/символ. При символьной скорости 28 Гбод обеспечивается битовая скорость 112 Гбит/с, которая достаточна для передачи информации со скоростью 100 Гбит/с и применения предварительной коррекции ошибок с 12 % избыточностью.

В стандартной сетке *DWDM* (*Dense Wavelength Division Multiplexing* (плотное мультиплексирование с разделением по длине волны.) 50 ГГц системы связи 100 Гбит/с формат модуляции *DP-QPSK* обеспечивают спектральную эффективность 2 бит/Гц. Увеличить спектральную эффективность до 3–х бит/Гц можно при использовании плотной спектральной сетки 33,3 ГГц. Применение сложных алгоритмов многосимвольной обработки (*MAP* (*Maximum a posteriori probability* (оценка апостериорного максимума) или *MLSE* (*Maximum-likelihood sequence estimation* (последовательное оценивание по методу максимального правдоподобия) позволило довести спектральную эффективность до 4–х бит/с/Гц в сетке 25 ГГц/с [9, 10]. Поскольку при использовании сетки 33,3 ГГц не требуется применение сложных алгоритмов многосимвольной обработки (*MAP* или *MLSE*), то *DWDM* системы связи с 100 Гбит/с *DP-QPSK* форматом модуляции и скоростью передачи информации порядка 12–15 Тбит/с могут быть реализованы на основе коммерчески доступных компонент с использованием только *C* диапазона.

Основным доводом в пользу перехода от волоконно-оптической системы передачи (ВОСП) с энергетическим приемом к системам с когерентным приемом является возможность использования различных видов многоуровневой модуляции: амплитудной (АМ), фазовой (ФМ), частотной (ЧМ) и поляризационной, а также их комбинаций, например, квадратурной амплитудной модуляции (КАМ). Отметим, что все известные фотодетекторы дают отклик на поток фотонов и мало чувствительны к оптической фазе и частоте несущей, а также состоянию поляризации [11].

Для определения параметров вектора напряженности электрического поля в модулированной световой волне принимаемого сигнала применяют когерентный прием, основанный на смешении сигнала с когерентным опорным оптическим полем со стабильной фазой от дополнительного источника излучения (гетеродина) и детектирования интерференции двух оптических полей на фоточувствительной площадке ФД. Регистрируемый в результате когерентного приема фототок содержит информацию об амплитуде, частоте и фазе сигнального поля.

По сравнению с энергетическими приемниками прямого детектирования гетеродинные и гомодинные приемники имеют следующие преимущества:

- возможность электронной компенсации хроматической и поляризационно-модовой дисперсии;

- увеличение отношения сигнала к шуму примерно на 3 дБ даже по сравнению с идеальным не шумящим ФП прямого детектирования. Реальный выигрыш от использования когерентного приема значительно больше и может составлять 10–15 дБ;

- малая чувствительность когерентного приема к нежелательному фоновому излучению. При достаточной мощности гетеродина гетеродинный и особенно гомодинный методы приема позволяют достичь квантового предела детектирования.

Недостатком когерентного приема является техническая сложность обеспечения согласования волновых фронтов и поляризаций на поверхности фотодиода принимаемого излучения и излучения гетеродина. В настоящее время для смешивания сигнала и гетеродина используются устройства интегральной оптики. Высокие требования предъявляются к стабильности частот и фаз несущих частот источника излучения и гетеродина.

Когерентные системы связи позволяют реализовывать любые многоуровневые форматы модуляции, обеспечивая увеличение скорости передачи информации в несколько раз в зависимости от емкости формата.

Другое преимущество когерентных систем состоит в сохранении фазовой и поляризационной информации оптического сигнала при преобразовании в электрическую форму. Это позволяет осуществлять постобработку электрических сигналов, включая компенсацию хроматической и поляризационной-модовой дисперсии. Следует особо подчеркнуть, что, благодаря такой обработке сигналов могут быть адаптивно компенсированы также и колебания во времени величины поляризационно-модовой дисперсии.

В настоящее время *Nippon Telegraph and Telephone Corporation* (*NTT*) в сотрудничестве с *Technical University of Denmark, Fujikura Ltd., Hokkaido University, the University of Southampton* и *Coriant GmbH* продемонстрировали возможность создания системы передачи сверхбольших емкостей на несколько сотен километров с усилителями. Они построили экспериментальную систему с пропускной способностью 1 Пбит/с на 32-сердцевинном оптическом волокне, работающую на расстоянии 205,6 км.

Таким образом, был установлен новый мировой рекорд по дальности системы передачи в 1 Пбит/с с использованием оптического усилителя в одном частотном диапазоне *C*.

В качестве дальнейшего улучшения своих результатов исследователи отмечают, что дальность передачи может быть увеличена в будущем до 1000 км. Для этого с целью увеличения помехоустойчивости необходимо уменьшить канальную скорость оптического канала до 510 Гбит/с, тогда потенциал системы позволит увеличить расстояние передачи до тысячи километров.

Объединение когерентного детектирования с цифровой обработкой сигналов предоставляет новые возможности, неосуществимые в отсутствие фазовой информации об электрическом поле оптического сигнала. Поэтому исследователи когерентных систем связи надеются, что возрождение систем когерентной оптической связи уже в ближайшем будущем обеспечит инновационное развитие существующих оптических систем связи [12].

Список использованных источников:

1. Winzer, P.J. Advanced optical modulation formats / R.J. Essiambre – Rimini: Proc. ECOC 2003, 2003. – Vol. 4 – 1002 p.

2. Величко, М.А. Новые форматы модуляции в оптических системах связи / О.Е. Наний, А.А. Сусьян – М.: Lightwave Russian Edition, 2005. – № 4 – 21 с.

3. Kikuchi, K. Coherent transmission system / K. Kikuchi. – ECOC, 2008. – Paper Th2A1.

4. De Lange, O.E. Wideband optical communication systems: Part II'fre' quency division multiplexing / O.E. De Lange – Proc. IEEE, 1970. – Vol. 58. – no. 10 – 1683 p.

5. Okoshi, T. Frequency stabilization of semiconductor lasers for heterodyne'type optical communi' cations systems / K. Kikuchi. – Electron. Lett., 1980. – Vol. 16. – no. 5. – 179 p.

6. Favre, F. High fre' quency stability of laser diode for heterodyne communications systems / D. Le Guen. – Electron. Lett., 1980. – Vol. 16. – no. 18. – 709 p.

7. Derr, F. et al. / F. Derr. – Electron. Lett., 1991. – Vol. 27 – no. 23 – 2177 p.

8. О'Шиа, Д., Лазерная техника / Р. Коллен, У. Родс. – Пер. с англ. М.: «Атомиздат», 1980. – 256 с.

9. Перспективные DWDM системы связи со скоростью 20 Тбит/с на соединение / О.Е. Наний [и др.]. // Фотон-экспресс, 2012. – № 3, С.34–37.

10. Spectrally Efficient Long-Haul Optical Networking Using 112–Gb/s PolarizationMultiplexed 16–QAM. / P.J. Winzer [et al.]; ed.: J. Lightw. Technol., 2010. – V. 28 – P. 547–556.

11. Наний О.Е. Дальность работы и пропускная способность когерентных систем связи / В.Н. Трещиков, Р.Р. Убайдуллаев – М.: Вестник связи, 2013. – № 9 – С.13–19.

12. Сайт о провайдинге и телекоммуникациях nag.ru [Электронный ресурс]. – Режим доступа: http://nag.ru/go/text/32269/. – Дата доступа: 24.02.2021.

MODERNIZATION OF THE LOCAL NETWORK ЛОКАЛЬНОЙ CITY AL-DIWANJA

H. A. Al-Zalzly , Z.H.Myhsen

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Khatskevich O. A .Ph.D, Assoc. Prof.

Modernization of local communication networks in the Republic of Iraq is an extremely important task. The relevance of this work is due to the fact that the ADSL2 + technology used by the population no longer fully satisfies the needs of users both in terms of quality and speed. For this reason, it becomes necessary to introduce a new network, install newer and more reliable equipment, and introduce new technologies. Multiservice networks play a huge role as it is necessary to satisfy the needs of customers in transferring various types of traffic and providing customers with a wide range of services. Meanwhile, data transmission channels suitable for providing one service are not always suitable for providing another. The increase in the volume of services provided forces operators and providers to develop several different networks in parallel. This is costly and often involves significant technical difficulties. The object of implementation was a multiservice local network of one of the districts of the city of Al-Diwaniyah (Iraq). This city is a fairly typical provincial city of Iraq, located in the southern part of the country. The modernization area includes several administrative buildings, a school and a number of residential buildings. The number of apartments in this group of houses is 1728, the expected number of subscribers should be about 50-60%. The projected local multiservice network should provide the ability to provide the following services:

- the interconnection of computers;
- access for users who order this service;
- - broadcasting over a local network - this service works only within the limits of our multiservice network;
- television (iptv) for workstations in the network; - access to file servers.

It has been proposed to use Fast Ethernet and Gigabit Ethernet technologies in the area, which will bring undeniable benefits. The projected multiservice Ethernet network, using a single channel for transmitting data of various types of traffic, allows to reduce the variety of types of equipment, improve the quality and bandwidth of the network, apply uniform standards and a single cabling system, and centrally manage the communication environment to provide the most complete range of services. The above possibilities allow to reduce the cost of designing and implementing a network, simplifies technical implementation, and also allows taking into account the needs of a modern user. The above possibilities allow reducing the cost of designing and implementing a network, simplifying technical implementation, and also allowing to take into account the needs of a modern user. Zyxel switches were chosen as SPD equipment, which made it possible to organize a secure and high-speed transfer. Zyxel switches were chosen as SPD equipment, which made it possible to organize safe and high-speed data transmission within the network, as well as to make reservation of connections at the core and distribution levels. The use of this equipment provided ample opportunities for monitoring, diagnostics, management of various network nodes, as well as automatic signaling in case of any problems in the network. transfer of data within the network, as well as perform reservation of connections at the core and distribution levels. The use of this equipment provided ample opportunities for monitoring, diagnostics, management of various network nodes, as well as automatic signaling in case of any problems in the network.

In conclusion, we can say that the proposed project of a multiservice Ethernet network in the Al Diwaniyah microdistrict will provide users of this network with high-quality, high-speed Internet access, as well as access to a huge volume of media content within the local network.

PROTECTION OF INFORMATION ON THE COMMUNICATION MULTISERVICE NETWORK OF THE LOGISTIC CENTER

Z. H. Myhsen, H. A. Al-Zalzly

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Khatskevich O. A .Ph.D, Assoc. Prof.

For the effective operation of corporate communication networks of logistics centers, it is necessary to have modern protection of programs, databases and information transmission facilities. A typical logistics center in the city of Al-Diwaniya, with branches in Baghdad, Basra and Kirkuk, was selected as the object of the study. The research subjects of this work are the principles of organization, operation and ways to improve the efficiency of a corporate multiservice c The corporate network of the logistic center is a complex multi-profile structure with a hierarchical management system. Therefore, when developing a project for system integration, it is important to properly design a network, from the reliable and correct operation of which will depend subsequently the steady operation of the entire banking data network.

The projected network should ensure the exchange of data between the structural divisions of the center, its branches and external organizations, the use of electronic mail. Connection to the Internet at workplaces of all users, the possibility of using an internal information portal.

Communication network based on FTTx technology. Scientific novelty lies in the creation of a multiservice network with the possibility of applying the proposed solutions to existing communication networks. The model proposed in the work allows one to calculate the characteristics of the quality of service, to assess the effectiveness of the use of FTTx technology in multiservice communication networks. The practical value lies in the possibility of creating a corporate multiservice communication network with minimization of costs for organization and technical operation, rational use of space and at the same time providing the necessary level of quality characteristics, in particular, reliability indicators.

Simulation modeling of the modernized communication network was carried out using the Riverbed Modeler software product, which is a set of tools for creating, modeling and studying communication networks. Allows you to analyze the impact of client-server applications and new technologies on the network; to model hierarchical networks, multi-protocol local and global networks, taking into account routing algorithms; evaluate and analyze the performance of simulated networks. Also, using the package, you can check the communication protocol, analyze the protocol interactions, optimize and plan the network. Riverbed Modeler contains a comprehensive library of protocols and objects..

A result of the simulation, telecommunication and server equipment from Cisco and Dell, respectively, was selected. Based on the data on the parameters of the transmitted traffic and the network topology, the main characteristics were calculated. Taking into account the selected equipment, the used broadband access technology and the values of the parameters obtained as a result of the calculations, a virtual model of a multiservice communication network was developed. The proposed communication network model meets all technical requirements and allows to fully solve the assigned tasks.

For secure connection of geographically dispersed offices appropriate to use technology VPN MPLS. From other technologies building virtual private networks, such as VPNs, ATM or Frame Relay, VPN MPLS technology distinguishes good scalability, the ability to automatically configure and natural integration with other IP services, including Internet access, Web and e-mail services.

MPLS VPN functionality can be summarized as follows:

-MPLS allows a single converged network to support both new and existing facilities, creating an efficient migration path to IP infrastructure.

-MPLS operates over existing systems and transmission networks (ATM, Frame Relay, X. 25, IEEE 802.3, etc).

-MPLS allows you to generate traffic. Routing data packets are carried out through the application of technology of processing labels.

-MPLS supports the provision of services with a guaranteed quality of service (QoS). Packages that need to be delivered with high quality, can be marked, allowing service providers to provide certain small latency for voice and video signals in end-to-end connection.

-MPLS provides appropriate security level to make IP network the same safe as frame relay network in WAN, reducing the need for encryption in IP networks.

When sending confidential information, it is important to ensure a high level of reliability of encryption. The most famous representative of the Organization's encryption technology of protective channel in VPNs is the technology of Internet Protocol Security (IPSec-protected IP).

The main purpose of the IPSec service is to ensure safe PD over IP networks using any link-layer technology (PPP, Ethernet, ATM, etc.). Use Internet Protocol security (IPSec) ensures integrity, authenticity and confidentiality of the data; its membership now includes almost 20 proposals for standards and RFC 18.

IPSec in the following techniques:

-encryption of the original IP packet that provides secrecy of data contained in the package, such as a field in the IP header and the data field;

digital signature IP packets that provides authentication package and source-the sender of the package;

-encapsulate the IP packet in a new secure IP packet with a new header that contains the IP address of the device that disguises the internal network topology.

Thus, the use of VPN MPLS based Ethernet networks with data encryption protocol , IPSEC allows you to design a modern corporate network and create Foundation for further modeling network, whose goal is to further optimization.

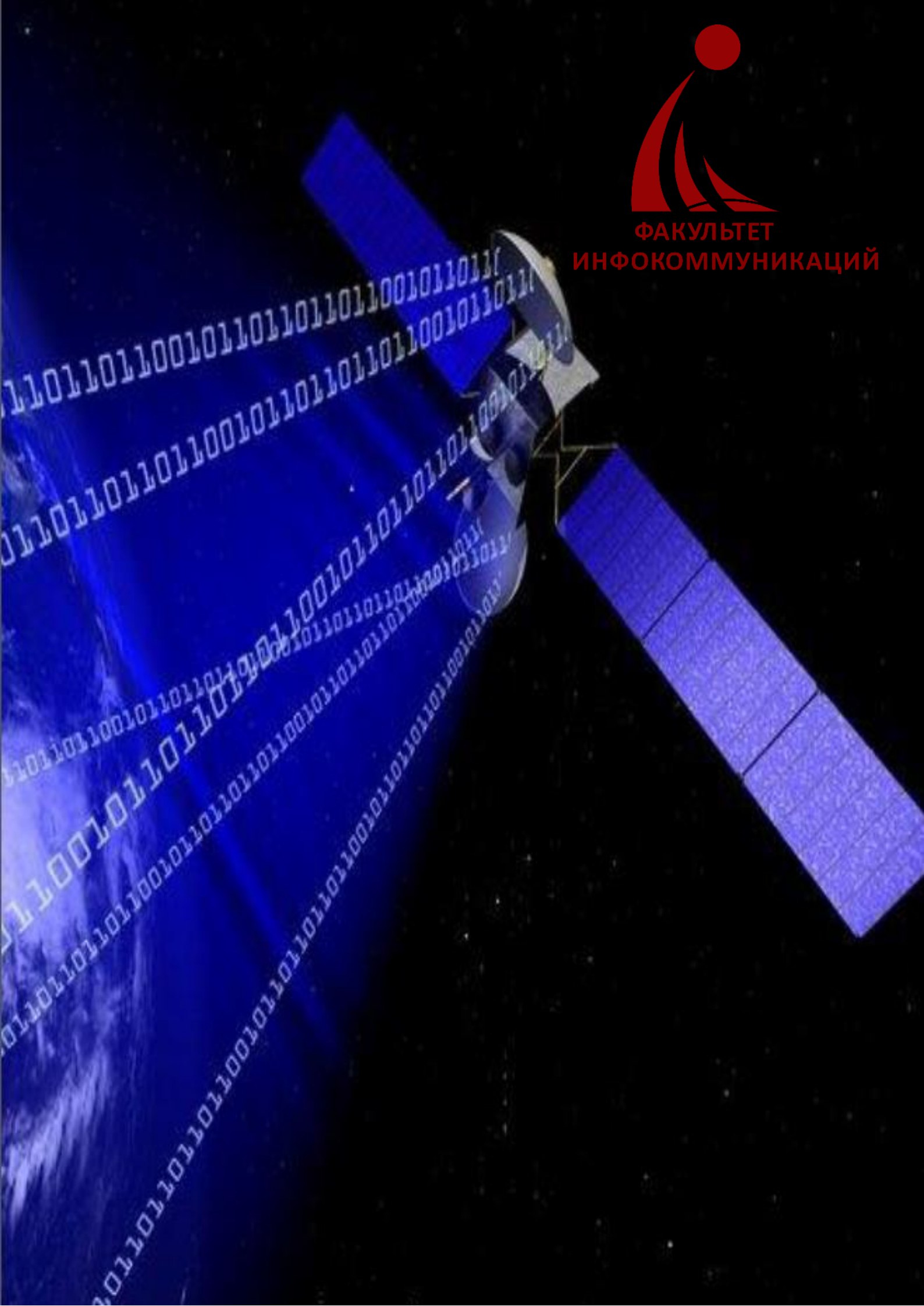
Based on the results of this study clearly visible steps of designing a modern corporate network connection. Applying the information, you can create and optimize the performance of existing networks, disabling network efficiency and reliability to a whole new level.

According to the comparative analysis of the simulation results, it can be said that the proposed model of the modernized multiservice communication network of the logistics center meets all the parameters formulated in the terms of reference. This configuration of the data transmission network provides a high level of performance, flexibility, and also makes it possible to expand it in the future.

ИНФОКОММУНИКАЦИИ

Сборник материалов 57-ой научной конференции аспирантов, магистрантов и студентов

Ответственный за выпуск *Т.М. Печень*


ФАКУЛЬТЕТ
ИНФОКОММУНИКАЦИЙ