9 785768 109936

ИНФОКОММУНИКАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СОСТОЯНИЕ, ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Материалы I Всероссийской научно-практической конференции

25–26 апреля 2014 г.

Курск 2014

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Юго-Западный государственный университет»
(ЮЗГУ)

ИНФОКОММУНИКАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СОСТОЯНИЕ, ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Материалы I Всероссийской
научно-практической конференции

25-26 апреля 2014 г.

Курск 2014

УДК 621.39(063)
ББК 32.968я431
И 74

Рецензент
Доктор технических наук, профессор
НИЦ (г.Курск) 18 ЦНИИ МО РФ *В.Н. Николаев*

И 74 **Инфокоммуникации и информационная безопасность: состояние, проблемы и пути решения**: материалы I Всероссийской науч.-практ. конф. / редкол.: А.М. Потапенко (отв.ред) [и др.]; Юго-Зап. гос. ун-т. – Курск, 2014. – 388 с.

ISBN 978-5-7681-0993-6

Материалы конференции посвящены исследованию современных проблем в области инфокоммуникаций и информационной безопасности.

Материалы конференции предназначены для широкого круга исследователей, занимающихся как телекоммуникационными технологиями, так и обработкой информации в территориально-распределённых системах сбора, обработки и доведения информации, защитой информации в системах и при передаче. Материалы представляют несомненный интерес для аспирантов технических специальностей и студентов направлений подготовки «Телекоммуникации», «Защита информации».

УДК 621.39(063)
ББК 32.968я431

ISBN 978-5-7681-0993-6

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Сборник содержит материалы I Всероссийской научно-практической конференции «Инфокоммуникации и информационная безопасность: состояние, проблемы и пути решения», целью которой является ознакомление с работами, посвящёнными вопросам создания и развития инфотелекоммуникационных сетей, защите информации.

Материалы конференции посвящены вопросам использования результатов космической деятельности в целях развития региона, информационных систем обеспечения функциональной деятельности отраслевых объектов, систем кодирования и защитыинформации. Рассмотрены вопросы моделирования устройств приёма, обработки и формирования сигналов в программной среде GNURADIO, возможности применения и распространения этого программного продукта, представления методов модуляции в системах связи в программной среде MATLAB+SIMULINK. Предложены основные направления использования результатов космической деятельности в целях развития региона, варианты построения сети города, рассмотрены основные радиотелекоммуникационные системы, системы защиты информации.

Материалы конференции предназначены для широкого круга исследователей, занимающихся как телекоммуникационными технологиями, так и обработкой информации в территориально-распределённых системах сбора, обработки и доведения информации.

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 621.395.4

Е.А. Шиленков, С.С. Хотынюк

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ЛИНЕЙНЫЙ ПРЕДИКТОР В ОРТОГОНАЛЬНОМ РЕЧЕВОМ КОДЕРЕ

На основе особенностей произношения и фонетического восприятия русской речи (непроизношения гласных звуков в безударных слогах) предложен способ сжатия цифрового речевого потока путём внедрения линейного предиктора в процесс ортогонального кодирования.

Русская речь отличается от остальных множеством динамических параметров, в том числе частотным диапазоном и временным слуховым восприятием. Особенно наглядно последнее объясняется фонетической транскрипцией русских слов.

Запись устной речи в полном соответствии с её звучанием не может быть осуществлена обычным орфографическим написанием. При орфографическом письме отсутствует полное соответствие между звуками и буквами, в графике отсутствуют знаки, необходимые для записи всех звуков устной речи. Так, например, редуцированные гласные в безударных слогах непроизносимы, а значит, неслышимы [1].

Учитывая данную особенность русской речи, можно предположить возможность внедрения в стандартизированные речевые кодеры устройства, обеспечивающего более плотное сжатие без серьёзных осложнений разборчивости.

Ввиду акустических особенностей слуха человека в целом в речевом кодировании (сжатии) получили широкое распространение вокодеры с адаптивным речевым предсказанием. Их главная отличительная особенность – автокорреляционный анализ ансамбля предыдущих дискретных отсчетов сигнала с текущим с целью предсказания последующих. Результатом вычисления являются дифференциальные значения, которые содержат кодовую последовательность с меньшей разрядностью. Обобщенная структурная схема кодера с линейным предиктором изображена на рисунке 1.

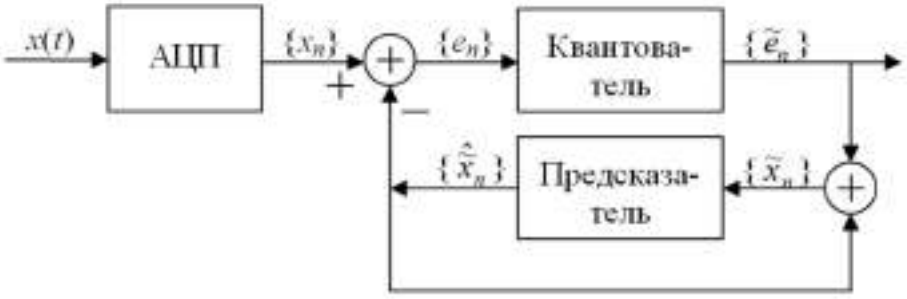


Рис. 1. Структура дифференциального кодера с обратной связью

В представленной схеме процесс предсказания реализован в цепи обратной связи, охватывающей устройство квантования (квантователь). Входной сигнал в формате ИКМ (PCM) для предсказателя обозначен $\tilde{x}_n$. Он представляет собой сигнальный отсчет x_n, дифференцированный в результате вычисления сигнала ошибки в квантователе.

Математическое выражение для выходного дифференцированного сигнала представленного адаптивного кодера, в котором последующее входное значение сравнивается только с одним предыдущим, представлено в формуле [2]

$$\hat{\tilde{x}}_n = \sum_{k=1}^{M} a_k \cdot \tilde{x}_{n-k} \ . \qquad (1)$$

Показанная на схеме (см. рис. 1) разность $e_n = x_n - \hat{\tilde{x}}_n$ является входным сигналом квантователя, далее по схеме сигнал $\tilde{e}_n$ обозначает его выход. Сжатие реализуется путём кодирования выходного сигнала ошибки предсказания $\tilde{e}_n$ последовательностью двоичных символов с меньшей разрядностью квантования, что и является результатом работы всего кодера. Полученная ошибка $\tilde{e}_n$ также суммируется с предсказанной величиной $\hat{\tilde{x}}_n$ с целью получения $\tilde{x}_n$.

Основной же идеей применения ортогонального звукового кодирования является использование неидеальности слуха человека в частотном диапазоне. Основанием для построения подобных кодеров стала психоакустическая модель звукового восприятия, по структуре которой происходит построение маски в кодере для «неслышимой» информативной составляющей.

На рисунках 2 и 3 изображены результаты эксперимента по определению границ маскирования для частотной области реального речевого сигнала помехой с частотой 1 КГц.

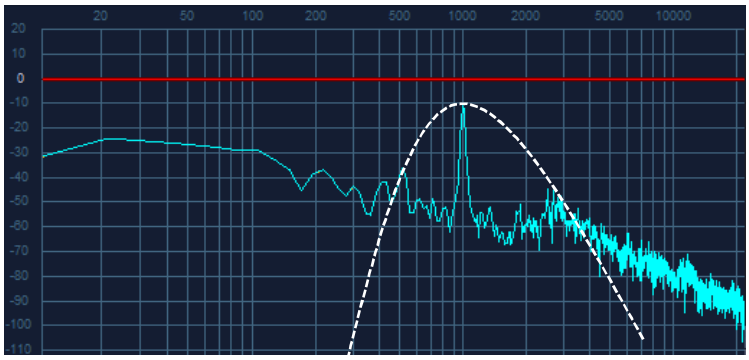


Рис. 2. Частотная маска для реального речевого сигнала: — – максимум для неискаженного сигнала; — – результат быстрого преобразования Фурье; – – граница частотного маскирования

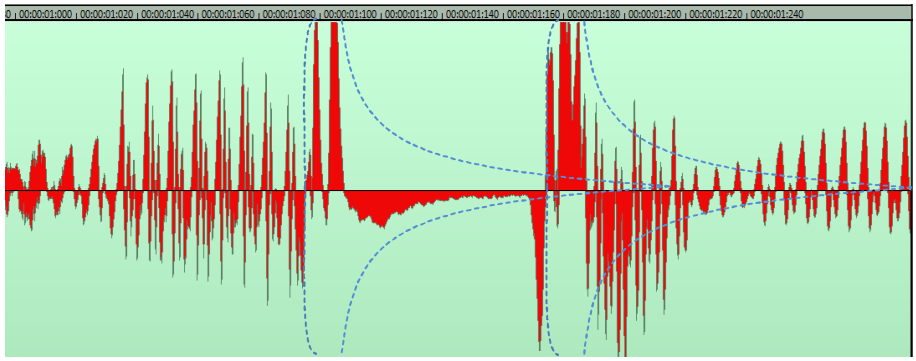


Рис. 3. Временная маска для реального речевого сигнала: — – дискретные временные значения в формате PCM; – – граница временного маскирования

Функция психоакустической модели, отображающая порог частотного маскирования (выделенная белым пунктиром на рис. 2), определяется по формуле [2,4]

$$SF_{дБ}(x) = 15{,}81 + 7{,}5 \times (x + 0{,}474) - 17{,}5 \times \sqrt{1 + (x + 0{,}474)^2}\ . \quad (2)$$

Аппроксимированные пороговые значения для временной области, показанные на рисунке 3 синими пунктирами, были вычислены с помощью двойной округло-экспоненциальной функции Плака–Мура [1]. Пороговые значения для симметричных и асимметричных входных сигналов установлены одновременно сверху и снизу. Каждая сторона временного окна (W) определяется по следующей формуле [5,6]:

$$W(t) = (1-\omega)\left(1+\frac{2t}{Tp}\right)\exp\left(-\frac{2t}{Tp}\right) + \omega\left(1+\frac{2t}{Ts}\right)\exp\left(-\frac{2t}{Ts}\right), \quad (3)$$

где Tp – постоянная времени, связанная с нарастающим к пику действующим значением амплитуды дискретного сигнала; Ts – по-

стоянная времени, связанная с окончанием (спадом) маски; ω – точка перехода между пиковыми и конечными частями функции.

В обоих случаях, для временного и частотного маскирования, сжатие исходного сигнала происходит путём удаления дискрет, находящихся ниже порога маскирования.

В развитие известных техник ортогонального речевого кодирования, представленных группой MPEG [2,3,4,5], автором предложен вариант интеграции функции линейного предсказания в структуру модифицированного кодера MP3. По своей сути главной отличительной чертой ортогональных кодеров от линейных является преобразование «время-частота». Сжатие потока в MPEG достигается путём определения факторов маскирования в частотной области, удаления низких по амплитуде частотных коэффициентов и переквантования оставшихся кодом с меньшей длиной [4].

Основная идея более плотного сжатия заключается в преобразовании (переквантовании, удалении) частей временного потока перед ортогональным преобразованием за счет внедрения блока линейного предиктора в процесс полифазной линейной фильтрации.

Модифицируемая область ортогонального кодера представлена на рисунке 4.

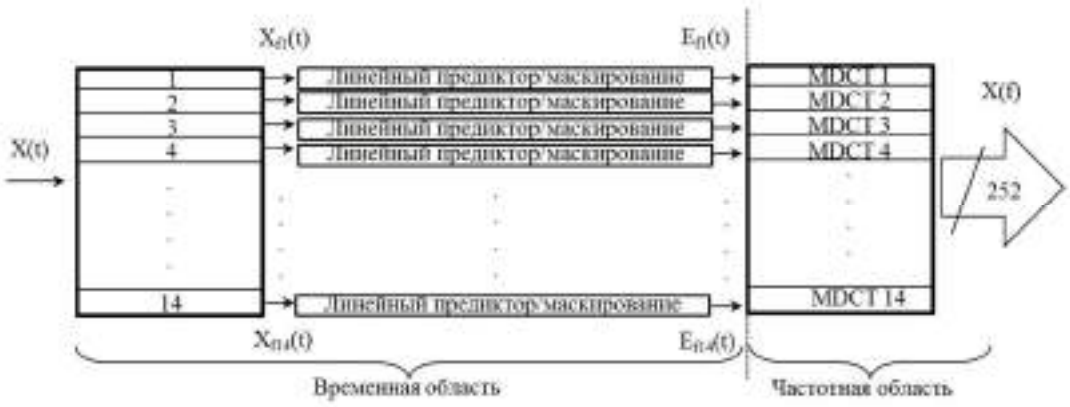


Рис. 4. Линейный предиктор в структуре ортогонального кодера

На вход кодера приходит сигнал X(t) в формате ИКМ (PCM). Далее происходит разделение на 14 критических полос $X_1(t)$ – $X_{14}(t)$ при помощи полифазного КИХ-фильтра. Каждый временной поток попадает в блок «Линейный предиктор», в котором осуществляется процедура наложения временной маски. Результатом является параллельный выходной поток $E_1(t)$ – $E_{14}(t)$, который сле-

дом подвергается частотному кодированию посредством модифицированного косинусного преобразования (MDCT)[6,7].

Реальный ортогональный кодер работает в цифровых устройствах кодирования/квантования, работа которых трудно объяснима математическими выражениями в декартовой системе счисления. Ввиду трудности представления принципа работы предиктора в виде математической модели как вариант способа отображения его работы предложен функциональный алгоритм (рис. 5).

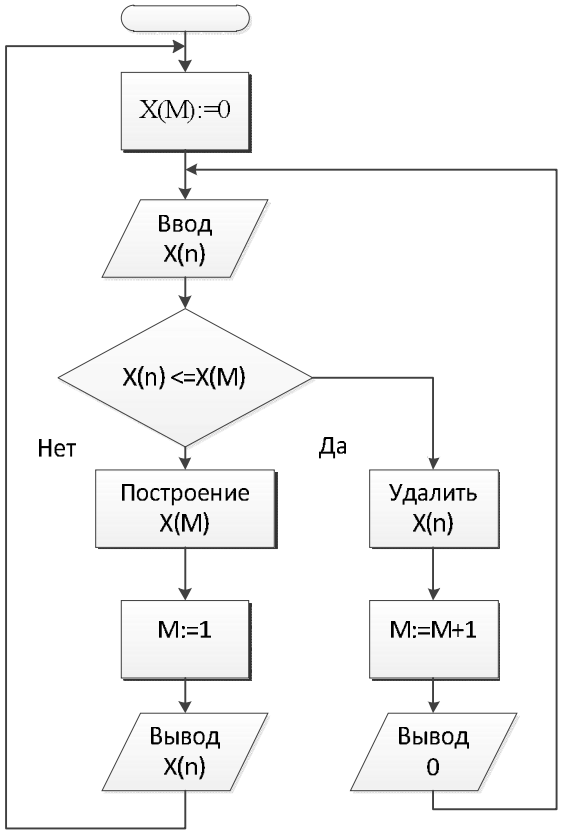


Рис. 5. Алгоритм работы блока «Линейный предиктор/маскирование»: X(n) – входной сигнал от полифазного фильтра; X(M) – построенная временная маска; n – номер временного отсчета входного сигнала; M – номер временного отсчета маски

Пришедший на вход устройства отсчет сравнивается уровнем маски, построенной ранее. В случае, если он оказывается меньшим, на выходе формируется нулевое значение, в обратном случае происходит перестройка маски соответственно новому пиковому значению и на вывод X(n) попадает в неизменном виде. Длина маски увеличивается прямо пропорционально увеличению количества

уровней квантования (уменьшения шума квантования) и вычисляется по формуле (3).

Изменение длины маски в зависимости от частоты дискретизации и разрядности показано в таблице.

Соответствия количества отсчетов временной маски

Разрядность кода	Максимальное затухание, дБ	Максимальная длина, мс	Количество М		
			8КГц	22,05КГц	44,1КГц
8 бит	24	40	320	882	1764
12 бит	36	60	480	1323	2646
16 бит	48	100	800	2205	4410
24 бит	72	>160	1280	3308	6615

В результате вычислений блока «Линейный предиктор/маскирование» на вход преобразователя «время-частота» подаётся поток данных с удалёнными в результате маскирования временными отсчетами. Данный процесс проиллюстрирован на рисунке 6.

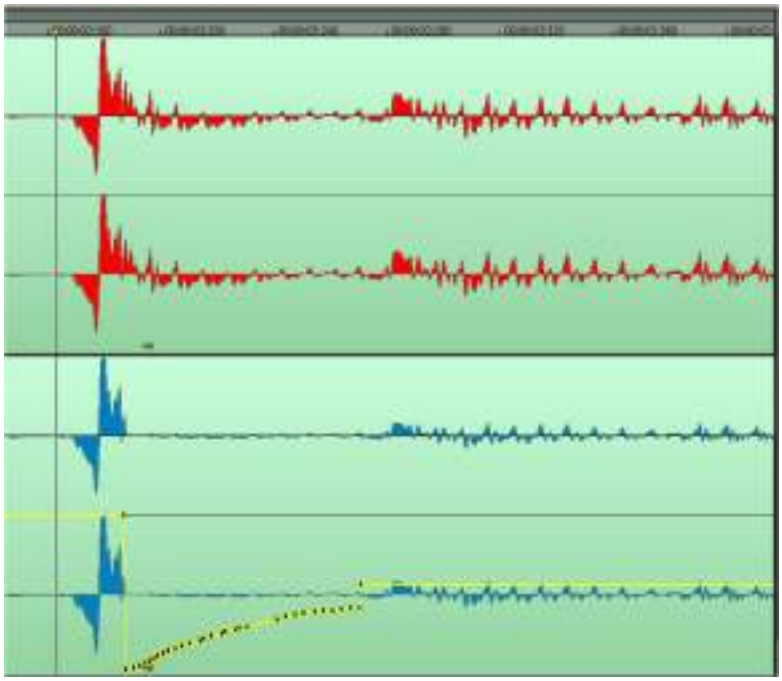


Рис. 6. Иллюстрация работы блока «Линейный предиктор/маскирование»:
— входной PCM сигнал; — наложенная функция временной маски;
— выходной сигнал

При частоте дискретизации речевого сигнала 8 КГц и разрядности кода 8 бит количество удалённых отсчетов в представлен-

ном результате эксперимента ориентировочно составит 640, количество маскированной (непередаваемой) информации будет равно 640 x 8 = 5120 бит. Соответственно, при дальнейшем ортогональном кодировании путём использования модифицированного дискретного косинусного преобразования частотные коэффициенты также будут нулевыми на всём удалённом участке.

Стоит отметить следующее: разборчивость речи при таком перераспределении временного потока остаётся на приемлемом уровне, что подтверждено экспериментально; данный подход не целесообразно применять для сжатия музыкальных либо иных звуковых сигналов.

Комплекс предложенных процедур позволяет увеличить степень плотности сжатия речевого сигнала, однако остаётся открытым вопрос о реальной скорости битрейта. Данный расчет может быть аппроксимирован при помощи результатов углубленного фонетического анализа наиболее употребляемых слов словосочетаний в русском языке.

Список литературы

1. Валгина Н.С., Розенталь Д.Э., Фомина М.И. Современный русский язык: учебник / под ред. Н.С. Валгиной. – 6-е изд., перераб. и доп. – М.: Логос, 2002. – 528 с.

2. Spiegel M.F., Schroeder M. Simultaneous and nonsimultaneous masking within natural speech // The Journal of the Acoustical Society of America. – New York, 1979. – P. 66.

3. Bernstein L.R., Trahiotis C. The effects of signal duration on NoSo and NoSpi thresholds at 500 Hz and 4 kHz // The Journal of the Acoustical Society of America. – New York, 1999. – P. 105.

4. Zwicker E. Subdivision of the Audible Frequency Range into Critical Bands (Frequenzgruppen) // The Journal of the Acoustical Society of America. – New York, 1961. – P. 33, 248.

5. Terhardt E. On the perception of periodic sound fluctuations (roughness) // Hearing Research. – 1979. – № 1. – P. 155.

6. Yang X., Waxman C.MP3 Coding Scheme. – Philadelphia : University of Pennsylvania, 2012. – 18 p.

7. Guckert J. The use of FFT and MDCT in MP3 audio compression // Math. – 2012. – №2270. – P. 6-8.

8. ISO/IEC 11172-3. Stage: 90.60 (2010-06-17). Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s – Part 3: Audio.

СЕКЦИЯ 1
СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕКОММУНИКАЦИЙ

УДК 621.395.4

Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА ДЕСКРИПТОРА LZSSTACKER

Представлена алгоритмическая последовательность дескрипции формата архиватора Stacker с динамическим окном.

Структура протокола IPComp представляет особый интерес для поиска сжатых данных в общем потоке по его уникальному полю заголовка. Протокол IPComp является разновидностью протоколов IP канального уровня. Рассмотрим структуру заголовка сжатого потока: архивные данные инкапсулируются путем изменения заголовка IP и вставки заголовка IPComp, после которого непосредственно следует сжатый поток. Определим различия модификаций заголовков IP в IPv4 и IPv6 и структуры заголовка IPComp.

Установка полей заголовка IPv4 для передачи сжатого потока:

1. Общая длина: длина всего инкапсулированного потока, в том числе заголовок IP, заголовок IPComp и сжатый поток.

2. Протокол: поле протокола установлено в значение 108, выделенное для данных IPComp.

3. Контрольная сумма заголовка: контрольная сумма интернет-заголовка в заголовке IP. Все остальные поля заголовка IPv4 сохраняются неизменными, в том числе и любые другие заголовки.

Установка полей заголовка IPv6 для передачи сжатого потока:

1. Длина сжатого потока.
2. Next Header установлен в 108 для данных IPComp.
3. Все остальные поля заголовка IPv6 сохраняются неизменными, в том числе и любые несжатые варианты заголовков.

Заголовок IPComp помещается в пакет IPv6, используя те же правила, что и фрагмент IPv6 заголовка. Однако, если пакет IPv6 содержит как фрагмент IPv6 заголовка, так и заголовок IPComp, то фрагмент IPv6 заголовка должен предшествовать заголовку IPComp в пакете.

Четырёхбайтный заголовок IPComp (рис.) имеет следующую структуру: Next Header – восьмибитный селектор; сохраняет данное поле протокола IPv4 или IPv6 от оригинального заголовка IP; установлен в значение 108 для данных IPComp; флаги – восьмибитное поле. Зарезервировано для будущего использования. Должно быть установлено в ноль. Должно быть проигнорировано принимающим узлом;индекс параметра сжатия (CPI) – 16-битный индекс. Индекс CPI сохраняется в сетевом порядке.

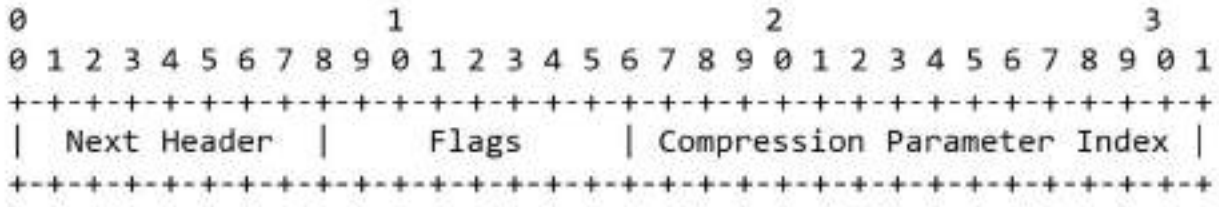


Рис. Четырёхбитный заголовок IPcomp

Значения 0-63 обозначают *хорошо известные* алгоритмы сжатия, которые не требую дополнительного рассмотрения. Значения идентичны идентификаторам IPCOMP Transform и определены в [SECDOI]. Значения 64-255 зарезервированы для использования в будущем. Значения 256-61439 согласовываются между двумя приватными узлами по их собственным конфиденциальным алгоритмам сжатия.

Первые 4 алгоритма сжатия для IPComp [RFC 2407]

Transform ID	Value
RESERVED	0
IPCOMP_OUI	1
IPCOMP_DEFLATE	2
IPCOMP_LZS	3

Алгоритм архивирования StackLZS представлен подробно в описании ANSIX3.241-1994. Сжатие LZS и декомпрессия используют алгоритм типа LZ77. Последние два килобайта несжатых данных являются словарём с изменяющимся скользящим окном. Компрессор LZS ищет соответствия между данными, которые будут сжаты, и предшествующими 2 Кб данных. Если он находит совпадение, то оно кодируется сочетанием *Смещение/Длина* для

поиска совпадения в словаре. Если совпадений не найдено, следующий байт данных кодируется как «литерал» – исходный байт. Сжатый поток данных заканчивается *маркером окончания*.

Данные кодируются в поток переменной длины. Литерал кодируется как бит «0», за которым следуют 8 битов *исходного байта*.

Смещение/Длина кодируются как бит «1», далее идет код смещения, а затем код длины. В конце устанавливается исключительный код – *Маркер окончания*.

Смещение может иметь минимальное значение 1, максимальное – 2047. Значение 1 указывает на самый последний байт в буфере истории, текущий байт данных есть начало повтора. Смещение кодируется как:

– если смещение меньше 128: бит «1» предшествует 7-битному значению смещения;

– если смещение больше или равно 128: бит «0» предшествует значению смещения с 11-битной длиной.

Маркер окончания кодируется как 9-битный маркер 110000000. После конечного маркера по мере необходимости нулевые биты в количестве от 0 до 7 дополняют поток до границы байта.

Транскрипция сжатого потока данных:

<*Сжатый поток*>:= [<*Сжатая строка*>] <*Маркер окончания*>
<*Сжатая строка*>:= 0 <*Исходный байт*> | 1 <*Сжатый байт*>
<*Исходный байт*>:= <b><b><b><b><b><b><b><b> (8-bitbyte)
<*Сжатый байт*>:= <*Смещение*><*Длина*>
<*Смещение* >:= 1 <b><b><b><b><b><b><b> | (7-bit смещ.)
0 <b><b><b><b><b><b><b><b><b><b><b>(11-bit)

<*Маркер окончания*>:= 110000000
<b>:= 1 | 0
<*Длина*>:=

00	= 2	1111 0110	= 14
01	= 3	1111 0111	= 15
10	= 4	1111 1000	= 16
1100	= 5	1111 1001	= 17
1101	= 6	1111 1010	= 18
1110	= 7	1111 1011	= 19

1111 0000 = 8 1111 1100 = 20
1111 0001 = 9 1111 1101 = 21
1111 0010 = 10 1111 1110 = 22
1111 0011 = 11 1111 1111 0000 = 23
1111 0100 = 12 1111 1111 0001 = 24
1111 0101 = 13 ...

Методика нахождения и дескриптора для LZS:

1. Искать четырёхбайтный заголовок: первый байт – 108dec, второй – 00hex, третий и четвертый вариативные, для определения заголовка IPComp.

2. Искать слово (WORD) по каждому из вариантов:

№	1 байт	2 байт
1	11000000	00000000
2	X1100000	00000000
3	XX110000	00000000
4	XXX11000	00000000
5	XXXX1100	00000000
6	XXXXX110	00000000
7	XXXXXX11	00000000
8	XXXXXXX1	10000000

где X – любой возможный бит для поиска *Маркера окончания*.

3. Читать следующий бит текущего байта сжатого потока:

а) если бит равен 0, то это несжатая строка, вставить в результат следующие восемь бит, это *Исходный байт*;

б) если бит равен 1, провести проверку на код 110000000 (если да, то завершить процесс – это *Маркер окончания)*, в противном случае это сжатая строка, читать *Смещение*/*Длина*.

4. Читать первый бит *Смещения:*

а) если первый бит смещения равен 0, то размер смещения 7 бит. Читать 7 бит, перевести результат в декартовое счисление;

б) если первый бит смещения равен 1, то размер смещения 11 бит. Читать 11 бит, перевести результат в декартовое счисление.

5. Читать первый бит *Длины*. Определить полный код длины лексикографически (см. транскрипцию). Перевести результат в декартовое счисление.

6. Отсчитать *Смещение* побайтно от конца словаря, копировать число найденных ранее байт согласно *Длине*. Вставить в конец. Перейти к пункту 3.

---

1. Geraldine C. Data Compression Method – Adaptive Coding with Sliding Window for Information Interchange. – NY., 2004.

УДК 621.395.4

Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА ПОИСКА СЖАТЫХ БЛОКОВ В ПОТОЧНЫХ ДАННЫХ

Представлена последовательность нахождения сжатой информации в потоке данных и структурные признаки отделения служебных байтов.

Для поиска сжатой информации внутри структуры длинного архивного файла или потока необходимо выделять служебные байты и непосредственно блок (в некоторых источниках - словарь). Каждый архиватор добавляет в начало и конец сжатого файла собственные заголовки и окончания. В случае, если размер сжатого файла больше, чем допустимый словарь, блоки разделяются. Так, например, максимальный размер блока в ZIP (Deflate) равен 32 Кбайт. В общем виде структуру архива можно представить так:

заголовок	блок 1 (32Кб)	разделитель	блок 2 (32Кб)	…	окончание

В заголовке обычно указывают: версию архиватора, название файла или директории, количество блоков, тип разделителя, размер исходных и сжатых данных; в окончании присутствует контрольная сумма и т.д.

Пример отделения служебной информации от блока приведен на рисунке 1.

Исходя из представленной структуры, целесообразно обосновать способ выделения заголовков, окончаний и разделителей. Заголовок уникален для каждого нового архива и размер его вариативен, то же и у окончания. Но разделитель, как правило, остается постоянным и часто содержится в заголовке.

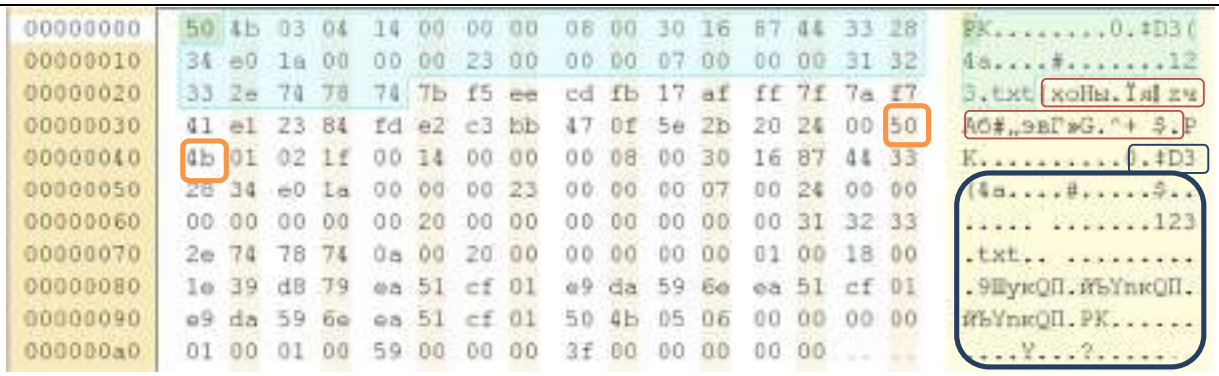


Рис. 1. Структура архива ZIP версии 6.3: красным показан сжатый блок, остальное – служебная информация

Главным отличием анализа поточных данных является неопределённость точки входа в архив, т.е. для нахождения служебных байтов необходимо накопить количество информации из потока, равное большему размеру, чем один блок. В данном случае поиск блока возможен по разделителю. Часто в качестве него выступает заголовок канального уровня (рис. 2).

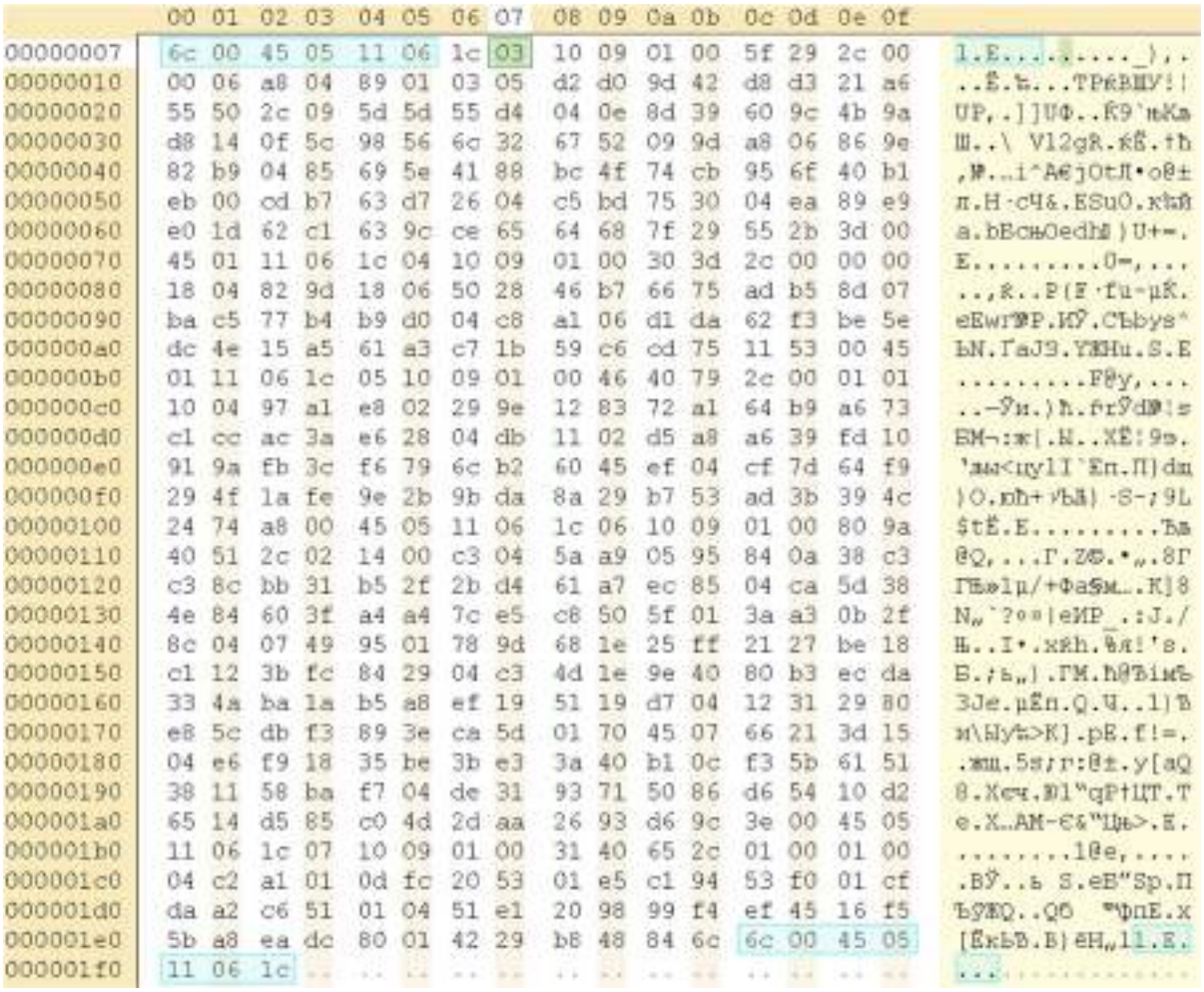


Рис. 2. Сжатый поток с выделенным заголовком

Таким образом, методика нахождения разделителя блоков может быть следующей:

1. Провести поиск повторяющихся конструкций байтов (от 3-х и более подряд).

2. Выстроить найденные конструкции в порядке убывания размера и указать частоту повторений в файле.

3. Проанализировать количество информации, заключенной между первым найденным повтором. В случае, если оно меньше или равно 32 Кб, сделать вывод о нахождении разделителя. В противном случае провести анализ для меньшей байтовой конструкции.

4. Результатом поиска может явиться как первая конструкция, удовлетворяющая условию максимального размера блока, так и последующие.

5. Для окончательного нахождения разделителя необходимо проанализировать первый байт сжатого блока.

---

1. PKWARE, Inc. ZIP File Format Specification. – URL: http: www.pkware.com/documents/casestudies/APPNOTE.TXT.

УДК 621.396.96

В.В. Беляков, С.С. Хотынюк

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ИСПОЛЬЗОВАНИЯ СПЕКТРА РАДИОЭФИРА

Рассмотрена методика осуществления контроля радиочастотного спектра, осуществляемого с целью слежения за выполнением распределения частот для нужд различных служб.

В связи с высокой загруженностью электромагнитного поля эффективность использования радиоэфира становится всё более проблематичной. Для повышения стабильности работы сетей прибегают к контролю использования спектра. Контроль использования спектра необходим на практике, поскольку в реальной жизни санкционирование использования спектра практически не даёт никаких гарантий того, что служба, которой было дано разрешение на использование определённой полосы частот, не выйдет за пределы своих полномочий и не нарушит предписанные правила.

Нарушения в использовании спектра могут быть вызваны сложностью оборудования, взаимодействием с другим оборудованием, неисправной работой или преднамеренным неправильным его использованием. Эта проблема еще более усугубляется вследствие ускоренного роста количества наземных беспроводных и спутниковых систем, а также оборудования, которое может создавать помехи, например компьютеры и другие непреднамеренные источники излучения.

Для проведения инспекций существует специальная система контроля спектра, которая предусматривает применение метода проверки и является «замыкающим» звеном в процессе управления использованием спектра, которое осуществляется непрерывно.

Система контроля спектра предназначена для достижения следующих целей [1]:

– содействие в решении проблем электромагнитных радиочастотных помех в местном, региональном или глобальном масштабе таким образом, чтобы обеспечить одновременную совместимую работу радиослужб и станций;

– содействие в обеспечении допустимого качества приема населением звуковых и телевизионных вещательных передач;

– обеспечение необходимых данных контроля для управления использованием электромагнитного спектра со стороны администрации, касающегося фактического использования частот и полос частот (т. е. занятость каналов и перегрузка полос частот), проверка надлежащих технических и эксплуатационных характеристик передаваемых сигналов, обнаружение и опознавание несанкционированных передатчиков, а также ведение и проверка;

– обеспечение необходимых данных контроля для программ, организуемых Бюро радиосвязи.

Процесс раздела радиочастотного спектра между различными радиослужбами либо на исключительной, либо на совместной основе называется распределением спектра. На международном уровне это распределение регулируется всемирными конференциями радиосвязи (ВКР). На основе международной таблицы распределения частот службы контроля и исполнительные органы могут составлять национальные таблицы распределения частот, распре-

делять полосы частот радиослужбам и давать разрешения на эксплуатацию конкретных систем.

Для обеспечения эффективного использования спектра необходимо выделять рассматриваемой службе те полосы частот, которые будут обеспечивать распространение радиоволн а также удовлетворять требованиям этой службы. Например, если организация обеспечивает всенаправленное покрытие большой территории, такой как вещательное телевидение, ей выделяются полосы частот в относительно низкочастотной части спектра; частным подвижным радиослужбам распределяются полосы частот ОВЧ/УВЧ-диапазона для обеспечения ограниченного местного покрытия; для глобальных воздушных и морских служб, которые требуют всемирного охвата, распределяются полосы частот ВЧ-диапазона. Данные распределения частот иногда подразделяются на планы распределения каналов, чтобы обеспечить соблюдение конкретных требований по загрузке каналов и многократному использованию каналов и частот.

Поскольку радиочастотный спектр является ограниченным ресурсом, а потребности пользователей как частных, так и государственных систем продолжают расти, необходимо создать механизм, с помощью которого можно осуществлять присвоение частот конкретным службам и системам таким образом, чтобы при этом было обслужено наибольшее число пользователей. Данный механизм реализуется посредством процесса координации частот.

Координация частот начинается с процесса выбора частот для системы, при которых не будут создаваться помехи другим системам. Затем можно осуществить обмен такой информацией с соответствующими заинтересованными сторонами или «скоординировать» ее для обеспечения совместимости между системами. Цель данного процесса – максимальное повышение возможности многократного использования частоты при сведении к минимуму помех между системами связи при их эксплуатации.

Существует несколько ключевых элементов, которые необходимо учитывать в процессе координации частот [2].

Во-первых, администрация должна определить правила и регламентные положения, которые будут служить основой процесса координации частот.

Во-вторых, должен быть осуществлен обмен информацией между заявителем новой службы и координирующей организацией.

Информация должна включать достаточное количество технических данных с тем, чтобы координирующая организация могла провести подробный анализ помех для обеспечения того, чтобы новая служба не создавала вредных помех существующим радиосредствам. Эффективность координации частот непосредственно связана с точностью и сроком действия записей, содержащихся в базе данных, и возможностью точно прогнозировать работу существующих и планируемых систем.

Координация частот и исследования по вопросам совместимости между существующими и планируемыми радиосредствами – необходимые части эффективной системы управления использованием спектра независимо от того, проводятся ли они на национальном или международном уровне.

Совместное использование частот может быть облегчено путем регулирования мощности, пространственного разнесения пользователей, развязки за счет диаграмм направленности антенн, координации пользователей по времени, допущения определенного уровня помех, пока они еще не стали вредными, или применения новых технологий, обеспечивающих возможность сосуществования нескольких передач на одной и той же частоте [3].

Преимущества системы управления использованием спектра не могут быть реализованы, если пользователи не выполняют требований полученной лицензии и не соблюдают соответствующих правил и регламентных положений. Регламентные правила обычно включают положения, определяющие действия, которые могут быть предприняты при обнаружении какого-либо нарушения со стороны пользователя. В зависимости от серьезности нарушений могут быть приняты меры воздействия в диапазоне от предупреждений и штрафов до лишения лицензий и прекращения работы систем.

Без эффективных процедур обеспечения соблюдения правил может быть нарушена целостность процесса управления использованием спектра. Обнаружение сигналов несанкционированных передатчиков иногда может осуществляться с помощью метода слухового контроля на частотах, на которых, по жалобам санкциони-

рованных пользователей, имеются помехи или на которых, согласно записям, отсутствуют пользователи с санкционированными присвоениями частот. Радиопеленгация, подвижные станции слежения и информация слухового контроля являются полезными инструментами для опознавания и определения местонахождения несанкционированных передатчиков после их обнаружения.

В таблице представлен пример распределения радиочастот на территории Курской области.

Пример распределения радиочастот
на территории Курской области

f_{min}, кГц	f_{max}, кГц	Службы
37,5	38,25	Подвижная служба, фиксированная служба, радионавигационная служба
38,25	39,986	Подвижная служба, фиксированная служба
39,986	40,02	Подвижная служба, фиксированная служба, служба космических исследований
40,02	40,98	Подвижная служба, фиксированная служба
40,98	41,015	Подвижная служба, фиксированная служба, служба космических исследований
41,015	44	Подвижная служба, фиксированная служба
44	47	Подвижная служба, фиксированная служба
47	48,5	Сухопутная подвижная служба, фиксированная служба, радиолокационная служба
48,5	56,5	Радивещательная служба, радиолокационная служба
56,5	58	Сухопутная подвижная служба, фиксированная служба
58	66	Радивещательная служба, радиолокационная служба
66	74	Радивещательная служба, радиолокационная служба
74	74,6	Подвижная служба, фиксированная служба
74,6	75,4	Воздушная радиовещательная служба
75,4	76	Подвижная служба, фиксированная служба
76	100	Радивещательная служба

Окончание табл.

f_{min}, кГц	f_{max}, кГц	Службы
100	104	Радивещательная служба
104	108	Радивещательная служба, воздушная подвижная служба
108	117,975	Воздушная радиовещательная служба
117,975	137	Воздушная подвижная служба

Таким образом, выполнение представленных действий гарантирует эффективное использование радиочастотного спектра и обеспечивает беспроблемную работу систем и служб связи.

Список литературы

1. Справочник по управлению использованием спектра на национальном уровне / Международный союз электросвязи; Бюро радиосвязи. – Женева, 1995.

2. Справочник по компьютерным методам управления использованием спектра / Международный союз электросвязи; Бюро радиосвязи. – Женева. 1999.

3. МСЭ-R SM.1139. Система международного контроля [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 621.396.96

В.В. Беляков, С.С. Хотынюк

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ РАДИОЭФИРА НА ТЕРРИТОРИИ ГОРОДА КУРСКА

Представлена организация осуществления контроля радиочастотного спектра на территории города Курска.

Заявления о помехах, мешающих работе определённых служб связи (как местным операторам, так и обычным физическим лицам), совершенно нередкое явление. Для проведения мониторинга и радиоконтроля в городе Курске существуют государственные организации специального назначения, одной из которых является радиочастотный центр (РЧЦ). В его полномочиях проводить мероприятия по контролю за эфиром в пределах Курской области, выявлять нарушения в использовании спектра, рассмотрение жалоб

как физических, так и юридических лиц о помехах в эфире, мешающих осуществлению деятельности данных лиц.

Для отслеживания и контроля нарушений организация использует специальную аппаратуру и программное обеспечение, предоставленные им от компаний, производящих данное оборудование и имеющих контракт на эти поставки. Для местного мониторинга и контроля использования спектра у РЧЦ имеются подвижные станции пеленгования источников радиоизлучений, наиболее эффективным из которых является комплекс БАРС МПИ-2.

Данная передвижная станция предназначена для анализа загрузки поддиапазонов частот, фиксированных частот, пеленгования источников радиоизлучений ОВЧ-СВЧ-диапазонов, измерений частотных и временных параметров радиосигналов, а также напряженности электрического поля. Комплекс удовлетворяет требованиям ГОСТ Р52536-2006.

В Комплексе БАРС МПИ-2 реализованы: улучшенные основные технические параметры, в том числе: расширен диапазон рабочих частот до 18 ГГц; увеличена полоса одновременного обзора и анализа до 20МГц; повышена точность измерения энергетических, частотных и временных параметров сигналов; реализован структурный доступ к цифровым системам транкинговой связи (в том числе стандарт TETRA), сотовой связи второго (стандарты GSM, CDMA) и третьего (стандарт UMTS) поколений, беспроводного широкополосного радиодоступа (стандарты 802.11 и 802.16), радиовещания (DAB) и телевизионного вещания; уменьшены массогабаритные характеристики и энергопотребление за счет перехода на технологию CompactPCI.

CompactPCI – системная шина, широко используемая в промышленной автоматике. Электрически шина отличается от PCI стандарта 2.2 тем, что позволяет подключить большее число устройств.

Рассмотрим структуру комплекса БАРС МПИ-2 (рис. 1 – 3). Он состоит из антенно-фидерного коммутационного устройства (АФКУ), измерительных антенн П6-59 и Пб-ЛПА, блоков аналого-цифровых радиоприемных устройств ЦРПУ-01 и ЦРПУ-02, блока конверторов, персональной электронной вычислительной машины ПЭВМ.

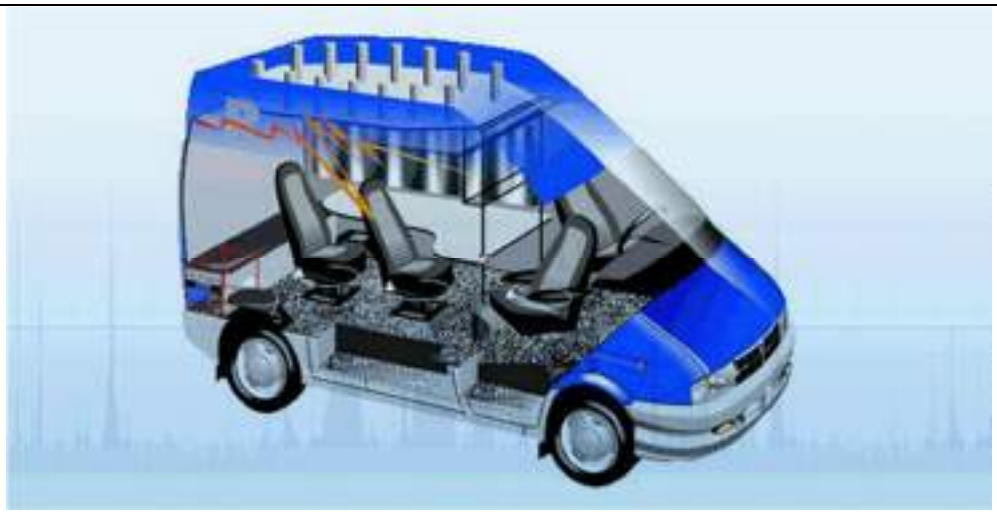


Рис. 1. Структура комплекса пеленгования источников радиоизлучений Барс МПИ-2

Рис. 2. Вид Барс МПИ-2 изнутри

Антенно-фидерное коммутационное устройство предназначено для приема радиосигналов при пеленговании источников радиоизлучений в ОВЧ-УВЧ-диапазонах и представляет собой многоэлементные антенные решетки из ненаправленных антенных элементов, объединенные с электронным коммутационным устройством, позволяющим попарно или непосредственно (в зависимости от модификации) подключать антенные элементы в различных комбинациях. Измерительная антенна Пб-59 предназначена для измерения в составе комплекса напряженности электрического поля, а также пеленгования источников радиоизлучения в СВЧ-диапазоне и представляет собой рупорную антенну. Измери-

тельная антенна Пб-ЛПА используется для измерения в составе комплекса напряженности электрического поля и представляет собой логопериодическую антенну.

Рис. 3. Пример проведения инспекции радиоэфира

Для получения частотных характеристик радиосигнала цифровые отсчеты сигнала на выходе ЦРПУ-01 подвергаются математической обработке в ПЭВМ с применением модуля интегрального измерителя, реализованного программно. Результат измерения отображается на экране ПЭВМ.

Комплекс решает следующие задачи: высокоскоростное обнаружение и регистрация радиоизлучений с возможностью опознавания сигналов могут быть выполнены одним из следующих методов: на слух, на программно-реализованном анализаторе спектра, путем сравнения обнаруженных источников радиоизлучений с параметрами РЭС, хранящимися в базе данных.

Подвижная станции может выполнять оценку загрузки поддиапазонов частот, частотных каналов с предоставлением амплитудно-частотной, частотно-временной панорамы, а также экспресс-анализ параметров радиоизлучений.

Инструментальный контроль энергетических, частотно-временных и пространственных параметров радиоизлучений включает в себя:

– измерение напряженности электромагнитного поля;

– измерение центральной частоты;

– измерение ширины полосы частот;

– измерение временных характеристик;

– определение вида и параметров модуляции;

– пеленгование (определение местоположения при работе в составе пеленгаторной группы) источников радиоизлучений, в том числе помех, с отображением результатов на картографическом фоне;

– определение местоположения ИРИ подвижным комплексом с применением триангуляционного метода на маршруте движения;

– оценка местоположения ИРИ по разностям измерений уровня сигнала на маршруте движения;

– определение местоположения базовых станций пеленгаторной группой или одним подвижным комплексом при работе в движении;

– автоматическое пеленгование с использованием рупорной антенны.

Контроль параметров и служебной информации в современных цифровых сетях сотовой связи, транкинговой связи, беспроводного широкополосного радиодоступа, цифрового телевизионного вещания и радиорелейных линиях связи:

– в сетях сотовой связи стандартов GSM/DCS;

– в сетях сотовой связи стандарта CDMA (IMT-MC-450);

– в сетях сотовой связи стандарта UMTS;

– в сетях транкинговой связи стандарта TETRA;

– в сетях широкополосного беспроводного радиодоступа стандарта 802.11;

– в сетях широкополосного беспроводного радиодоступа стандарта 802.16;

– в сетях широкополосного беспроводного радиодоступа стандарта DECT;

– в сетях цифрового телевизионного вещания стандарта DVB-T.

Основные тактико-технические характеристики:

– диапазон анализируемых частот 25–18000 МГц;

– полоса пропускания аналоговых трактов 20 МГц;

– скорость сканирования при анализе загрузки частотного диапазона 500 МГц/с.

Таким образом, описанный комплекс позволяет проводить высокоэффективный анализ радиочастотного спектра на территории города Курска.

Список литературы

1. ГОСТ Р52536-2006. Положения о единой технической политике предприятий радиочастотной службы. – М.: Изд-во стандартов, 2009.

2. Справочник по компьютерным методам управления использованием спектра / Международный союз электросвязи; Бюро радиосвязи. – Женева, 1999.

3. МСЭ-R SM.1537. Автоматизация и интеграция систем контроля использования спектра с автоматизированным управлением спектра [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Общество с ограниченной ответственностью «Специальный Технологический Центр» [Электронный ресурс]. – Режим доступа: http://www.stc-spb.ru/.

УДК 621.394.74

А.Ю. Богомазов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МОДЕЛИРОВАНИЕ ВЛИЯНИЯ ЭФФЕКТА МНОГОЛУЧЕВОГО РАССЕИВАНИЯ РАДИОСИГНАЛА В СПУТНИКОВЫХ СИСТЕМАХ СВЯЗИ

Предложен подход к оценке эквивалентных энергетических потерь при приеме сигналов спутниковых систем связи при многолучевом распространении радиоволн.

Интенсивное развитие инфокоммуникационных систем, в частности, высокоскоростных цифровых систем спутниковой связи (ССС), использующих сигналы с шириной спектра, соизмеримого с полосой когерентности канала, приводит к необходимости учета вредного влияния многолучевого распространения радиоволн на мелкомасштабных неоднородностях ионосферы, фактора рассеяния радиоволн в ионосфере на достоверность приема сигналов. При этом на входе приемной антенны возникает явление множественной интерференции, приводящей к существенному искаже-

нию спектра принятого сигнала, что, в свою очередь, приводит к энергетическим потерям и повышению вероятности ошибки на символ на выходе демодулирующей системы комплекса приема сигналов цифровых ССС. В связи с этим весьма актуальной является задача оценки уровня таких энергетических потерь в зависимости от изменяющихся условий приема. В дальнейшем будем использовать понятие эквивалентных энергетических потерь (ЭЭП), которые определим как такое дополнительное увеличение отношения сигнал/шум на входе приемной системы (антенна), которое бы обеспечило прежний уровень вероятности ошибки на символ в отсутствии многолучевости.

Распределение электронной концентрации в ионосфере представим в следующем виде [2]:

$$N_э = 1.7 N_{\max} \frac{\sqrt{R^2 + h^2 + Rh\sin\beta} - h_d - R}{h_m - h_d} \times$$

$$\times \exp\left(-\frac{1}{2}\left[\frac{\sqrt{R^2 + h^2 + Rh\sin\beta} - h_d - R}{h_m - h_d} \right]^2 \right),$$

где β – угол наклона трассы распространения электромагнитных волн относительно горизонта;

R – радиус Земли;

h_d – нижняя граница ионосферы;

h_m – высота слоя ионосферы с максимальной концентрацией электронов.

В ионосфере показатель преломления [2]

$$n(f) = \sqrt{1 - f_p^2 / f^2} = \sqrt{1 - 80.8 N_э / f^2},$$

где f_p – плазменная частота.

Фазовые сдвиги на элементарных отрезках накапливаются вдоль пути распространения радиоволн и приводят к фазовому набегу [2]:

$$\varphi = \frac{2\pi f}{c} \int_{l_1}^{l_2} n dl = \frac{2\pi f}{c} \int_{l_1}^{l_2} (1 - 0.5 f_p^2 / f^2) dl.$$

Представим сигнал $S(t)$ на входе приемной антенны в фиксированный момент времени t=const при многолучевом распространении радиоволн в виде суммы векторов $S_1(t)$ $S_2(t)\ldots$ $S_N(t)$, где N-количество лучей.

При этом выражение для сигнала на выходе антенны будет иметь вид [3]

$$S(t)=\sum_{i=1}^{N}\lambda_i e^{i\omega(t+\tau_i)}e^{i\nu(t+\tau_i)}, \qquad (1)$$

где λ_i – амплитуда сигнала i-го луча;

τ_i – временная задержка i-го луча по отношению к основному;

ω – круговая частота сигнала;

$\nu(t)$ – информационная составляющая сигнала, обусловленная его модуляцией.

Преобразуем выражение (1) в комплексный вид, т.е.

$$S(t)=\sum_{i=1}^{N}\lambda_i\cos\omega(t+\Delta t_i)+i\sum_{i=1}^{N}\lambda_i\sin\omega(t+\Delta t_i). \qquad (2)$$

Условно выберем в качестве направления базисного вектора оси абсцисс направление вектора с максимальной амплитудой S_1. Тогда мгновенное значение фазовой погрешности суммарного сигнала или фазового шума $\varphi_ш$, вызванного многолучевым распространением радиоволн в момент времени t=0, определим как аргумент выражения (2):

$$\varphi_i=\operatorname{arctg}\left[\left(\sum_{i=1}^{N}\lambda_i\sin\omega\Delta t_i\right)\Big/\left(\sum_{i=1}^{N}\lambda_i\cos\omega\Delta t_i\right)\right]. \qquad (3)$$

Дисперсия мгновенного значения фазового шума σ^2 определяется как средняя мощность фазовой погрешности на интервале длительности периода несущей частоты сигнала:

$$\sigma^2=\frac{1}{2\pi}\int_0^{2\pi}\operatorname{arctg}^2\left[\left(\sum_{i=1}^{N}\lambda_i\sin\omega\Delta t_i\right)\Big/\left(\sum_{i=1}^{N}\lambda_i\cos\omega\Delta t_i\right)\right]d\omega. \qquad (4)$$

В силу априорной неопределенности параметров канала распространения радиоволн при его многолучевости фаза, определяемая выражением (3), является случайной функцией амплитуд пар-

циальных лучей и их временных задержек. Для определения закона распределения величины φ проведено статистическое моделирование выражения (3) при условии равномерного распределения $\omega\Delta t_i$ на интервале $[0,\pi]$ и при различных соотношениях между λ_i и их количеством.

Оценка результатов по критерию Пирсона показала, что полученные гистограммы с доверительной вероятностью 0,95 совпадают с нормальным законом распределения [4]:

$$W(\varphi)=\frac{1}{\sqrt{2\pi\sigma}}e^{-\varphi^2/2\sigma^2}, \qquad (5)$$

где σ^2 – дисперсия фазового шума сигнала, подверженного влиянию многолучевости.

При выводе ЭЭП воспользуемся известным представлением плотности вероятности фазы суммарного процесса гармонического сигнала и гауссова шума [4]:

$$W(\varphi)=(2\pi)^{-1/2}\cdot|g|\cdot\exp(-\frac{g^2\varphi^2}{2}). \qquad (6)$$

Из анализ графических зависимостей (5) и (6) следует, что определенному значению дисперсии фазового шума σ^2 в выражении (5) соответствует определенное значение отношения сигнал/шум g в выражении (6). При этом ход кривых с достаточной для практики точностью можно считать идентичными.

Учитывая практическую идентичность распределений (5) и (6), установим зависимость отношения сигнал/ шум g от дисперсии фазового шума σ^2. Для этого приравняем выражение (5) к (6):

$$\frac{1}{\sqrt{2\pi\sigma}}e^{-\varphi^2/2\sigma^2}=(2\pi)^{-1/2}\cdot g\cdot\exp(-\frac{g^2\varphi^2}{2}). \qquad (7)$$

Решив уравнение (7) относительно g при φ=const, получим

$$g=\frac{\exp(-LambertW(0,-(\frac{\varphi^2\exp(-\varphi/\sigma^2)}{\sigma})\exp(\frac{-\varphi}{2\sigma^2})}{2}}{\sigma^{1/2}}. \qquad (8)$$

Выражение (8) позволяет рассчитать эквивалентное отношение сигнал/шум при наличии в точке приема нескольких парциальных лучей.

Значение ЭЭП вследствие многолучевости определим как

$$\Delta g = \frac{g_0}{1 + g_m}, \tag{9}$$

где g_0 – максимальное значение отношения сигнал/шум на выходе конкретного типа антенны при отсутствии многолучевости. В качестве верхнего предела принимается максимальное значение коэффициента направленного действия при согласованной поляризации;

g_m– эквивалентное отношение сигнал/шум на выходе конкретного типа антенны при наличии многолучевости.

Из выражений (8) и (9) следует, что

$$\Delta g = g_0 / (1 + \frac{\exp(-LambertW(0, -\frac{\varphi^2 \exp(-\varphi/\sigma^2)}{\sigma}) \exp(\frac{-\varphi}{2\sigma^2})}{2\sigma^{1/2}}). \tag{10}$$

Выражение (10) представляет сбой математическую модель ЭЭП в АФУ при наличии многолучевого распространения радиоволн.

На рисунке представлена графическая зависимость ЭЭП от уровня дисперсии фазового шума, обусловленного многолучевым распространением радиоволн в ионосфере.

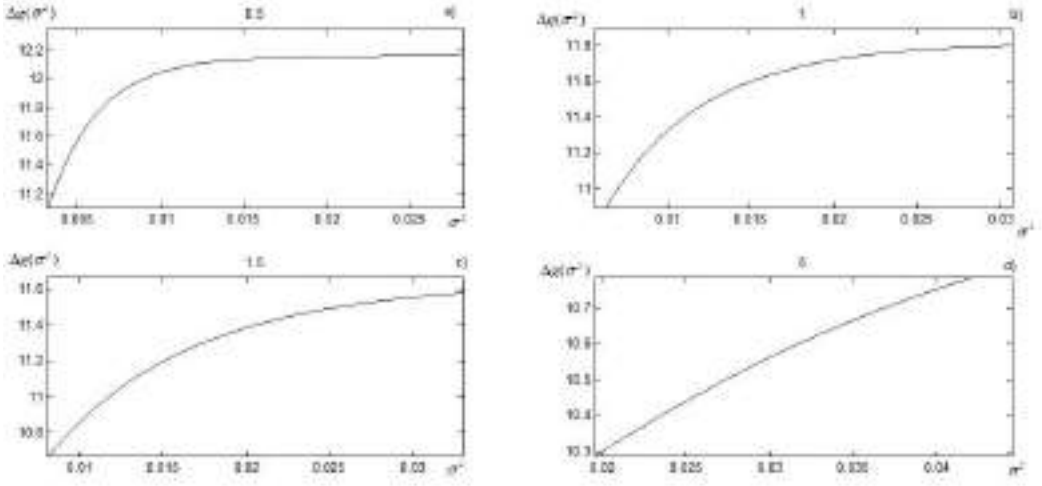


Рис. 1. Зависимость ЭЭП от дисперсии фазового шума сигнала при различных электронных плотностях в ионосфере

При различной электронной концентрации в ионосфере набег фазы сигнала составлял: a) 0.5^{o}; b) 1^{o}; c) 1.5^{o}; d) 5^{o}. Анализ приведенной зависимости показывает, что ЭЭП имеют наибольшую скорость роста при дисперсии фазового шума от 0 до 0,5 радиан. В дальнейшем скорость роста снижается, что обусловлено ростом взаимной компенсации фаз парциальных лучей.

Выводы

1. Разработана математическая модель эквивалентных энергетических потерь на выходе приемной антенны в условиях многолучевого распространения радиоволн на трассе Земная станция – космический аппарат, при этом ЭЭП определяются количеством парциальных лучей и уровнем фазовых сдвигов.

2. Полученная математическая модель выражения позволяет прогнозировать уровень эквивалентных энергетических потерь в конкретных условиях эксплуатации приемных систем спутниковых цифровых линий связи.

Список литературы

1. Космические траекторные измерения / под ред. П.А. Агаджанова, В.Е. Дулевича, А.А. Коротселева. – М.: Сов.радио, 1969. – 504 с.

2. Теоритические основы радиолокаций / под ред. В. Е. Дулевича. – М.: Сов. радио, 1978. – 608 с.

3. Петренко П.Б., Бонч-Бруевич А.М. Моделирование и оценка ионосферных искажений широкополосных радиосигналов в локации и связи // Вопросы защиты информации. – 2007. – №3. – С. 24-29.

4. Тихонов В.И., Харисов В.Н. Статистический анализ радиотехнических устройств и систем: учеб. пособие для вузов. – М.: Радио и связь, 1991. – 608с.

УДК 621.396

А.Н. Зикий, П.Н. Зламан, О.А. Горбатенко

Южный федеральный университет, Ростов-на-Дону

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СТУПЕНЧАТОГО АТТЕНЮАТОРА

Представлены результаты экспериментального исследования ступенчатого аттенюатора с цифровым управлением. Аттенюатор построен на микросхеме AT263, испытан в диапазоне частот 0,4-2 ГГц.

Электронно-управляемые аттенюаторы используются в приемно-передающей [1-4] и измерительной аппаратуре [5], поэтому отечественные и зарубежные фирмы выпускают широкую номенклатуру аттенюаторов СВЧ. Они могут иметь как аналоговое, так и цифровое управление. В данной работе проведено исследование аттенюатора с цифровым управлением.

Объектом исследования является аттенюатор на основе микросхемы AT263 фирмы M/A Com. Этот аттенюатор был использован в составе модулятора [1] и передатчика [5], однако детальное его исследование в работах [1,5] не проводилось. Принципиальная схема аттенюатора приведена на рисунке 1.

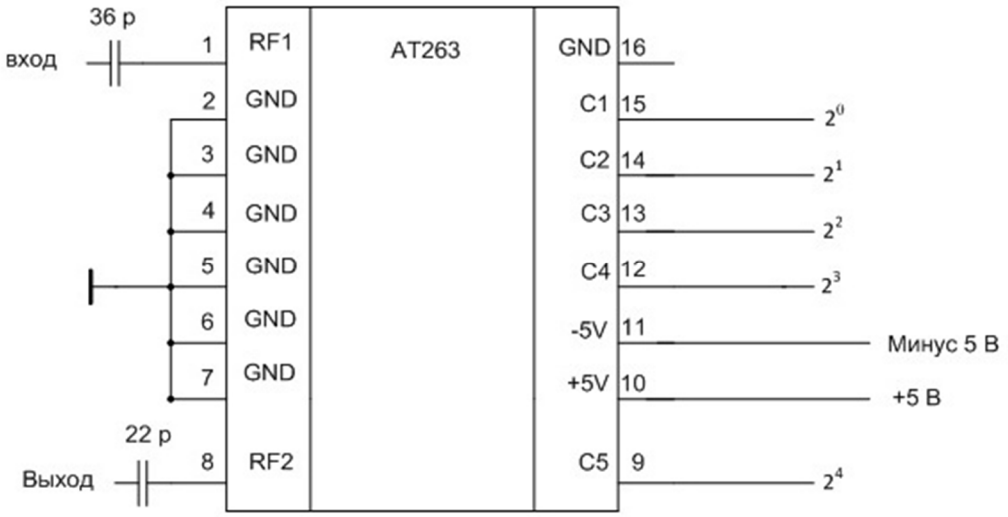


Рис. 1. Принципиальная схема аттенюатора

Целью настоящей работы является исследование частотных зависимостей потерь для различных управляющих кодов, изучение дополнительных функциональных возможностей, сопоставление с подобными устройствами.

Исследование аттенюатора проводилось на измерительной установке, структурная схема которой приведена на рисунке 2.

Источником сигнала служил генератор E8267D фирмы AgilentTechnologies. В качестве измерителя уровня выходного сигнала использован анализатор спектра типа 8564EC той же фирмы. Измерение проводилось по точкам в диапазоне рабочих частот 0,4-2 ГГц с шагом 100 МГц.

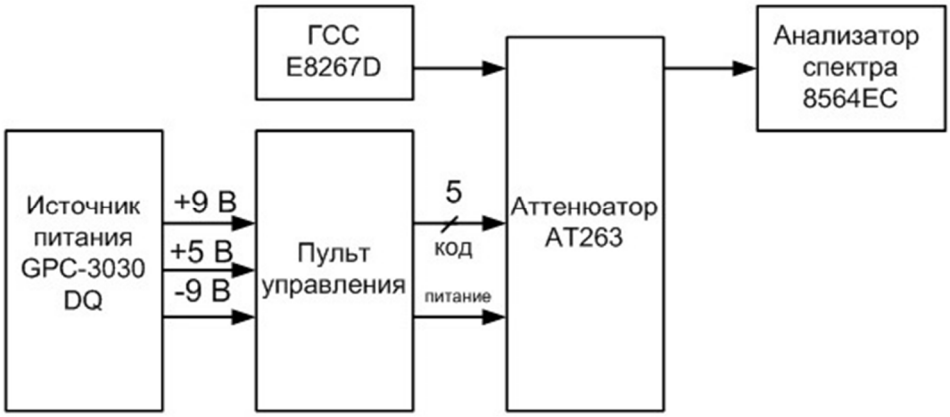


Рис. 2. Структурная схема измерительной установки

Пятиразрядный код управления подавался на аттенюатор от специального пульта управления, состоящего из пяти тумблеров типа МТ1, формирующих логические нули и единицы.

В первом эксперименте на аттенюатор был подан нулевой код управления. Результаты измерений оказались равны 4±0,5 дБ (вместе с потерями двух кабелей).

Во втором эксперименте на аттенюатор был подан код управления 2^4=16, результаты измерений представлены на рисунке 3.

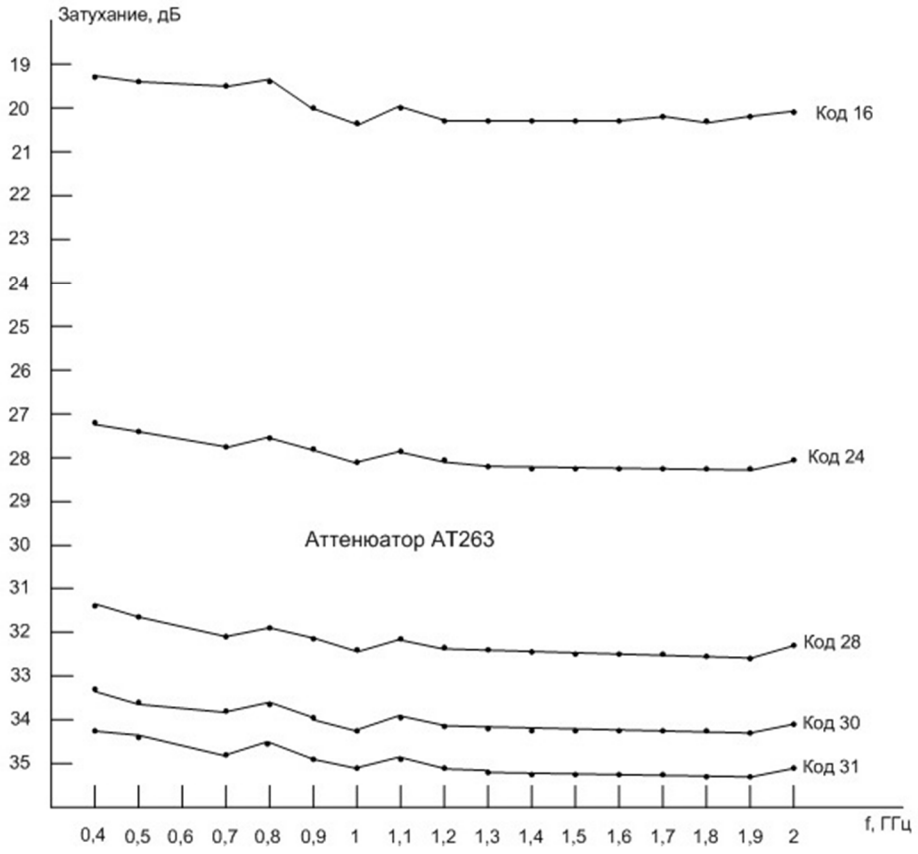


Рис. 3. АЧХ аттенюатора при разных кодах управления

В третьем эксперименте на аттенюатор был подан код управления $2^4+2^3=24$, результаты измерений занесены на рисунок 3.

В четвертом эксперименте на аттенюатор был подан код управления $2^4+2^3+2^2=28$, результаты измерений занесены на рисунок 3.

В пятом эксперименте на аттенюатор был подан код управления $2^4+2^3+2^2+2^1=30$, результаты измерений заносились на рисунок 3.

В шестом эксперименте на аттенюатор был подан код управления $2^4+2^3+2^2+2^1+2^0=31$, результаты измерений заносились на рисунок 3.

Выводы

1. Начальное затухание не превышает 4±0,5 дБ в диапазоне частот 0,4 – 2 ГГц. В него включены потери двух кабелей.

2. Максимальное затухание не превышает 35,0±1,0 дБ в диапазоне частот 0,4 – 2 ГГц.

3. Полное затухание соответствует коду затухания плюс начальное затухание.

4. Высокое быстродействие аттенюатора позволяет его использовать в качестве импульсного модулятора.

Список литературы

1. AT-263 Digital Attenuator, 31dB, 5-bit, TTL Driver, DC-2 GHz. M/A-COM [Electronic resource]. – URL: http: www.macom.com.

2. Модулятор передатчика сложных сигналов / С.Э. Додаев, А.Н. Зикий, П.Н. Зламан, В.О. Слащева // Электротехнические и информационные комплексы и системы. – 2012. – Т. 8. – №2. – С. 3-5.

3. Белов Л.А. Устройства формирования СВЧ-сигналов и их компоненты: учебное пособие. – М.: Издательский дом МЭИ, 2010. – 320 с.

4. Румянцев К.Е. Прием и обработка сигналов: учебное пособие. – М.: Академия, 2004. – 528 с.

5. Зикий А.Н., Зламан П.Н. Передатчик сигналов с ППРЧ // Новости научного прогресса: матер. 9-й Междунар. науч.-практ. конф. (17-25 августа 2013 г.). – София (Болгария), 2013. – С. 26-29.

6. Радиоизмерительная аппаратура СВЧ и КВЧ. Узловая и элементная базы / под ред. А.М. Кудрявцева. – М.: Радиотехника, 2006. – 208 с.

7. Белов Л.А. Аттенюаторы СВЧ // Электроника: НТБ. – 2006. – №2.

УДК 621.394.74

Д.И. Изотов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РЕЗУЛЬТАТЫ ИЗМЕРЕНИЯ ПАРАМЕТРОВ ТЕРМОЭЛЕКТРИЧЕСКИХ ИСТОЧНИКОВ АЛЬТЕРНАТИВНОГО ЭЛЕКТОРОПИТАНИЯ

Показано возможное применение автономных источников электрической энергии на основе термоэлектрических генераторных модулей для питания маломощных передатчиков.

Развитие современной техники и технологий неразрывно связано с поиском новых источников энергии, в первую очередь электрической. Основное требование – увеличить объем ее выработки, но в последнее время на передний план выходят дополнительные условия: энергия должна вырабатываться экологически чистым путем, должна быть возобновляемая и никак не связана с углеродом. Термоэлектрическая генерация является одним из перспективных, а в некоторых случаях единственно доступным способом прямого преобразования тепловой энергии в электрическую.

Исследование элементов Пельтье заключалось в измерении напряжения и тока, протекающего через сопротивление $R = 200$ Ом.

Элементы Пельтье предназначены для генерации разности температур на сторонах модуля при подведении к его контактам разности потенциалов. Поэтому в ходе исследования при их подключении в обратном режиме значения токов и напряжений были в десятки раз меньше, чем для элементов Зеебека при тех же разностях температур.

Цель исследования – подтвердить линейный характер изменения тока и напряжения и квадратичный характер изменения мощности в термоэлектрических источниках.

Результаты практических исследований с элементами Пельтье представлены в таблице.

Результаты практических исследований элементов Пельтье

t, ° С	$U1$, В	$I1$, мА	$U2$, В	$I2$, мА	$U3$, В	$I3$, мА	$U4$, В	$I4$, мА
70	1,63	6,23	1,08	6,07	0,734	4,37	0,604	4,03
65	1,40	6,12	1,06	5,83	0,666	4,11	0,590	3,78
60	1,35	5,67	1,05	5,43	0,629	4,03	0,553	3,54

Окончание табл.

t, °С	$U1$, В	$I1$, мА	$U2$, В	$I2$, мА	$U3$, В	$I3$, мА	$U4$, В	$I4$, мА
55	1,17	4,41	1,04	4,29	0,533	3,91	0,528	3,23
50	1,05	4,23	0,80	4,11	0,500	3,84	0,477	3,07
45	1,02	4,11	0,79	3,87	0,436	3,52	0,411	2,87
40	0,95	4,01	0,76	3,62	0,386	2,93	0,350	2,66
35	0,82	3,89	0,70	3,40	0,323	2,77	0,286	2,52

Для обеспечения питания маломощных передатчиков используются элементы Зеебека, для которых известны результаты измерения при малых температурах.

Ниже приведены результаты испытаний двух образцов ТГМ в таком режиме.

Как видно из результатов испытаний, приведенных на рисунке 1, генераторный модуль ТГМ-199-1,4-1,5 обеспечивает выходное напряжение порядка 400 мВ и выходную мощность порядка 45 мВт при наличии минимальной разности температур 10°С. График показывает, что необходимое для устойчивой работы современных микросхем для EnergyHarvesting-решений напряжение 30 мВ будет обеспечено при разности температур на сторонах модуля 2…3°С.

Испытания проводились при изменении температуры горячей стороны от 35 до 50°С с шагом 5°С при фиксированном значении температуры холодной стороны модуля 25°С. Следует ожидать получения большего значения выходного напряжения в случае применения генераторных модулей серии ТГМ-287, имеющих большее число термопар и, как следствие, пропорционально большее значение термоЭДС.

Как уже было сказано, значения снимаемых с модуля тока и напряжения с увеличением разности температур возрастают в линейной, а мощность – в квадратичной пропорции. На приведенных графиках разность в поведении напряжения и мощности неочевидна, поскольку в начале отсчета кривизна квадратичной функции невысока и нивелируется погрешностями замеров.

Это хорошо видно на рисунке 2, где представлены графические характеристики того же модуля в широком интервале температур.

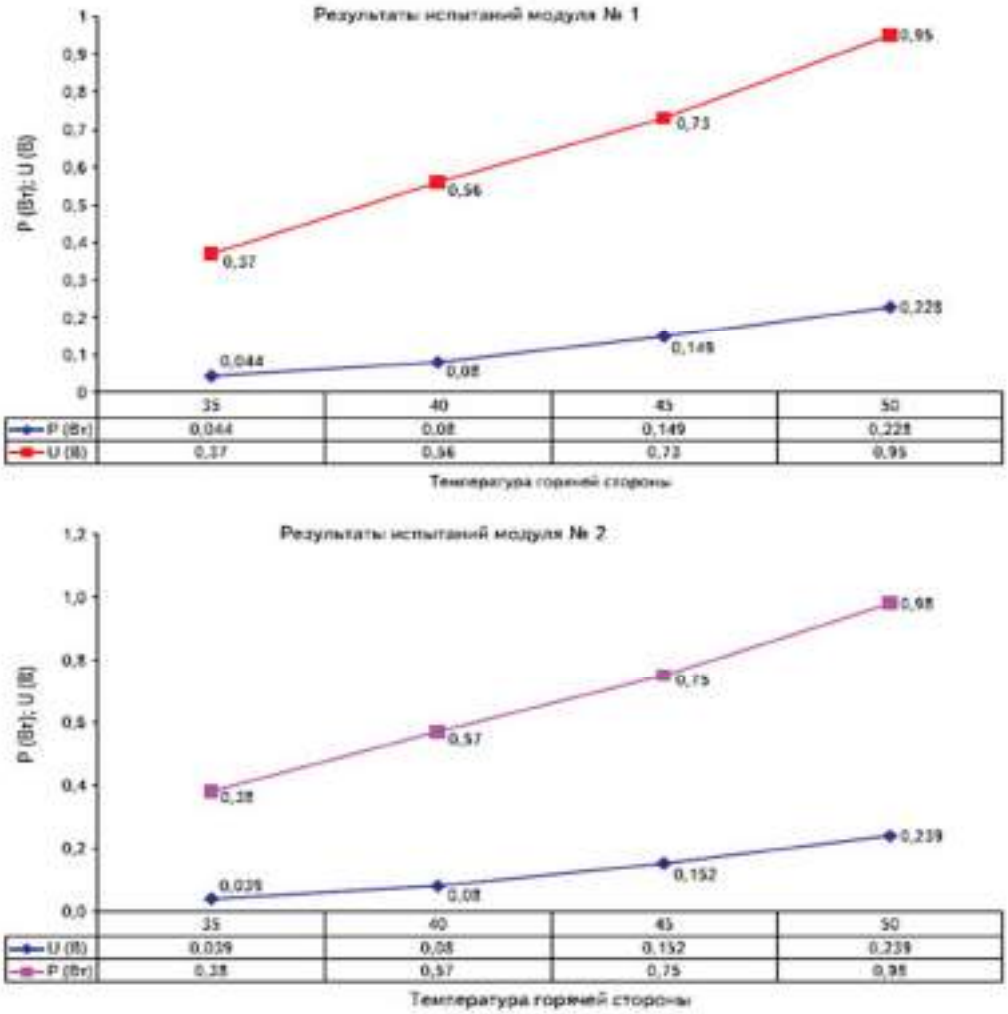


Рис. 1. Результаты испытаний генераторных модулей на малых перепадах температуры при *Т*с = 25 °С

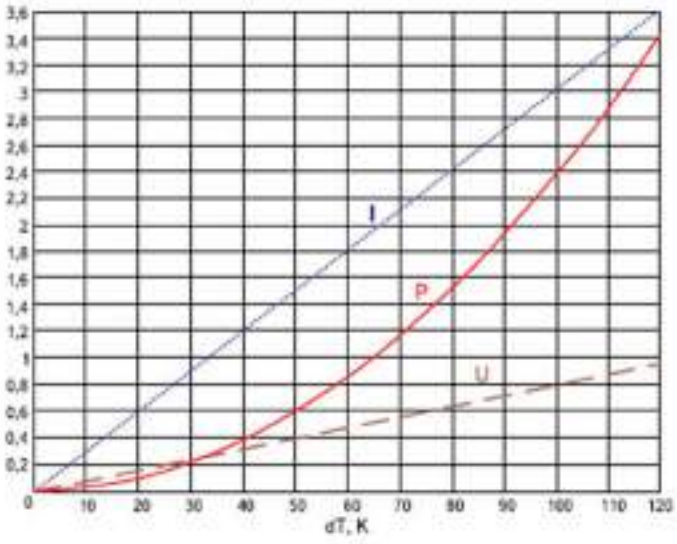


Рис. 2. График зависимости тока *I* (А), напряжения *U* (В) и мощности *P* (Вт) от разности температур между горячей и холодной сторонами генераторного модуля

Выводы

Автономные источники электрической энергии на основе термоэлектрических генераторных модулей находят применение для питания маломощных передатчиков.

ТГМ обеспечивает выходное напряжение порядка 400 мВ и выходную мощность порядка 45 мВт при наличии минимальной разности температур 10 °С. А необходимое для устойчивой работы современных микросхем для EnergyHarvesting-решений напряжение 30 мВ обеспечивается при разности температур на сторонах модуля 2…3 °С.

---

1. Бурштейн А. И. Физические основы расчета полупроводниковых термоэлектрических устройств. – М: Физматгиз, 1962. – 383 с.

2. Тахистов Ф. Ю. Оптимизация параметров термоэлектрического генераторного модуля с учетом эффективности теплообмена на сторонах модуля. – СПб.: Изд-во ФТИ, 2008. – 272 с.

УДК 004.942: 621.396.2

В.Г. Дорохов[1], А.Н. Замыцкий[2], В.В. Матвеенко[2], А.А. Спашко[1]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) ФГУП «18 ЦНИИ» МО РФ

ПОСТРОЕНИЕ МОДЕЛИ ПОМЕХОУСТОЙЧИВЫХ ПАКЕТОВ ДАННЫХ В РАДИОЛИНИЯХ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ПЕРСПЕКТИВНОЙ ПРОГРАММНОЙ СРЕДЫ MATLAB

Рассмотрена модель помехоустойчивых пакетов данных в радиолиниях передачи информации на основе перспективной программной среды MATLAB.

При проектировании командных радиолиний управления одно из наиболее важных мест занимает выбор и обоснование структуры передаваемого сообщения (формат передачи). Данное сообщение при заданной длительности должно позволить получить требуемые вероятностные характеристики в условиях воздействия помех. Существующие расчетные модели позволяют получать данные характеристики, однако в ходе разработки командных радиолиний управления возникает необходимость изменения как са-

мой структуры сообщения, так и его составных частей, применяя при этом разнообразные помехоустойчивые последовательности. Таким образом, создание имитационных моделей помехоустойчивых пакетов данных в радиолиниях передачи информации является актуальным.

Целью настоящей статьи является рассмотрение результатов исследования возможности построения имитационных моделей помехоустойчивых пакетов данных в радиолиниях передачи информации на основе перспективной программной среды MATLAB

Предлагается построение имитационной модели помехоустойчивых пакетов данных в радиолиниях передачи информации на основе посимвольного кодирования сообщения с помощью 11-позиционного кода Баркера.

Структура данного пакета данных (передаваемого сообщения) представлена на рисунке 1. Она включает в себя три составные части: синхронизирующую последовательность, содержащую n символов; адресную часть, состоящую из m символов; командную часть, включающую q символов.

Для повышения помехоустойчивости передаваемого сообщения применяется избыточное кодирование каждой из трех его частей помехоустойчивым кодом (11-позиционным кодом Баркера) с приемом в целом [1].

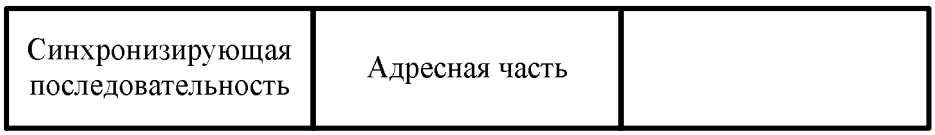


Рис. 1. Структура передаваемого сообщения (формат передачи)

Основой имитационной модели является функция, формирующая требуемую импульсную последовательность. Такой функцией в MATLAB является [2]

pulstran(t,d1,'rectpuls',tau), (1)

где t – вектор отсчетов;

d1 – вектор задержек;

'rectpuls' – функция формирования прямоугольного импульса;

tau – вектор длительности импульсов.

Вектор отсчетов задает отсчет времени по оси абсцисс. Вектор задержек d1формирует задержку импульсов в последовательности. Для формирования импульсной последовательности требуемой полярности и амплитуды используется функция задания вектора амплитуд d1(:,2)=[1 −1 1 −1]. В данном случае сформирован меандр из 4-х импульсов. Функция 'rectpuls' формирует прямоугольный импульс. Вектор длительностей tau устанавливает длительность импульсов в последовательности.

Формирование сложных составных последовательностей можно производить посредством суммирования их частей, сдвинутых по времени. Так, составную последовательность Yможно представить как сумму последовательностей y_1, y_2, y_3, сформированных описанным образом и сдвинутых одна относительно другой по времени на требуемую величину:

$$Y=y_1+y_2+y_3, \quad (2)$$

где y_1−синхронизирующая последовательность;

y_2 – последовательность адресной части;

y_3 – последовательность командной части.

Каждый символ сообщения (2) состоит из последовательности a_i, кодированной 11-позиционным кодом Баркера,что является процедурой прямого расширения спектра сигнала, повышающей помехоустойчивость системы.

Вектор кодированной последовательности a_i может быть определен как

$$a_i=[\,1\ 1\ 1\ -1\ -1\ -1\ 1\ -1\ -1\ 1\ -1]. \quad (3)$$

Графическое изображение имитационной модели кодированного символа представлено на рисунке 2.

Тогда

$$y_1=\sum_{i=1}^{n} a_i; \quad y_2=\sum_{i=n}^{n+m} a_i \quad y_3=\sum_{i=n+m}^{n+m+q} a_i, \quad (4)$$

где i – текущий номер символа на временной оси.

С учетом (4) выражение (2) может быть записано следующим образом:

$$Y=\sum_{i=1}^{n} a_i+\sum_{i=n}^{n+m} a_i+\sum_{i=n+m}^{n+m+q} a_i. \quad (5)$$

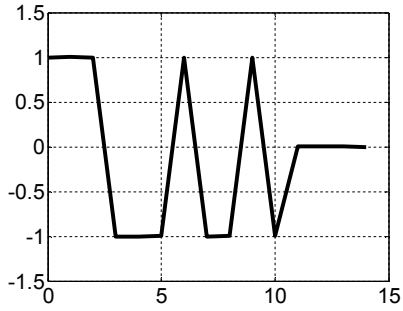


Рис. 2. Модель символа сообщения, состоящего из последовательности, кодированной 11-позиционным кодом Баркера

Выражение (5) и функция MATLAB(1) могут быть положены в основу создания модели помехоустойчивого пакета данных, графическое изображение которой представлено на рисунке 3.

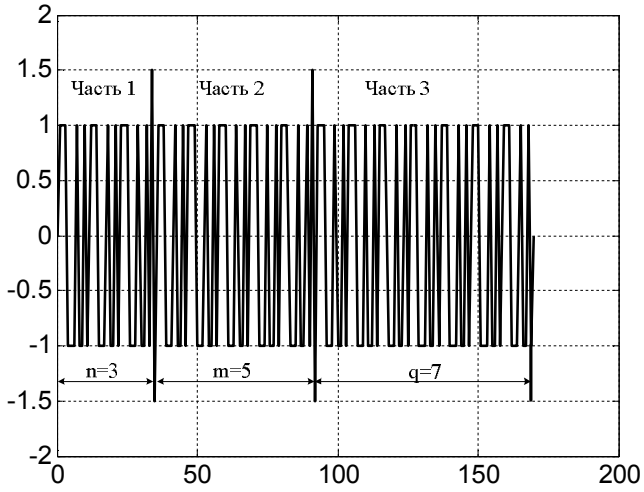


Рис. 3. Детальная структура модели помехоустойчивого пакета данных

В соответствии со структурой передаваемого сообщения (см. рис. 1) данная модель состоит из трех частей. Для примера, часть 1 содержит $n = 3$ символа, часть $2 – m = 5$ символов, часть $3 – q = 7$ символов.

Данная модель является имитационной и позволяет смоделировать процесс прохождения пакета данных по каналу распространения. Так, если канал распространения является гауссовым, то результат прохождения сигнала можно представить в виде аддитивной смеси сигналов пакета данных Y и шума $y(n)$ различной интенсивности:

$$Y_{\Sigma}=Y+y(n). \qquad (6)$$

В программной среде MATLAB указанную помеху можно смоделировать функцией

$$\text{randn}(\text{size}(t)). \qquad (7)$$

График, изображающий воздействие указанной помехи на пакет данных, представлен на рисунке 4.

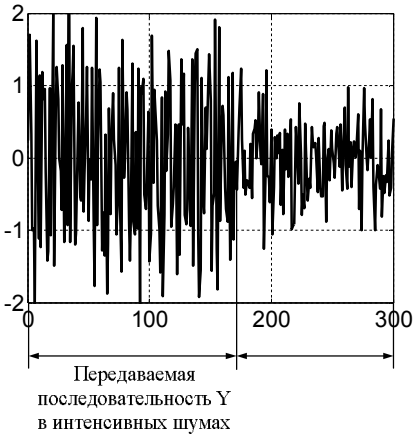


Рис. 4. Графическая интерпретация воздействия интенсивной шумовой помехи на пакет данных

Каждый элемент модели пакета данных может быть подвержен поэлементной оптимальной обработке, а каждая часть пакета − оптимальному приему в целом. Это позволяет оперативно исследовать разрабатываемые пакеты данных на помехоустойчивость.

Таким образом, построенная модель помехоустойчивых пакетов данных в радиолиниях передачи информации на основе перспективной программной среды MATLAB позволяет в ходе разработки указанных радиолиний исследовать возможности применяемой структуры пакетов, определять их помехоустойчивость и в случае необходимости производить их усовершенствование.

1. Защищенные радиосистемы цифровой передачи информации / П.Н. Сердюков, А.В. Бельчиков, А.Е. Дронов [и др.]. – М.: АСТ, 2006. – 403 с.

2. Дьяконов В.П. MATLAB и SIMULINK для радиоинженеров. – М.: ДМК Пресс, 2011. – 976 с.: ил.

УДК 004.942: 621.396.2

В.Г. Дорохов[1], А.Н. Замыцкий[2], В.В. Матвеенко[2]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) ФГУП «18 ЦНИИ» МО РФ

МОДЕЛЬ ТРОИЧНО-СИММЕТРИЧНОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ

Рассмотрена модель, формулы для расчета вероятностных характеристик и пропускная способность троично-симметричного дискретного канала передачи информации.

Возрастающие потребности в циркулировании больших объемов информации обусловливают необходимость поиска новых способов ее передачи, в том числе и с использованием сигналов, удовлетворяющих этим потребностям. Хорошо разработанные и исследованные в настоящее время двоичные одномерные последовательности в основном исчерпали свои возможности. Вместе с тем известно [1], что многомерные сигналы (в том числе и троичные) обладают некоторыми замечательными свойствами, привлекающими внимание исследователей. Исходя из этого задача поиска новых видов сигналов, исследования их информационных способностей и возможностей эффективного формирования и приема является актуальной.

Целью данной статьи является рассмотрение результатов разработки и исследований модели троично-симметричного канала передачи двухмерных троичных сигнальных последовательностей.

Известна модель двоично-симметричного канала (рис. 1) [1]. Эта модель подразумевает передачу двоичных последовательностей, образующих двумерный симплекс, представленный двухфазными сигналами с манипуляцией ±π.

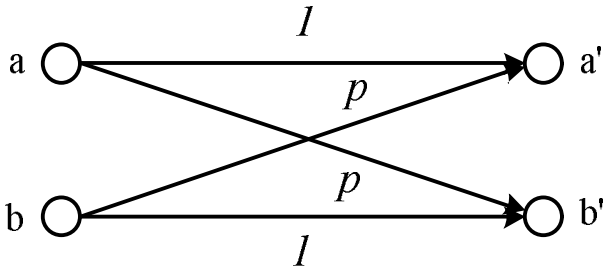


Рис. 1. Модель двоично-симметричного канала передачи информации

Символы a, b – передаваемые, символы a', b' – принимаемые после прохождения канала с шумами (искажениями), а матрица переходных вероятностей представлена в таблице 1.

Таблица 1

Матрица переходных вероятностей

	a'	b'
a	$1-p$	p
b	p	$1-p$

Данная модель сыграла значительную роль в развитии теории передачи дискретных сообщений и теории помехоустойчивого кодирования.

Вероятности ложной тревоги $P_{лт\ дв}$ и правильного приема $P_{пр\ дв}$описываются следующими выражениями:

$$P_{лт\ дв} = \sum_{i=0}^{k} C_n^i 2^{-n}; \quad (1)$$

$$P_{пр\ дв} = \sum_{i=0}^{k} C_n^i p^i (1-p)^{n-i}, \quad (2)$$

где i, k – текущее имаксимальное количество допустимых ошибок при приеме двоичной последовательности;

n – длина двоичной последовательности;

p – вероятность ошибочного символа в канале.

По аналогии с двоично-симметричным каналом можно предложить модель троично-симметричного канала.

Предположим, что по каналу с шумами передаются троичные символы *a, b, c*, образующие правильный симплекс, которые могут быть представлены сигналами с трехфазной манипуляцией: 0; $\frac{2\pi}{3}$; $\frac{4\pi}{3}$. Тогда модель троичного канала передачи информации может быть представлена так, как на рисунке 2.

Символы *a, b, c* – передаваемые, символы a', b', c' – принимаемые после прохождения канала с шумами.

Вероятности правильного приема $Q_{aa'}$, $Q_{bb'}$, $Q_{cc'}$ символов канала по линиям $a-a'$, $b-b'$, $c-c'$ соответствуют вероятностям приема символов a', b', c' при посылке соответственно символов a, b, c. При этом $Q_{aa'}=Q_{bb'}=Q_{cc'}=Q$.

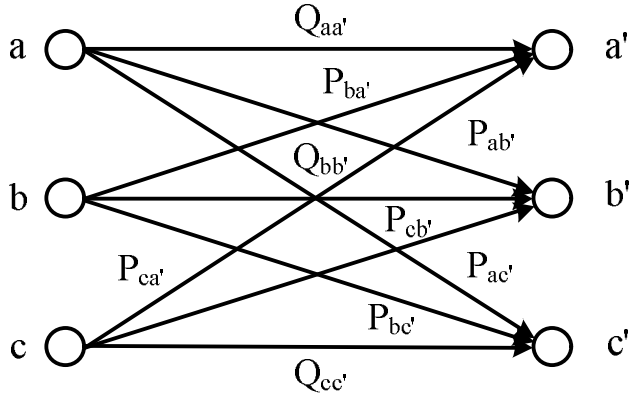


Рис. 2. Модель троичного канала передачи информации

Вероятности ошибочного символа $P_{ab'}$, $P_{ac'}$, $P_{ba'}$, $P_{bc'}$, $P_{ca'}$, $P_{cb'}$в канале по линиям $a–b'$, $a–c'$, $b–a'$, $b–c'$, $c–a'$, $c–b'$соответствуют вероятностям приема символов b', c'вместо a, символов a', c'вместо b, символов a', b'вместо c.

Для троичного канала имеют место следующие соотношения:

$$Q_{aa'}+P_{ab'}+P_{ac'}=1;$$
$$Q_{bb'}+P_{ba'}+P_{bc'}=1;$$
$$Q_{cc'}+P_{ca'}+P_{cb'}=1. \quad (3)$$

Если при этом

$$P_{ab'}=P_{ac'}=P_{ba'}=P_{bc'}=P_{ca'}=P_{cb'}; \quad (4)$$
$$P_{ab'}+P_{ac'}=\text{p};$$
$$P_{ba'}+P_{bc'}=\text{p};$$
$$P_{ca'}+P_{cb'}=\text{p}; \quad (5)$$
$$\text{Q}+\text{p}=1, \quad (6)$$

то модель (см. рис. 2) может рассматриваться как модель троичносимметричного канала, а матрица переходных вероятностей представляется таблицей 2.

Таблица 2

Матрица переходных вероятностей

	a'	b'	c'
a	Q	*p*/2	*p*/2
b	*p*/2	Q	*p*/2
c	*p*/2	*p*/2	Q

Вероятности ложной тревоги $P_{\text{лт тр}}$ и правильного приема $P_{\text{пр тр}}$ описываются соответственно следующими выражениями:

$$P_{\text{лт тр}} = \sum_{i=0}^{i_{\text{макс}}} \sum_{j=0}^{j_{\text{макс}}} \frac{n!}{i!*j!*(n-i-j)!} * 3^{-n}; \quad (6)$$

$$P_{\text{пр тр}} = \sum_{i=0}^{i_{\text{макс}}} \sum_{j=0}^{j_{\text{макс}}} \frac{n!}{i!*j!*(n-i-j)!} * \left(\frac{p}{2}\right)^{i+j} * (1-p)^{n-i-j}, \quad (7)$$

где i, j, $i_{\text{макс}}$, $j_{\text{макс}}$ – текущие и максимальные значения допустимых ошибок соответственно при приеме троичной последовательности ($i_{\text{макс}}+j_{\text{макс}} \leq k$);

n – длина троичной последовательности.

Пропускная способность двоично-симметричного канала с вероятностью ошибки p определяется как [2]

$$C_{дв}(p)=1+p*\log_2 p+(1-p)*\log_2(1-p). \quad (8)$$

Сохраняя аналогию в рассуждениях с (8), можно дать определение пропускной способности троично-симметричного канала (см. рис. 2) с вероятностью ошибки p, которая может быть записана следующим образом:

$$C_{тр}(p)=1+p*\log_3 p+ p*\log_3 p +(1-2p)*\log_3(1-2p) =$$
$$= 1+2p*\log_3 p +(1-2p)*\log_3(1-2p). \quad (9)$$

Графики пропускной способности двоично-симметричного (пунктир) и троично-симметричного (сплошная) каналов представлены на рисунке 3.

Не теряя общности, будем считать для двоично-симметричного канала рабочей зоной изменения p от 0 до 1/2, а для троичного канала – от 0 до 2/3.

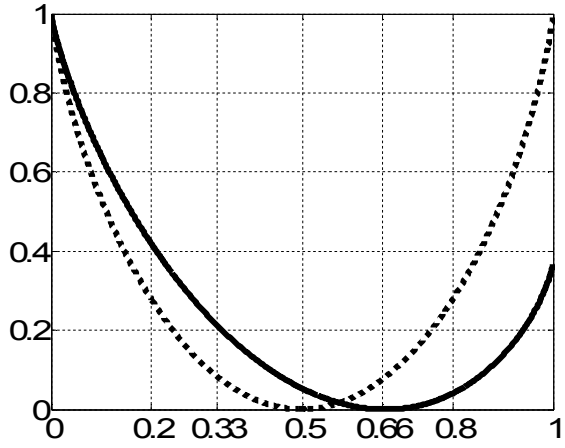


Рис. 3. Графики пропускной способности двоично-симметричного (пунктир) и троично-симметричного (сплошная) каналов

Из рисунка 3 следует, что троично-симметричный канал обладает преимуществом по пропускной способности перед двоично-симметричным.

Таким образом, в статье предложена модель, получены формулы для расчета вероятностных характеристик и определена пропускная способность троично-симметричного дискретного канала передачи информации. Показано, что пропускная способность троично-симметричного канала выше, чем двоично-симметричного.

1. Финк Л.М. Теория передачи дискретных сообщений. – Изд. 2-е, перераб. и доп. – М.: Советское радио, 1970. – С. 728.

2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: [пер. с англ.]. – М.: Связь, 1979. – 744с., ил.

УДК 004.942:621.396.2

Л.А. Евланова, И.Г. Бабанин, В.В. Матвеенко

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА СОЗДАНИЯ МОДЕЛИ УКВ-ПРИЕМНИКА В ПЕРСПЕКТИВНОЙ СРЕДЕ GNURADIO

Рассмотрена методика создания УКВ-приемника на базе перспективной программной среды GNURadio.

Разработка современного УКВ-приемника является сложной, трудоемкой и продолжительной во времени задачей. Данная задача в ходе разработки требует оперативной проверки принятых технических решений как по отдельным блокам и устройствам, так ипо всему радиоприемному тракту в целом. Физическое моделирование в виде лабораторных макетов и опытных образцов требует значительных финансовых, материальных, трудовых и временных ресурсов. Исходя из этого создание имитационных моделей радиоприемных устройств в целом и УКВ-приемников в частности является актуальной задачей.

Целью данной статьи является рассмотрение результатов разработки методики создания модели УКВ-приемника в перспективной среде GNURadio.

На сегодняшний день широкое распространение получила свободно распространяемая программная среда динамического мо-

делирования GNURadio, построенная по технологии Software-Defined Radio(SDR), которая позволяет на программном уровне осуществлять моделирование и разработку радиотехнических систем. Программная часть SDR реализуется программным комплексом GNU Radio. Аппаратная часть SDR может реализовываться с помощью устройств нескольких типов, наиболее распространенными из которых являются устройства, называемые UniversalSoftwareRadioPeripheral (USRP) [1].

Сигналы с ЧМ – это модулированные сигналы, получаемые в результате изменения частоты несущей (амплитуда сигнала и его средняя мощность остаются неизменными).

Для частотно-модулированного сигнала математическая запись имеет следующий вид:

$$U_{\text{чм}} = U_0 \cos(\omega_0 t + M_{\text{чм}} \sin \Omega t + \varphi_0), \quad (1)$$

где U_0, ω_0 – амплитуда, частота несущего колебания соответственно;

$U_{\text{мод}}$, Ω – амплитуда, частота модулирующего колебания соответственно;

$M_{\text{ЧМ}} = \frac{\Delta\omega}{\Omega}$ – коэффициент частотной модуляции.

Преобразуем выражение (1) с целью анализа амплитудного спектра:

$$u_{\text{чм}}(t) = U_0 \cos \omega_0 t + \frac{M_{\text{чм}} U_0}{2} \cos(\omega_0 + \Omega)t - \frac{M_{\text{чм}} U_0}{2} \cos(\omega_0 - \Omega)t. \quad (2)$$

Для узкополосной ЧМ ($M << 1$) в спектре сигнала имеется только несущая и две боковые составляющие.

Для широкополосной УМ ($M >> 1$) имеем

$$\Delta f_{\text{УМ}} \approx 2FM_{\text{ум}} \text{ и } \Delta f_{\text{ЧМ}} \approx 2\Delta f_{\max}, \quad (3)$$

т.е. ширина спектра при ЧМ равна удвоенной величине девиации частоты и не зависит от частоты модуляции F. Этот случай представляет основной практический интерес, так как при больших M помехоустойчивость УМ существенно выше [2].

На основе данных математических выражений, а также с учетом особенностей формирования и обработки сигналов цифровыми методами можно представить GNURadio-модель радиоприемного устройства УКВ-диапазона (рис. 1).

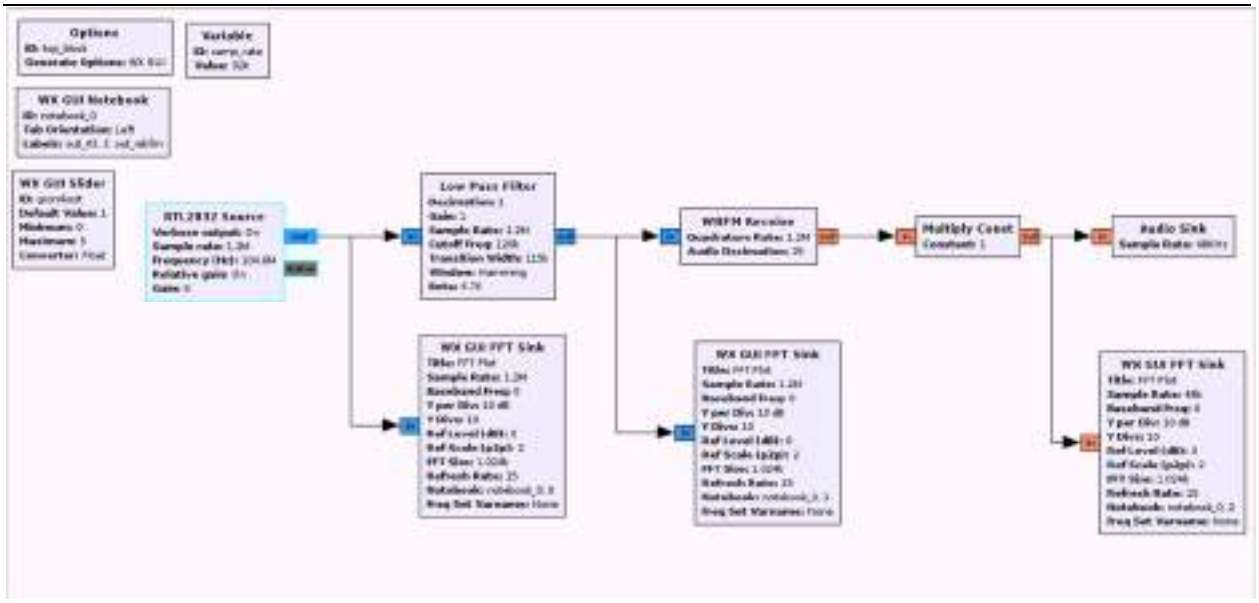


Рис. 1. GNURadio-модель устройства приема FM-сигналов

В состав данной модели входят следующие блоки:

– радиопереферия (RTL2832 Source);

– фильтр низких частот (Lowpassfilter);

– усилитель звуковой частоты (Multiplyconst);

– устройство воспроизведения звука (Audiosink);

– спектроанализатор (WXGUIFFTSink).

Входную цепь представляет собой фильтр, который осуществляет частотную избирательность. Широкополосный детектор осуществляет детектирование. Усилитель частоты модуляции усиливает радиосигнал до уровня, необходимого для нормальной работы оконечного устройства, а также осуществляет последетекторную фильтрацию шумов и помех, лежащих за пределами полосы пропускания.

Работоспособность данной модели проверена на практике. В качестве оконечного устройства использован приемник RTL2832U+E4000, который работает в диапазоне частот от 60 до 2200 МГц. Подключение к компьютеру осуществляется через высокоскоростной USB интерфейс.

На представленных частотах в г.Курске вещают следующие радиостанции (рис. 2):

– 102.9 МГц – радио «Маяк» (Вести);

– 103.7 МГц – радио «Курс»;

– 104.1 МГц – «Европа плюс».

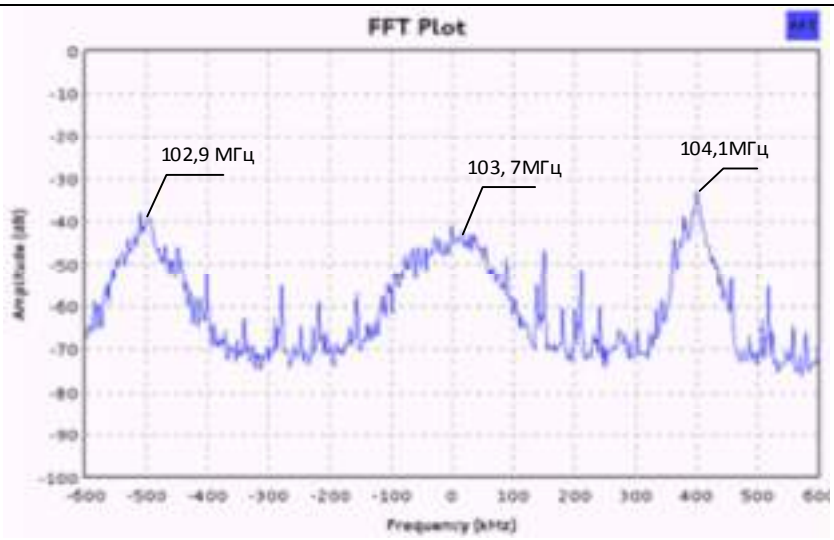


Рис. 2. Спектр сигнала на выходе оконечного устройства

На рисунке 3 представлен спектр сигнала на выходе фильтра, который осуществляет частотную избирательность.

Частотная избирательность количественно характеризует способность приемника выделять из всех радиочастотных колебаний и радиопомех, действующих на его входе, радиочастотный сигнал, соответствующий частоте настройки приемника (103,7МГц).

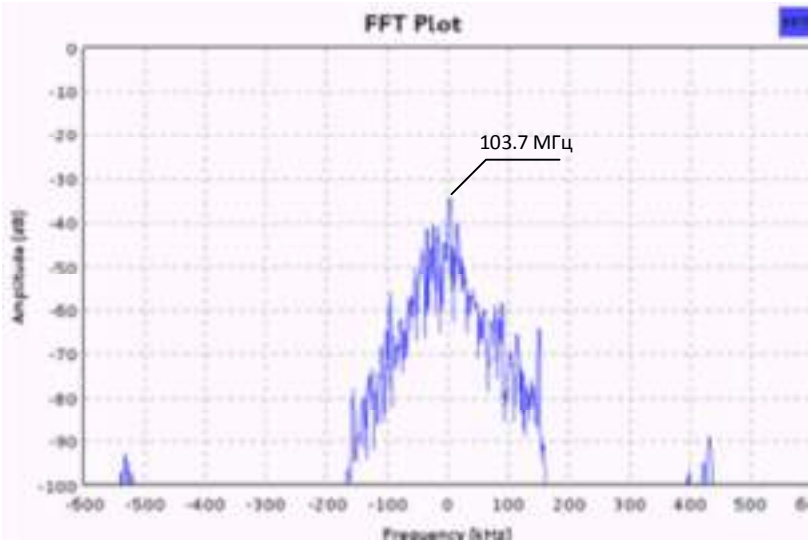


Рис. 3. Спектр сигнала на выходе фильтра низких частот

На рисунке 4 представлен спектр сигнала на выходе демодулятора, который представляет собой речевой сигнал, поступающий и воспроизводимый устройством воспроизведения звука.

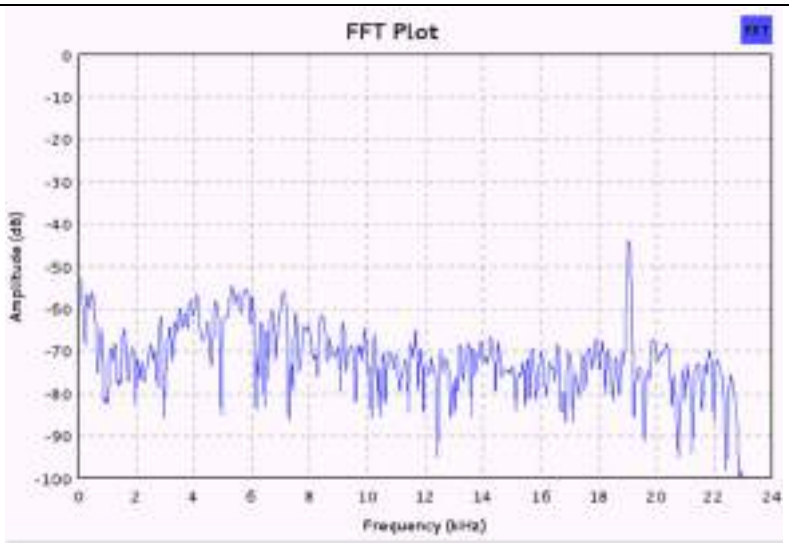


Рис. 4. Спектр сигнала на выходе демодулятора

Таким образом, рассмотренная модель УКВ-приемника в перспективной среде GNURadio является адекватной радиотехническим процессам, происходящим в нем, и позволяет производить оперативную разработку современных радиоприемных устройств при незначительных финансовых, материальных, трудовых и временных ресурсах.

---

1. WelcometoGNURadio! [Electronic resource] / GNURadiohttp. – URL: http://gnuradio.org/redmine/projects/gnuradio/wiki.

2. Лукьянюк С.Г., Потапенко А.М. Теория электрической связи. Сигналы, помехи и системы передачи: учебник / Юго-Зап. гос. ун-т. – Курск, 2012. – 223 с.

УДК 004.942: 621.396.2

А.Н. Замыцкий[2], В.В. Матвеенко[2], И.С. Собе-Панек[1]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) ФГУП «18 ЦНИИ» МО РФ

ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ ПРИЕМНОГО ТРАКТА ШИРОКОПОЛОСНЫХ СИГНАЛОВ ПРИ ВОЗДЕЙСТВИИ УЗКОПОЛОСНЫХ ПОМЕХ

Рассмотрены результаты исследования помехоустойчивости приемного тракта широкополосных сигналов при воздействии узкополосных помех.

Широкое использование метода прямого расширения спектра позволяет значительно повысить помехозащищенность радиоприемных устройств средств связи. Вместе с тем в состав подобных устройств входят высокочастотные тракты, имеющие широкие полосы пропускания и не способные на фоне приема полезных сигналов эффективно подавлять различного рода помехи, как широкополосные, так и узкополосные. Усложнение современной радиоэлектронной обстановки предъявляет более высокие требования к указанным трактам радиоприемных устройств, среди которых задача повышения помехоустойчивости широкополосных трактов является наиболее актуальной.

Целью настоящей статьи является рассмотрение результатов исследования помехоустойчивости приемного тракта широкополосных сигналов (ШПС) при воздействии узкополосных помех.

Структурная схема радиоприемного устройства для приема ШПС представлена на рисунке 1.

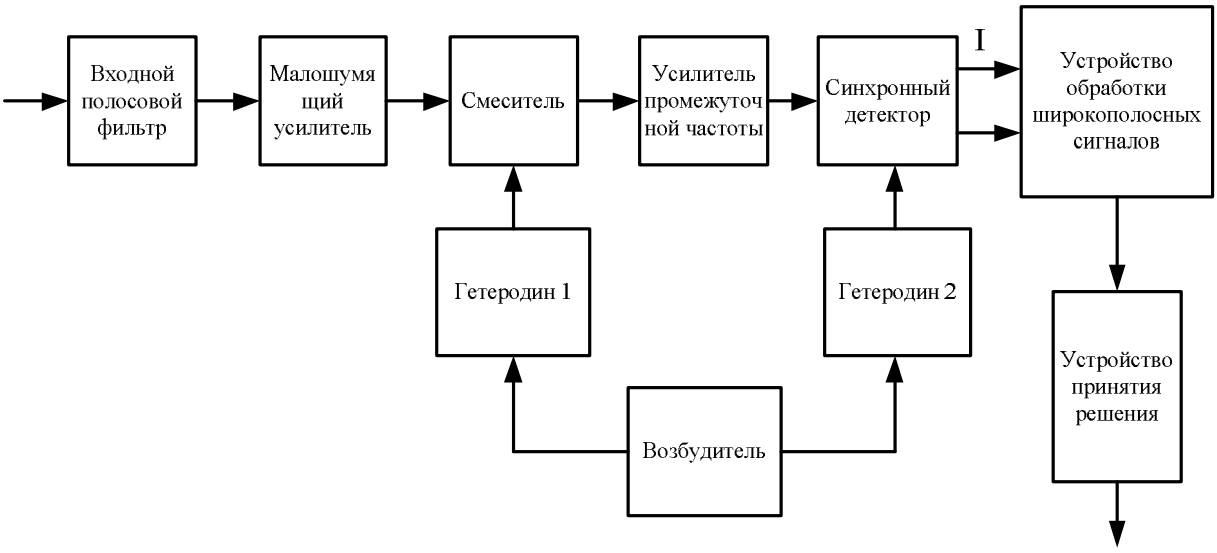


Рис. 1. Структурная схема радиоприемного устройства для приема ШПС

Основными элементами, обеспечивающими помехоустойчивость радиоприемного устройства, являются: входной полосовой фильтр, усилитель промежуточной частоты и устройство обработки широкополосных сигналов. Однако, поскольку сквозная полоса всего высокочастотного тракта должна быть согласована с широким спектром ШПС, вероятность попадания в него помех, среди которых и узкополосные, достаточно велика.

В ходе исследования данного тракта (см. рис. 1) была создана модель в программной среде MATLAB, в которую наряду с ШПС (манипулированный по фазе 11-позиционным кодом Баркера радиосигнал) введены три узкополосные помехи (гармонические колебания на разных, близко расположенных частотах), аддитивно воздействующие на сигнал в его полосе.

Математически данная модель может быть описана следующим выражением [1]:

$$u(t) = \sum_{n=1}^{N} a_n u_0[t-(n-1)\tau_0]\, cos\omega_0 + b_1 cos\omega_1 t + \\ + b_2 cos\omega_2 t + b_3 cos\omega_3 t, \quad (1)$$

где N – количество парциальных прямоугольных импульсов широкополосного сигнала;

u_0 – парциальный прямоугольный импульс;

a_n – амплитуда парциального импульса;

$(n-1)\tau_0$ – временной сдвиг парциального импульса;

b_1, b_2, b_3 – амплитуды 1-й, 2-й и 3-й узкополосных помех соответственно;

ω_0, ω_1, ω_2, ω_3 – несущие частоты широкополосного сигнала и узкополосных помех соответственно.

Спектр аддитивной смеси (1) может быть представлен как

$$S(\omega)=\int_{-\infty}^{\infty} u(t)\, e^{-i\omega t} dt = S_{\text{сигн}} + S_{\text{пом1}} + S_{\text{пом2}} + S_{\text{пом3}}, \quad (2)$$

где $S_{\text{сигн}}$, $S_{\text{пом1}}$, $S_{\text{пом2}}$, $S_{\text{пом3}}$ – спектры ШПС и узкополосных помех (1) соответственно.

На рисунке 2 представлены графики результата воздействия на приемный тракт ШПС трех узкополосных помех.

На графике *а*) изображен ШПС (манипулированный по фазе 11-позиционным кодом Баркера), график *б*) отражает его свертку, из графика *в*) очевиден результат суммирования сигнала и трех помех, на графике *г*) представлен суммарный спектр ШПС и трех помех, график *д*) показывает свертку ШПС и одной помехи, график *е*) демонстрирует свертку ШПС и трех узкополосных помех. Данные результаты получены при отношении помеха/сигнал=1/1 для каждой из трех помех.

Из рисунка 2 очевидно, что узкополосные помехи подавляют ШПС при незначительном отношении помеха/сигнал.

На основе полученных результатов можно сделать традиционный вывод о необходимости смены несущей частоты ШПС или сужении полосы его спектра. Однако система связи с ШПС обладает повышенной скрытностью именно за счет расширенного спектра, что является ее несомненным достоинством, поэтому сделанный вывод не может быть удовлетворительным. Тогда необходимо применить известный, но еще не получивший достаточно широкого распространения метод режекции помех в широкополосных радиоприемных трактах. Он основывается на использовании блоков режекторных фильтров [2] как в линейной части приемника, так и после смесителя и АЦП на промежуточной частоте.

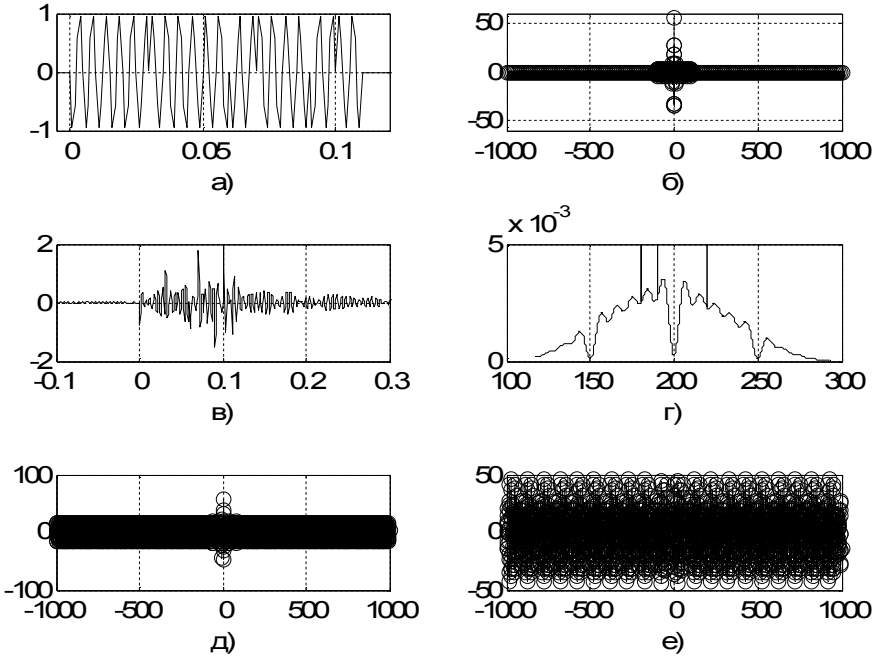


Рис. 2. Графики результата воздействия на приемный тракт ШПС трех узкополосных помех

На рисунке 3 представлена структурная схема радиоприемного устройства для приема ШПС повышенной помехоустойчивости.

В данной структурной схеме введены два блока аналоговых и цифровых режекторных фильтров, управляемых устройством принятия решения. Назначение аналоговых режекторных фильтров – подавление мощных узкополосных помех до смесителя. В данном случае они обеспечивают максимальный динамический диапазон в условиях сильных помех. Вместе с тем такого рода фильтры трудно реализуемы, обладают невысокими фильтрационными свойствами, громоздки, сложны в управлении и имеют грубые настройки.

Цифровые фильтры используются для устранения узкополосных помех, превышающих допустимое отношение помех/сигнал. Такие фильтры легко реализуемы, обладают высокими фильтрационными свойствами, управляются программно и могут быть настроены прецизионно.

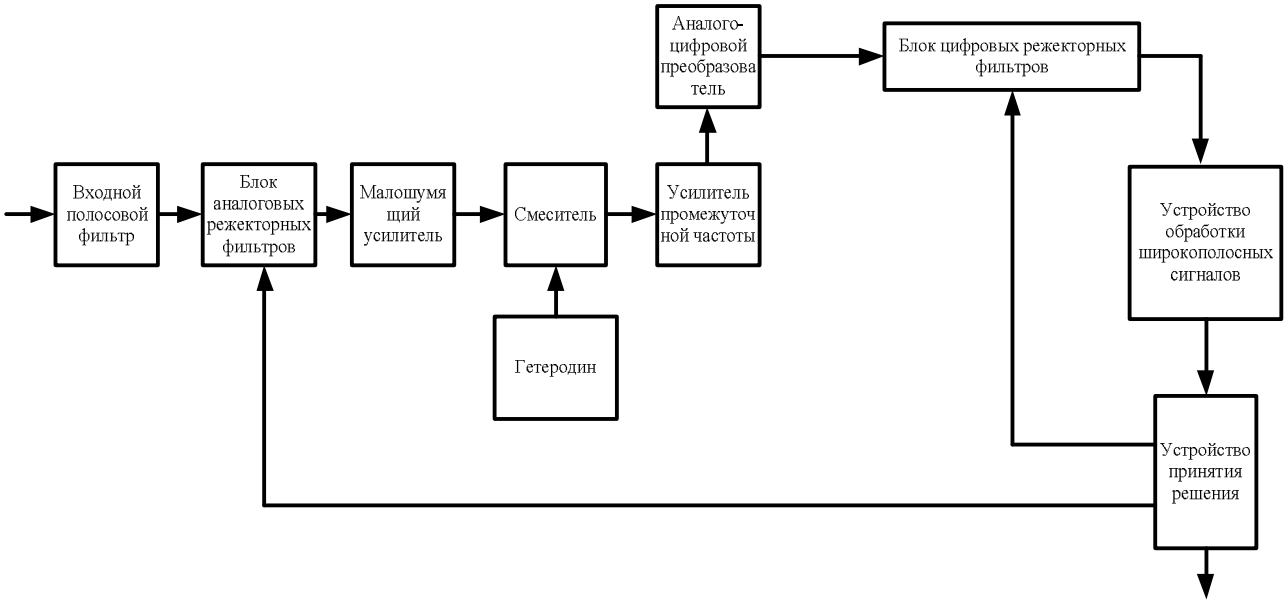


Рис. 3. Структурная схема радиоприемного устройства для приема ШПС повышенной помехоустойчивости

В ходе исследования тракта (см. рис. 3) была создана его модель в программной среде MATLAB, где введены режекторные фильтры через функции

```
[b,a]=cheby1(5,1,[218,222]/500,'stop');   (3)
q=filter(b,a,G3).                         (4)
```

Функция (3) описывает фильтр Чебышева 1-го рода 5-го порядка. Аналогичные функции могут описывать фильтры Баттерворта, Бесселя, эллиптические и другие. Функция (4) применяет функцию (3) для фильтрации.

Сигнал, прошедший через блоки режекторных фильтров, может быть представлен как

$$u_{\text{реж}}(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} S(\omega)K_{\text{анал}}(\omega)\,K_{\text{цифр}}(\omega)e^{i\omega t}d\omega, \qquad (5)$$

где $K_{\text{анал}}(\omega)$, $K_{\text{цифр}}(\omega)$ – коэффициенты передачи аналогового и цифрового блоков режекторных фильтров соответственно.

На рисунке 4 представлены графики результата воздействия на приемный тракт ШПС трех узкополосных помех и их режекции с помощью режекторных фильтров. На графиках (рис. 4, *а – г*) представлены ШПС, его свертка, аддитивная смесь (1), суммарный спектр (2) соответственно, режектированный спектр (рис. 4, *д*) и свертка очищенного сигнала (рис. 4, *е*). Данные результаты получены при отношении помеха/сигнал=1000/1 для каждой из трехпомех.

Из рисунка 4 видно, что при режектировании узкополосных помех, даже при значительном отношении помеха/сигнал, осуществляется уверенный прием сигнала (см. рис. 4, *е*). Вместе с тем наблюдается некоторое снижение его корреляционного пика (см. рис. 4, *е*) примерно в 2,5 раза, что объясняется режектированием некоторой доли спектральных составляющих самого сигнала.

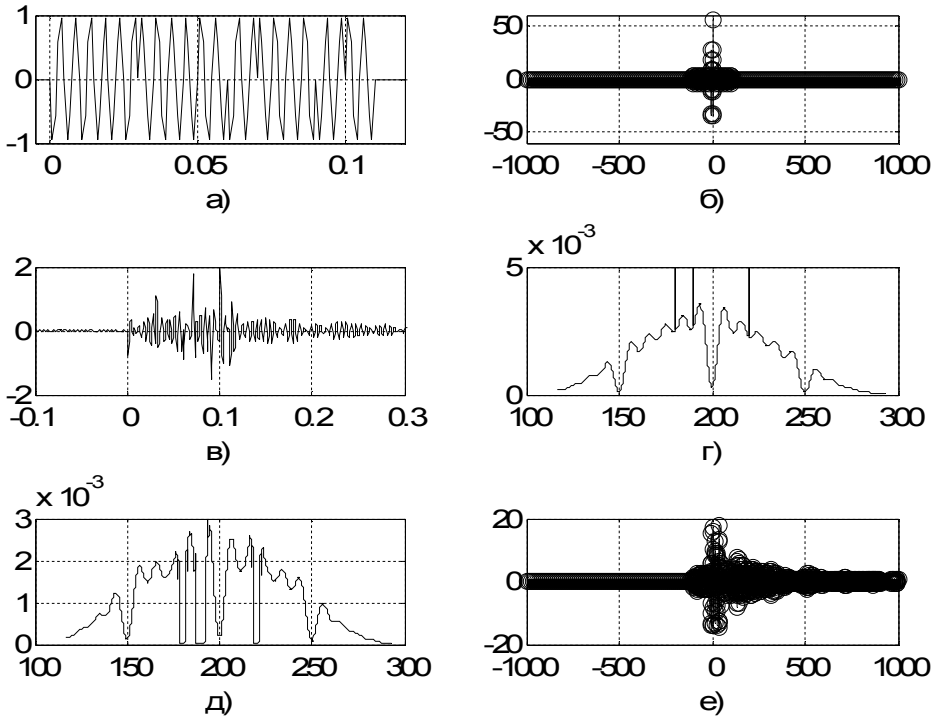


Рис. 4. Графики результата воздействия на приемный тракт ШПС трех узкополосных помех и их режекции с помощью режекторных фильтров

Таким образом, в результате исследования приемного тракта ШПС при воздействии узкополосных помех предложены модели помеховой обстановки и помехоустойчивого широкополосного тракта, рассмотрены результаты его функционирования и даны оценки помехоустойчивости.

Рассмотренный помехоустойчивый тракт позволяет осуществлять устойчивый прием ШПС в условиях воздействия множества мощных узкополосных помех.

---

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с., ил.

2. Бабанин И.Г., Матвеенко В.В., Шиленков Е.А. Способ построения быстродействующих цифровых фильтров для защиты широкополосных цифровых устройств // Актуальные проблемы инфотелекоммуникаций: матер. III Регион. науч.-практ. конф. / редкол.: А.М. Потапенко (отв. ред.) [и др]; Юго-Зап. гос. ун-т. – Курск, 2011. – 150с.

УДК 004.942: 621.396.2

А.Н. Замыцкий[2], В.В. Матвеенко[2], И.С. Собе-Панек[1]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) ФГУП «18 ЦНИИ» МО РФ

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СИГНАЛЬНО-ПОМЕХОВОЙ ОБСТАНОВКИ В ПРОГРАММНОЙ СРЕДЕ MATLAB

Рассмотрены результаты разработки имитационной модели сигнально-помеховой обстановки в программной среде MATLAB. Модель предусматривает создание аддитивной смеси сигнала, шумовой, узкополосных и импульсных помех с возможностью изменения их энергетических, временных и частотных параметров в соответствии с требованиями для проверки широкополосных трактов радиоприемных устройств.

Условия современной телекоммуникационной связи характеризуются сложной сигнально-помеховой обстановкой. При построении широкополосных трактов радиоприемных устройств для данных условий возникает необходимость оценки их устойчивости к воздействию интенсивных помех разного рода. Создание реальной сигнально-помеховой обстановки требует значительных финансовых, трудовых, временных и аппаратурных затрат. Исходя из этого задача разработки имитационных моделей такой обстановки является актуальной.

Целью настоящей статьи является рассмотрение результатов разработки имитационной модели сигнально-помеховой обстановки в программной среде MATLAB.

В полосе реального широкополосного тракта наряду с полезными сигналами действуют различного рода помехи. К ним могут быть отнесены такие, как шумовые, узкополосные, импульсные. На входе тракта суммарное их воздействие может быть описано аддитивной смесью с полезным сигналом:

$$\mathrm{v}(t)=\mathrm{u}(t)+\mathrm{q}(t)+a_1(t)+a_2(t)+\ldots+a_k(t)+b_1(t)+ +b_2(t)+\ldots+b_n(t), \quad (1)$$

где $u(t)$ – полезный сигнал;

$q(t)$ – шумовая гауссова помеха;

$a_1(t)$, $a_2(t)$, $a_k(t)$, − узкополосные помехи;

$b_1(t)$, $b_2(t)$, $b_n(t)$ − импульсные помехи;

k – количество узкополосных помех;

n – количество импульсных помех.

Выражение (1) является математической моделью сигнально-помеховой обстановки, которая может быть положена в основу имитационной модели.

Полезный сигнал $u(t)$в обобщенном виде может быть представлен как [1]

$$\mathrm{u}(t)=A_m(t)\cos\big(\omega t+\varphi(t)\big), \quad (2)$$

где $A_m(t)$ – амплитуда, изменяющаяся во времени;

ω – несущая частота;

$\varphi(t)$ – фаза, изменяющаяся во времени.

Задавая функцию $A_m(t)$, можно получить амплитудную или импульсную модуляцию. Функция $\varphi(t)$ позволяет получить разные виды угловой модуляции: частотную или фазовую.

В программной среде MATLAB сигнал (1) с амплитудной и угловой модуляцией может быть легко представлен в тех же символах [2, 3]. Для формирования сигнальных импульсных последовательностей используется функция

y1=pulstran(t,d1,'rectpuls',tau), (3)

где d1 – задержка, с помощью которой можно задавать период следования импульсов;

'rectpuls' – функция генерации прямоугольного импульса;

tau – длительность импульса.

Шумовая гауссовая помеха $q\,(t)$ реализуется с помощью функции

$$\text{randn(size(t))}, \tag{5}$$

Данная помеха присутствует в любом радиоприемном тракте, и ее воздействие проявляется тем сильнее, чем меньше мощность сигнала на входе и ниже порог обнаружения.

Узкополосные помехи $a_1(t)$, $a_2(t)$,…$a_k(t)$можно представить как гармонические колебания устанавливаемого уровня:

$$a_k(t)=A_{mk}cos(\omega_k t), \tag{6}$$

где A_{mk}, ω_k – амплитуда и несущая частота k-й узкополосной помехи.

Каждая из данных помех может отличаться как по амплитуде, так и по несущей частоте.

В программной среде MATLAB выражение (6) описывается в тех же символах.

Импульсные помехи $b_1(t)$, $b_2(t)$,…$b_n(t)$представляются как

$$b_n(t)=B_{mn}cos(\omega_n t), \tag{7}$$

где B_{mn}, ω_n – амплитуда и несущая частота n-й импульсной помехи.

Каждая из данных помех может отличаться как по амплитуде, так и по несущей частоте, по длительности и по периоду следования, по временному положению относительно сигнала.

Для формирования помеховых импульсных последовательностей также используется функция (3).

На рисунке 1 представлены графики радиосигнала (*а*), гауссовой помехи (*б*), импульсной радиопомехи (*в*), узкополосных радиопомех с разными амплитудами и частотами (*г*, *д*), суммарной функции (*е*). Из данного рисунка видно, что имитационные модели рассматриваемых радиосигнала и радиопомех удовлетворительно воспроизводятся функциями MATLAB и позволяютпроизводить изменения их энергетических, временных и частотных параметров, что представляет значительный интерес для проверки широкополосных трактов радиоприемных устройств.

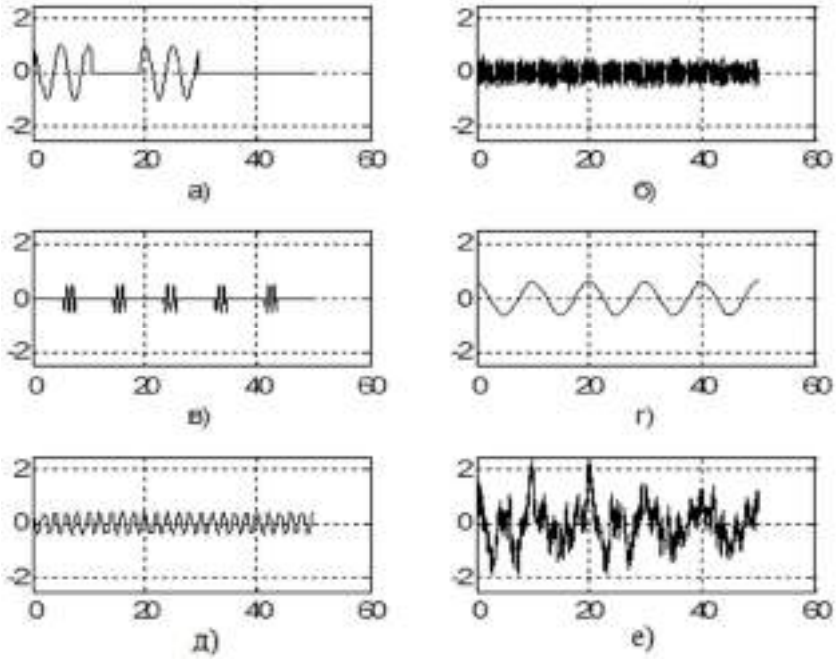


Рис. 1. Графики: *а* – сигнала; *б* – гауссовой помехи; *в* – импульсной помехи; *г*, *д* – узкополосных помех с разными амплитудами и частотами; *е* – суммарной функции (1)

Для спектра как сигналов, так и помех справедливо соотношение

$$S(\omega)=\int_{-\infty}^{\infty} s(t)e^{-i\omega t}dt, \qquad (8)$$

где $s(t)$ – функция, определяющая сигнал или помеху во временной области,

ω – круговая частота.

Так как преобразование Фурье является линейным [1], то суммарной функции (1) соответствует спектр

$$S_{\text{v}} = S_u + S_q + S_{a1} + S_{a2} + S_{ak} + S_{b1} + S_{b2} + S_{bn}, \qquad (9)$$

где S_u, S_q, S_{a1}, S_{a2}, S_{ak}, S_{b1}, S_{b2}, S_{bn} – спектральные характеристики сигнала, гауссовой, узкополосной и импульсной помех соответственно.

В программной среде MATLAB суммарная спектральная характеристика (9) может быть представлена следующей функцией:

$$S_{\text{v}} = \text{fft}(v,\text{h});$$
$$\text{pyy1} = S_v.*\text{conj}(S_v)/\text{h};$$
$$\text{f=c*(f1:f2)/h}, \qquad (10)$$

где fft–функция преобразования Фурье;

руу1 – функция отображения спектра;

h – частота дискретизации;

f – функция задания области отображения на частотной оси;

f_1, f_2–интервал частот отображения;

c – масштабирующий множитель для оси частот.

На рисунке 2 представлен график суммарной спектральной характеристики (9) сигнала, гауссовой, узкополосной и импульсной помех.

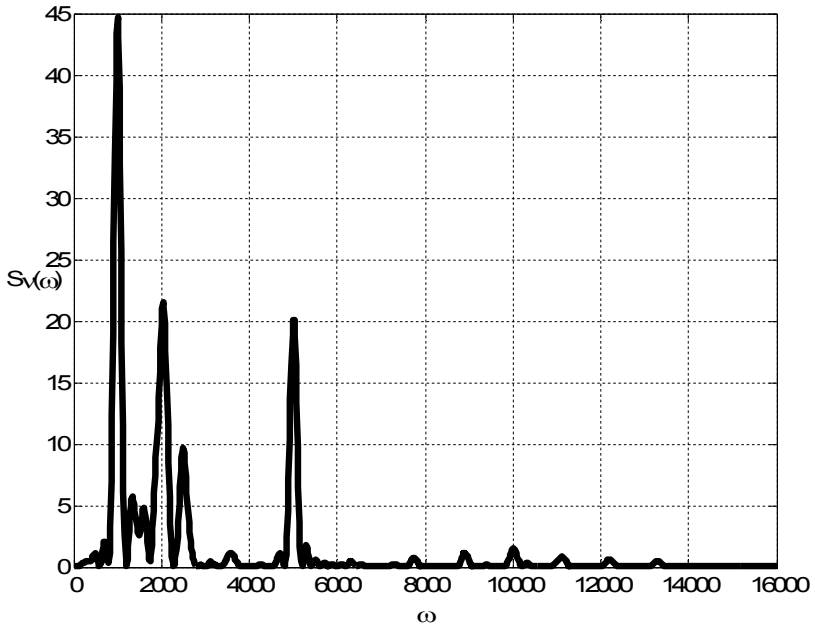


Рис. 2. График суммарной спектральной характеристики сигнала, гауссовой, узкополосной и импульсной помех

Из данного рисунка видно, что имитационная модель спектральной характеристики (9) удовлетворительно воспроизводится функциями MATLAB и позволяет определять несущую частоту, полосу и амплитуду спектра как сигнала, так и помех для последующей их селекции или режекции в широкополосном тракте радиоприемного устройства.

Таким образом, разработана имитационная модель сигнально-помеховой обстановки в программной среде MATLAB, представляющей аддитивную смесь полезного сигнала, шумовой, узкополосных и импульсных помех и позволяющей адекватно отражать их энергетическую, частотную и временную структуру и производить оперативные изменения в соответствии с требованиями для проверки широкополосных трактов радиоприемных устройств.

Список литературы

1. Баскаков С.И. Радиотехнические цепи и сигналы: учеб. для вузов по спец. «Радиотехника».– 3-е изд., перераб. и доп.– М.: Высш. шк., 2000. – 462 с.: ил.

2. Дьяконов В.П. MATLAB и SIMULINK для радиоинженеров. – М.: ДМК Пресс, 2011. – 976 с.: ил.

3. Рудаков П.И., Сафонов И.В. Обработка сигналов и изображений. MATLAB 5.x / под общ. ред. В.Г. Потемкина. – М.: ДИАЛОГ – МИФИ, 2000. – 416 с. – (Пакеты прикладных программ; Кн. 2).

УДК 004.942: 621.396.2

А.Н. Замыцкий[2], В.В. Матвеенко[2], А.А. Спашко[1]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) ФГУП «18 ЦНИИ» МО РФ

ИМИТАЦИОННАЯ МОДЕЛЬ ОЦЕНКИ ПОМЕХОУСТОЙЧИВОСТИ КОМАНДЫ УПРАВЛЕНИЯ НА ОСНОВЕ ПРОГРАММНОЙ СРЕДЫ MATLAB

Рассмотрены результаты исследования возможности построения имитационной модели оценки помехоустойчивости команды управления на основе программной среды MATLAB.

Проектирование командных радиолиний управления предполагает их проверку в реальных физических условиях и получение необходимых вероятностных характеристик приема при воздействии различного рода помех. Вместе с тем результаты подобных проверок могут потребовать соответствующих исследований структуры команды и ее доработки с целью повышения помехоустойчивости.Данная процедура требует значительных временных, финансовых, материальных и трудовых затрат. В связи с этим задача создания имитационных моделей оценки помехоустойчивости команд управления очень актуальна.

Целью настоящей статьи является рассмотрение результатов исследования возможности построения имитационной модели оценки помехоустойчивости команды управления на основе программной среды MATLAB.

Основными вероятностными характеристиками при приеме команд управления являются вероятности ложной тревоги $P_{лт}$ и правильного приема $P_{пр}$. Плотности распределения вероятности $f_{X,\sigma}(x)$ нормального гауссового шума и аддитивной его смеси с сигналом $f_{x,\sigma}(x+X)$ описываются соответственно следующими выражениями (рис. 1):

$$f_{x,\sigma}(x)= \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x)^2}{2\sigma^2}}; \quad (1)$$

$$f_{x,\sigma}(x+X)= \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-X)^2}{2\sigma^2}}, \quad (2)$$

где x, σ – текущее и среднеквадратическое значения шумовой выборки соответственно;

X–пиковое значение сигнала.

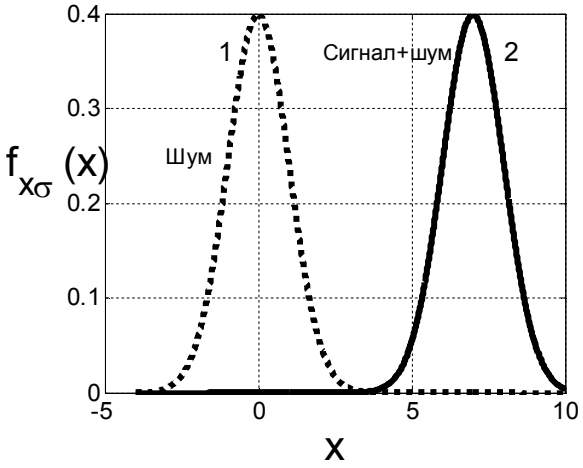


Рис. 1. Плотности распределения вероятности нормального гауссового шума и его аддитивной смеси с сигналом

Вероятность ложной тревоги устанавливается при отсутствии сигнала с помощью порога обнаружения $u_{пор}$ и определяется с учетом (1) интегралом ошибок:

$$P_{лт}=\frac{1}{\sigma\sqrt{2\pi}} \int_{u_{пор}}^{-\infty} e^{-\frac{x^2}{2\sigma^2}} dx. \quad (3)$$

Вероятность правильного приема определяется для сигнала при установленном пороге $u_{пор}$ и также может быть рассчитана с учетом (2) с помощью интеграла ошибок:

$$P_{по}=\frac{1}{\sigma\sqrt{2\pi}} \int_{u_{пор}}^{-\infty} e^{-\frac{(x-X)^2}{2\sigma^2}} dx. \quad (4)$$

Выражения (3), (4) дают возможность произвести достаточно точные теоретические расчеты. Вместе с тем интенсивность шумов σ или сигнала X может меняться, что оказывает влияние на вероятностные характеристики $P_{\text{лт}}$ и $P_{\text{по}}$.

При разработке структуры помехоустойчивой команды используются помехоустойчивые последовательности и коды. В данном случае целесообразно исследовать помехоустойчивость команды при ее прохождении через канал распространения. Это потребует физической реализации приемопередающей аппаратуры, канала распространения и источников помех и, соответственно, значительных временных, финансовых, материальных и трудовых затрат.

Одним из эффективных способов упрощения и удешевления подобного рода исследований является разработка имитационных моделей.

Имитационная модель для получения вероятности ложных тревог (рис. 2) должна включать: генератор гауссовых шумов, блок установки порога обнаружения и блок подсчета количества шумовых выбросов n, превысивших порог обнаружения $u_{\text{пор}}$, на интервале наблюдения T, блок расчета вероятности ложной тревоги. Отношение выбросов n к количеству отсчетов N на интервале наблюдения T соответствует вероятности ложной тревоги, т.е.

$$P_{\text{лт}} = \frac{n}{N}. \qquad (5)$$

Рис. 2. Структурная схема имитационной модели расчета вероятности ложных тревог

Генерация нормального гауссового шума в программной среде MATLAB реализуется с помощью функции randn(size(x)). При организации цикла с проверкой на условие превышения порога можно произвести подсчет количества ложных выбросов и рассчитать $P_{\text{лт}}$.

Рис. 3. Структурная схема имитационной модели расчета вероятности правильного приема

Имитационная модель для получения вероятности правильного приема (рис. 3) должна включать: формирователь сигналов команды, генератор гауссовых шумов, аналогичный предыдущей модели, формирователь аддитивной смеси сигнал + шум, блок установки порога обнаружения, блок подсчета числа принятых импульсных сигналов m, превысивших порог обнаружения $u_{\text{пор}}$, на интервале наблюдения T, блок расчета вероятности правильного приема. Отношение числа сигналов m, превысивших порог обнаружения, к количеству переданных сигналов M соответствует вероятности правильного приема:

$$P_{\text{по}}=\frac{m}{M}. \qquad (6)$$

Формирователь команды в программной среде MATLAB реализуется с помощью функции

pulstran(t,d1,'rectpuls',tau),

где t – вектор отсчетов;

d1 – вектор задержек;

'rectpuls' – функция формирования прямоугольного импульса;

tau – вектор длительности импульсов.

Модели (см. рис. 2, 3) должны функционировать совместно. Для их работы в программной среде MATLAB имитируется помехоустойчивая команда управления и задаются величины σ; $\frac{u_{\text{пор}}}{\sigma}=k$; $\frac{x}{\sigma}=w$, где k и w – коэффициенты, характеризующие превышение напряжений порога и пикового значения сигнала над среднеквадратическим значением шума (отношение сигнал/шум).

Адекватность разработанных моделей проверена с помощью выражений (3), (4). В таблице представлены результаты моделирования и расчета при различных значениях порога обнаружения k и отношения сигнал/шум w.

Величина порога обнаружения $k(\sigma)$	Отношение сигнал/шум $w(\sigma)$	$P_{лт}$ расчетное	$P_{лт}$ модели	$P_{по}$ расчетное	$P_{по}$ модели
2	4	$2{,}28\cdot10^{-2}$	$2{,}5\cdot10^{-2}$	0,977	0,98
3	5	$1{,}3\cdot10^{-3}$	$1{,}5\cdot10^{-3}$	0,977	0,97
4	6	$3{,}17\cdot10^{-5}$	$3{,}69\cdot10^{-5}$	0,977	0,978
5	7	$2{,}87\cdot10^{-7}$	$3\cdot10^{-7}$	0,977	0,98
5,2	8	$9{,}96\cdot10^{-8}$	$1\cdot10^{-7}$	0,997	0,998

Таким образом, получена и исследована имитационная модель оценки помехоустойчивости команды управления на основе программной среды MATLAB, позволяющая в реальном времени производить проектирование командных радиолиний управления.

1. Лезин Ю.С. Оптимальные фильтры и накопители импульсных сигналов. – Изд. 2-е, перераб. и доп. – М.: Советское радио, 1969. − 448 с.

2. Дьяконов В.П. MATLAB и SIMULINK для радиоинженеров. – М.: ДМК Пресс, 2011. – 976 с.: ил.

УДК 004.942; 621.396.2

А.Н. Замыцкий, Л.А. Евланова, И.Г. Бабанин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ТРАДИЦИОННОГО СПОСОБА МОДЕЛИРОВАНИЯ РАДИОТЕХНИЧЕСКИХ СИСТЕМ И ПЕРСПЕКТИВНОГО НА ОСНОВЕ ПРОГРАММНОЙ СРЕДЫ GNURADIO

Рассмотрены способы моделирования радиотехнических систем, производится их сравнительный анализ.

Современные способы реализации радиосистем можно разделить на две основные группы: традиционная аппаратурная (то есть технические характеристики аппаратуры определяются схемотехническими решениями) и цифровая (так называемое программно-зависимое радио или SDR – SoftwareDefinedRadiosystem). Каждая

из данных групп обладает достоинствами и недостатками. Вместе с тем, как аппаратурные, так и программно реализуемые решения требуют на этапе разработки моделирования, которое позволяет значительно сократить время и повысить качество разработки. Исходя из этого исследование новых способов моделирования радиотехнических систем является актуальной задачей.

Целью настоящей статьи является рассмотрение традиционного (аппаратного) и перспективного (на основе программной среды GNUradio) способов моделирования радиотехнических систем и сравнительная их характеристика.

Традиционный способ моделирования включает ряд этапов, требующих денежных средств, материалов, элементной базы, квалифицированного персонала, универсального оборудования.

На первом из данных этапов осуществляется выбор и обоснование методов разработки и конструирования радиоэлектронного устройства, его компоновочной схемы.

На втором этапе производится выбор и обоснование применяемой элементной базы. На данном этапе выбирается тип и размер радиоэлемента, удовлетворяющий требуемым электри-ческим характеристикам, устойчивости к механическим и климатическим воздействиям.

На третьем этапе осуществляется разработка конструкции блока, печатного узла и расчет массогабаритных показателей. Разработка конструкции печатного узла включает установку электрорадиоэлементов на печатную плату с учетом их особенностей. Разработка конструкции печатной платы включает выбор метода изготовления. Технологический процесс разработки и изготовления печатной платы комбинированным позитивным методом достаточно трудоемкий и продолжительный и состоит из множества операций.

На четвёртом этапе осуществляется выбор, обоснование и разработка способов электромонтажа, соединений модулей, обоснование способов защиты конструкции изделия и разработка деталей несущих конструкций.

На пятом этапе выполняется изготовление составных частей изделия, их сборка, испытания и оценка качества.

Очевидно, что все перечисленные этапы традиционного способа моделирования достаточно дороги, трудоемки и продолжительны по времени.

Концепция SDR позволяет переместить значительную часть обработки сигналов от аппаратуры в программное обеспечение, что придает радиосистеме большую гибкость. Это концепция, при которой некоторые аппаратно-реализуемые блоки радиосистемы заменяются программно-реализуемыми, это позволяет переместить реализацию существенного объема обработки сигналов из аппаратурной части в программную, что придает радиосистеме значительную универсальность и гибкость [1].

Программная часть SDR может быть реализована на основе перспективного программного комплекса GNURadio. Данный комплекс является свободным программным инструментарием для разработки программного обеспечения радиоустройств. Аппаратная часть при этом может реализовываться с помощью устройств, называемых UniversalSoftwareRadioPeripheral (USRP).

Сигнал, принятый антенной, попадает на плату USRP, на которой размещены малошумящий усилитель, усиливающий сигнал, и преобразователь частоты, понижающий рабочую частоту до промежуточной. Преобразование аналоговой формы сигнала в цифровую производится в АЦП (обратное преобразование – в ЦАП). Дальнейшая цифровая обработка производится с помощью программного комплекса GNURadio в компьютере [2] (рис.).

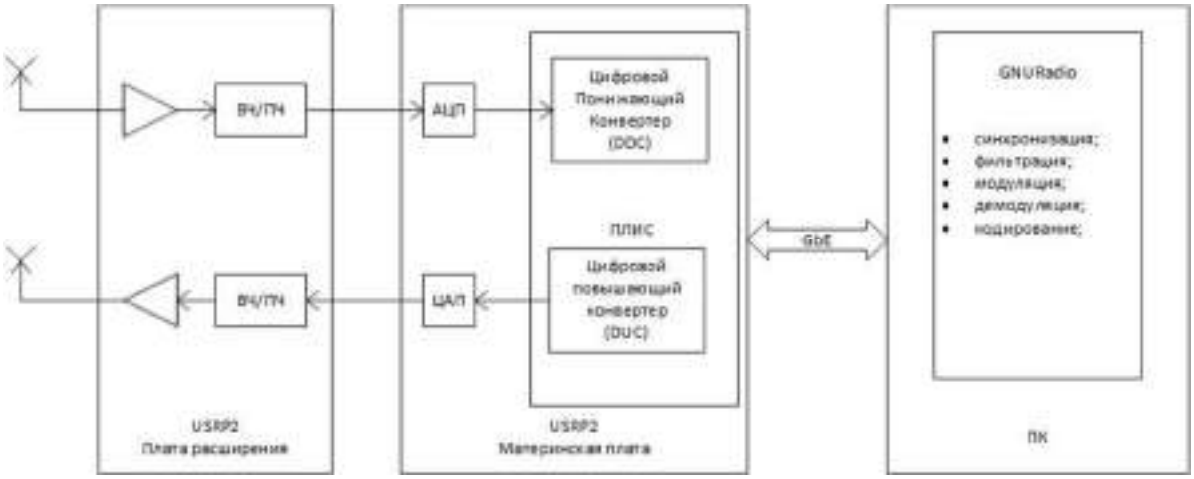


Рис. Структурно-функциональная схема USRP

Изначально проект GNUradio предназначен для задач обработки радиосигналов, он предоставляет набор стандартных хорошо оптимизированных компонент, пригодных для любой цифровой обработки сигналов.

Данный комплекс является открытым и свободно распространяемым. Это графическая среда моделирования аналоговых и дискретных систем. Она имеет множество библиотек, состоящих как из аналоговых, так и дискретных блоков. Каждый из блоков представляет собой полную программную модель его физического аналога и реализует соответствующие радиотехнические процессы (генерирование сигналов, модуляцию, демодуляцию, синхронизацию, фильтрацию и т.д.). Блоки работают в реальном времени и могут являться составными частями любой радиотехнической системы. Параметры блоков устанавливаются программно в зависимости от требуемых технических характеристик разрабатываемой системы. Сфера использования GNU Radio широка – данный программный комплекс применяется как для научных исследований, так и радиолюбителями.

Цифровая обработка сигналов по технологии SDR в программной среде GNURadio дает следующие преимущества по сравнению с традиционными способами разработки:

– уменьшение массы и габаритов изделия;

– уменьшение потребляемой мощности;

– упрощение конструкции;

– уменьшение стоимости (при учете использования недорогих АЦП);

– масштабируемость решения;

– продолжительность проектирования.

Но наряду с перечисленными преимуществами ЦОС имеет следующие недостатки:

– ограниченность быстродействия цифровой элементной базы;

– ограниченная разрядность и быстродействие АЦП и ЦАП;

– возникающие при ЦОС дополнительные искажения.

Таким образом, в результате рассмотрения традиционного (аппаратного) и перспективного (на основе программной среды GNUradio) способов моделирования радиотехнических систем и сравнительной их характеристики можно сделать вывод о том, что последний позволяет снизить продолжительность, трудоемкость и стоимость работ при проектировании, упростить и удешевить конструкции систем, улучшить их характеристики.

---

1. Software-defined radio [Electronic resource] // The Free Encyclopedia. – URL: http://en.wikipedia.org/wiki/Software-defined_radio.

2. Resource Allocation Studies Using Software Defined Radio (SDR) [Electronic resource] // Dashboardhttp. – URL: http://confluence.qu.edu.qa/display/NPRPRESEARCH/USRP2+Testbed.

УДК 004.733.4

С.Н. Михайлов, А.А. Шашорин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВАРИАНТ ТОПОЛОГИИ СЕТИ РАДИОДОСТУПА UTRAN ЖЕЛЕЗНОДОРОЖНОГО ОКРУГА ГОРОДА КУРСКА

Рассмотрен вариант топологии сети радиодоступа UTRAN Железнодорожного округа города Курска, позволяющий обеспечить полное покрытие территории округа качественной связью даже в часы пиковых нагрузок.

Современный этап развития телекоммуникаций характеризуется не только непрерывным увеличением числа пользователей, но и возрастающими требованиями к качеству услуг связи. Создание сетей UTRAN обусловлено потребностями абонентов в создании видеотелефонии, а также высокоскоростного доступа в Интернет без ограничения свободы их перемещения. Однако существующие сети связи имеют ряд существенных недостатков, среди которых: непредоставление полного покрытия территории зоной обслуживания сети, а также ограничение в предоставлении услуг связи во время пиковых нагрузок.

Одним из путей устранения этих недостатков выступает модернизация существующей сети. Основным этапом модернизации

может служить расчет сети с учетом характера местности и типа застройки.

Поэтому расчет варианта топологии сети радиодоступа UTRAN является актуальным и представляет практический интерес. Для расчета варианта топологии предлагается использовать общую методику расчета с учетом характерных особенностей местности, застройки и количества потенциальных абонентов.

Предельная емкость соты, количество одновременных соединений (пользователей):

$$N_{пр} = \left(1 + \frac{G_{обр}}{Eb/N0}.\frac{1}{v}\right).\left((1-\alpha)+i\right), \quad (1)$$

где $G_{обр}$– выигрыш от обработки или коэффициент расширения;

i – изоляция соты;

E_b/N_0 – отношение средней энергии бита к спектральной плотности шума;

v – коэффициент занятости услуги;

α – средние значения коэффициента ортогональности.

Величина загрузки соты, учитывая нагрузку от одного абонента, предельную емкость соты, а также количество пользователей, обслуживаемых сотой:

$$\eta = \frac{T1 \cdot N}{M1} + \frac{T2 \cdot N}{M2} + \frac{T3 \cdot N \cdot 1.4}{M3} + \frac{T4 \cdot N \cdot 1.4}{M4}, \quad (2)$$

где T1–T4 – нагрузка, создаваемая одним абонентом;

M1–M4 – предельная емкость соты (предельное количество одновременных соединений);

N – планируемое количество пользователей, обслуживаемых сотой.

Количество пользователей, обслуживаемых в одной соте, в случае равномерного распределения:

$$N_{соты} = N/\eta, \quad (3)$$

где N – планируемое количество пользователей, обслуживаемых сотой;

η берем из расчетов по формуле (2).

Количество необходимых базовых станций находим по формуле

$$К = N_{план} / N_{соты}, \quad (4)$$

где $N_{план}$ – планируемое количество пользователей;

$N_{соты}$ – количество пользователей, обслуживаемых одной сотой, в случае равномерного распределения.

Расчет относительной загрузки соты для типа местности «пригород» производим по следующей формуле:

$$\eta_{нисх}= ((0,02\cdot200)/73)+(0,006\cdot200/16)+(0,008\cdot200\cdot1,4/8)+ +(0,006\cdot200\cdot1,4/4)=0,831.$$

Количество пользователей, обслуживаемых в одной соте в случае равномерного распределения:

$$N_{соты} = 200/0,831 = 240,674 \approx 241.$$

Количество необходимых базовых станций для городского типа местности:

$$К = 16000/241 = 66,3 \approx 67.$$

Расчет относительной загрузки соты для типа местности «пригород»:

$$\eta= ((0,02\cdot250)/52)+(0,006\cdot250/13)+(0,008\cdot250\cdot1,4/9)+ +(0,006\cdot250\cdot1,4/7)=0,734.$$

Количество пользователей, обслуживаемых в одной соте, в случае равномерного распределения объектов:

$$N_{соты} = 250/0,734 = 340,6 \approx 341.$$

Количество необходимых базовых станций для пригородного типа местности:

$$К = 12000/341 = 35,19 \approx 36.$$

В результате анализа архитектуры сетей, рельефа местности и выполнения расчетов получены результаты, представленные ниже.

В ходе проведения анализа типа местности Железнодорожного района города Курска было определено, что на 90% территории преобладает равнинный ландшафт, остальные 10% относятся к пересеченному типу местности. По типу застройки округ делится на две приблизительно равные части. В северной части – пригородная застройка, в южной – городская. На основании анализа типа мест-

ности и с учетом оценки преобладающей застройки построена схема Железнодорожного района (рис. 1).

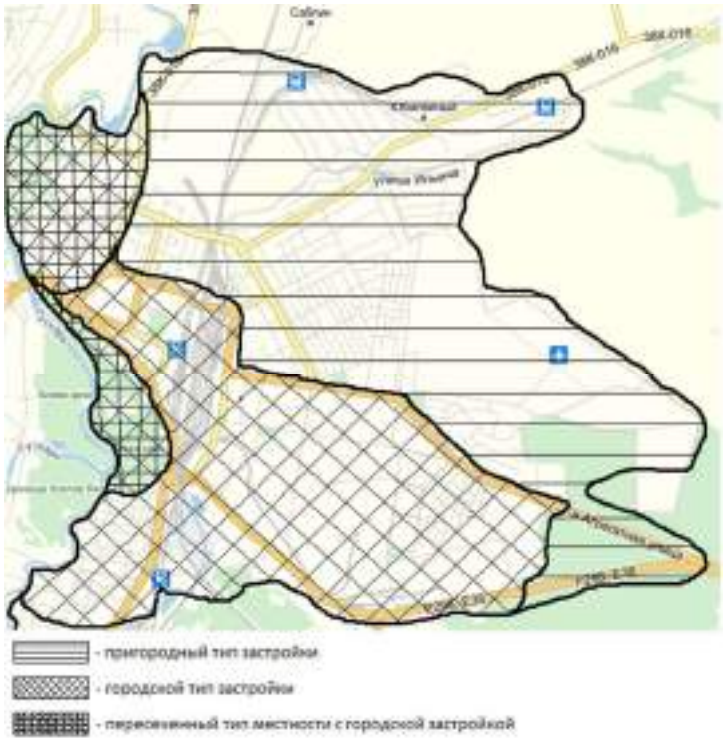


Рис. 1. Схема Железнодорожного района города Курска
с учетом типа местности и типа застройки

С учетом того, что планируемое количество пользователей одной соты типа микросота трехсекторная составляет 200 абонентов при общем количестве абонентов в зоне городской застройки 16000, из которых в зоне с пересеченным типом местности проживает приблизительно 3200 абонентов, количество базовых станций для этих участков составляет 16. Для участков с равнинной местностью и городской застройкой количество базовых станций с учетом емкости соты и количества предполагаемых абонентов составляет 51.

На части округа с равнинным типом местности и пригородной застройкой используются соты типа макросота с ненаправленной антенной, с оптимальным количеством пользователей для одной соты 250 абонентов. Планируемое количество абонентов для равнинной местности и пригородной застройки составляет 12000. С учетом емкости соты и количества предполагаемых абонентов необходимое количество базовых станций составляет 36.

Согласно информации, приведенной выше, общее количество базовых станций для Железнодорожного округа города Курска составляет 103. Их расположение представлено на рисунке 2.

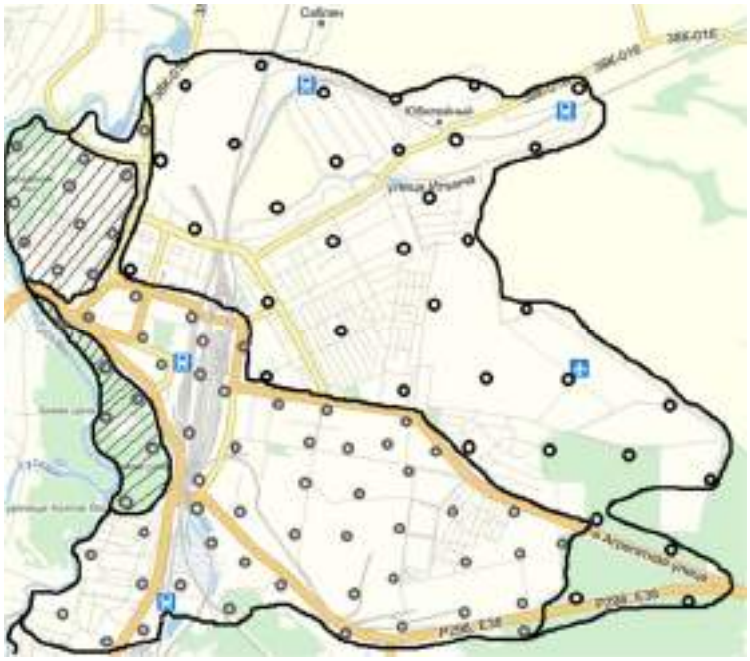


Рис. 2. Вариант расположения базовых станций
в Железнодорожном округе города Курска

Таким образом, приведенный вариант топологии сети радиодоступа позволяет обеспечить полное покрытие территории Железнодорожного округа качественной связью даже в часы пиковых нагрузок.

---

1. Тихвинский В.О. Сети подвижной связи 3-го поколения. Экономические и технические аспекты развития в России. – М.: Радио и связь, 2001. – 55 с.

УДК 621.394.74

И.Е. Мухин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРИНЦИПЫ СОЗДАНИЯ АВТОНОМНЫХ УДАЛЕННЫХ СИСТЕМ МОНИТОРИНГА НА ОСНОВЕ КОНЦЕПЦИИ НЕОБСЛУЖИВАЕМОГО ОБОРУДОВАНИЯ

Разработаны принципы синтеза автономных систем мониторинга на основе концепции необслуживаемого оборудования.

В современных условиях в связи с возросшим значением вопросов экономической эффективности при планировании, разработке и введении в строй современных систем телекоммуникации актуальное значение приобретают вопросы совокупной стоимости владения. Особую значимость эти вопросы приобретают при применении таких систем в условиях Крайнего Севера и т.п., где в силу обстоятельств ограничен или вообще отсутствует обслуживающий персонал.

В условиях увеличивающего объема трафика нарушение работоспособности таких систем даже на короткое время в денежном эквиваленте составляет существенную величину. Таким образом, в новых экономико-технических условиях развития общества возникает противоречие между требованиями сокращения совокупной стоимости владения автономными системами удаленного мониторинга за счет сокращения обслуживающего персонала и возрастающим при этом потоком неисправностей. Разрешение этого противоречия необходимо искать в направлении поиска научно-технических путей максимального снижения времени простоя таких систем из-за неработоспособного состояния до прибытия специалистов. Одним из таких путей является синтез систем удаленных автономных систем мониторинга на базе концепции необслуживаемого автономного оборудования (НАО) – такого оборудования, которое должно иметь возможность самостоятельного автоматического восстановления функций работоспособности в заданный период функционирования без участия персонала.

Реализация концепции НАО требует: введения поэлементной избыточности (на уровне модулей, узлов, компонентов) для автоматического восстановления функций отказавших модулей между регламентными работами; разработки функций отказоустойчивости на системном уровне (на уровне распределенной структуры НАО с избыточностью); наличия системы управления избыточностью, состоящей из подсистем локализации отказов и реконфигурации структуры НАО (в реальном времени).

При этом должны выполняться современные подходы к построению вычислительной среды, заключающиеся в отделении программных приложений от вычислительной платформы; унификации, масштабируемости и гибкости вычислительных средств;

поддержки различных сетевых технологий (мосты, программные интерфейсы приложений). Реализация основных положений этой концепции позволит значительно снизить стоимость систем мониторинга в целом; существенно расширить функциональных возможностей НАО; достичь предельно достижимых уровней надежности и безопасности.

При синтезе таких систем необходимо развитие технологии отказоустойчивой вычислительной среды с управляемой избыточностью, технологии поэлементной избыточности радиоэлектронного оборудования, развитие технологии проектирования базового отказоустойчивого масштабируемого вычислителя для комплексов необслуживаемого оборудовании, развитие технологии проектирования аппаратно-программных компонентов вычислительных, сетевых и периферийных средств на основе технологии систем на кристалле (СнК). При этом масштабируемая интегрированная сеть системы НАО должна строиться на базе сетевой технологии (единая сетевая инфраструктура распределенного НАО) с функцией поддержки единой информационно-вычислительной среды распределенного НАО. В целях удовлетворения требованиям поддержки растущего трафика в перспективе должна быть осуществлена поддержка интерфейсов AFDX, FibreChannel, SpaceWire/SpaceFibre, ARINC 429 и CAN. Вычислитель должен удовлетворять условиям открытости, гибкости, масштабируемости для разных приложений, включая потоковые вычисления.

Синтезированная устойчивая к отказам сетевая инфраструктура НАО должна обладать:

1) избыточными масштабируемыми внутрисетевыми связями;
2) адаптивной и избыточной маршрутизацией;
3) гарантированным внутренним интерфейсом для оконечных узлов;
4) разделением трафика по внутренним связям сети;
5) автоматическим обнаружением случайных ошибок протоколами SpaceWire;
6) автоматическим обнаружением постоянных ошибок «умными» маршрутизаторами;
7) возможностью подключения датчиков; высокоскоростным потоком данных;

8) передачей команд с детерминированным временем доставки;

9) сигналы жесткого реального времени со сверхмалыми задержками.

Основными этапами создания такой системы должны быть:

1) создание отказоустойчивой вычислительной среды с управляемой избыточностью;

2) создание системы с поэлементной избыточностью радиоэлектронного оборудования;

3) создание развитой системы сбора и обобщения информации о функционировании оборудования для анализа;

4) создание высокоразвитых алгоритмов для поиска (локализации) наблюдаемых и ненаблюдаемых отказов.

Таким образом, реализация изложенных принципов создания удаленных автономных систем мониторинга позволит существенно снизить стоимость их совокупного владения при одновременном повышении их надежности.

---

1. Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем.– М., 2006. – 501с.

УДК 004.724.2

И.Е. Мухин, И.С. Надеина

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ВЛИЯНИЯ СПЕКТРАЛЬНОЙ ЭФФЕКТИВНОСТИ СОВРЕМЕННЫХ ЦИФРОВЫХ СИГНАЛОВ НА ПОМЕХОУСТОЙЧИВОСТЬ УЗКОПОЛОСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Рассмотрена взаимосвязь между полосой частот сигнала и максимальной скоростью передачи данных для ограниченного количества видов манипуляций.

Широкое внедрение техники и компьютерных технологий стимулировало стремительное развитие цифровых систем передачи данных. Это объясняется наличием таких преимуществ, как высокая помехоустойчивость, слабая зависимость качества передачи от

длины линии связи, эффективность использования пропускной способности при передаче дискретных сообщений и др. В связи с этим необходимо проследить влияние спектральной эффективности современных цифровых сигналов на помехоустойчивость узкополосных современных систем инфокоммуникаций.

В работах [1, 2] установлены взаимосвязи между полосой частот сигнала и максимальной скоростью передачи данных для ограниченного количества видов манипуляций. В связи с этим вышеописанная задача сводится к систематизации имеющихся данных и разработке математических моделей для не рассмотренных типов цифровых модуляций.

Одним из важнейших критериев производительности цифровых систем связи является зависимость вероятности появления ошибочного бита P_b от отношения энергии сигнала S к средней мощности шума N ($\frac{S}{N}$).

Для нахождения шумовой составляющей в цифровой связи используется нормированное качество – отношение энергии сигнала на 1 бит к спектральной мощности аддитивного белого гауссова шума (АБГШ) в полосе 1 Гц, которое определяется как

$$\frac{E_b}{N_0} = \frac{SB}{NR_b}, \qquad (1)$$

где B – полоса частот канала связи;

R_b – битовая скорость передачи данных.

Отраженная в выражении (1) взаимосвязь используется в теореме Шеннона-Хартли, которая определяет максимальную безошибочную пропускную способность канала связи, подверженному воздействию АБГШ мощности N:

$$R_{bmax}\left[\text{бит / с}\right] = Blog_2\left(1 + S / N\right). \qquad (2)$$

Используя выражение (2) для нахождения границы предела пропускной способности канала по Шеннону, необходимо осуществить следующее преобразование:

$$\frac{R_{bmax}}{B} = log_2\left(1 + \frac{E_b R_b}{N_0 B}\right). \qquad (3)$$

Отношение $\frac{R_{bmax}}{B}$ определяет пропускную способность канала связи.

Приведем выражение (3) к виду

$$\frac{E_b}{N_0} = R_b max / B(2^{(R_b max/B)} - 1). \quad (4)$$

Из выражении (4) следует, что повышение скорости передачи данных осуществляется за счет увеличения полосы частот B или отношения мощности сигнала к мощности шума.

Для дальнейшей оценки скорости передачи информации в системе связи необходимо выявить зависимость между полосой частот и многопозиционностью модулированного сигнала.

Алгоритм для нахождения взаимосвязи описанных выше параметров определяется следующим образом:

1) нахождение полосы частот модулированного сигнала;

2) определение эффективности использования полосы сигнала.

Так, для амплитудной и бинарной фазовых манипуляций ($m = 2$), которые имеют только 2 уровня:

$$1)\ \Delta F = 2\text{В} = 2\frac{1}{2T_b} = \frac{E_b}{N_0} = R_b; \quad (5)$$

$$2)\ \frac{R_b}{B} = 2. \quad (6)$$

При фазовой и квадратурной амплитудной манипуляциях m-арных сигналов полоса частот и эффективность ее использования следующие:

$$1)\ \Delta F = 2\text{В} = 2\frac{1}{2T_b} = \frac{1}{T_b log_2 m} = \frac{R_b}{n}; \quad (7)$$

$$2)\ \frac{R_b}{B} = 2n = 2log_2 m\ . \quad (8)$$

Для частотной манипуляции m-арных сигналов при когерентном приеме $\Delta \text{f} = \frac{1}{2T_S}$:

$$1)\ \Delta F = (m-1)f + 2B = (m-1)\frac{1}{2T_s} + 2\frac{1}{2T_s} = \frac{m+1}{2T_b log_2 m} = \frac{(m+1)R_b}{2log_2 m}; \quad (9)$$

$$2)\ \frac{R_b}{B} = \frac{2log_2 m}{(m+1)}. \quad (10)$$

На рисунке из расчетов по формулам (3), (5) – (10) представлены зависимости спектральной эффективности цифровых сигналов при различных видах модуляции от отношения сигнал/ шум.

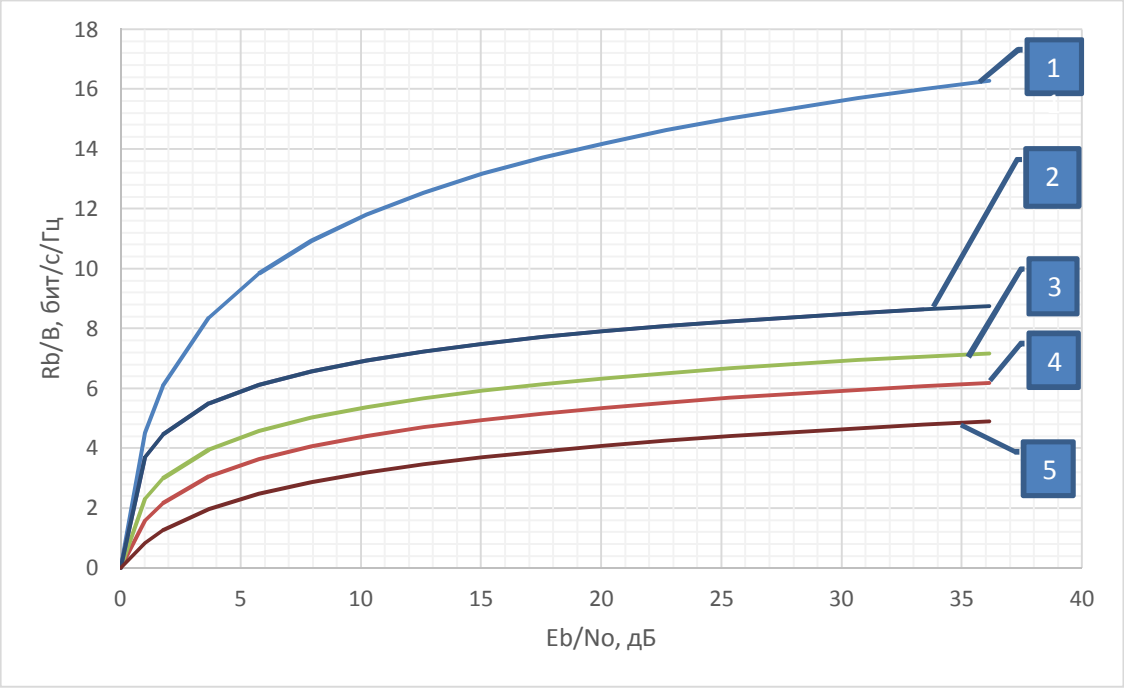


Рис. Сравнительная характеристика влияния спектральной эффективности современных цифровых сигналов на помехоустойчивость систем связи при $P_{осш} = 10^{-6}$: 1 – предел Шеннона; 2 – КАМ-64; 3 – PSK-4; 4 –FSK-4; 5 – ASK-2

Эти зависимости позволяют оценить скорость передачи данных для различных типов модуляции. Теоретическая спектральная эффективность использования полосы пропускания при различных видах манипуляции отражена в таблице.

Спектральная эффективность полосы пропускания при различных видах манипуляции

Тип манипуляции	Спектральная эффективность (бит/с/Гц)
2-АМн	1
4-ЧМн	2
4-ФМн	3

Окончание табл.

Тип манипуляции	Спектральная эффективность (бит/с/Гц)
16-КАМ	4
32-КАМ	5
64-КАМ	6
256-КАМ	8
1024-КАМ	10

Таким образом, полученные результаты позволяют провести сравнительный анализ сигналов с различными типами модуляций для их наиболее адекватного выбора при различных многопозиционных системах связи.

Список литературы

1. Теория электрической связи: учебное пособие / К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева. – Ульяновск: Изд-во УлГТУ, 2008.

2. Мелихов С.В., Кологривов В.А. Взаимосвязь качественных характеристик для различных видов цифровой манипуляции // Доклады ТУСУР. – 2006. – №6(14). – С. 68-77.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: [пер. с англ.]. – 2-е изд. – М.: Изд. Дом «Вильямс», 2007.

УДК 621.39

С.Н. Михайлов, А.С. Фильшин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОБОСНОВАНИЕ НАПРАВЛЕНИЯ МОДЕРНИЗАЦИИ ПЕРСПЕКТИВНОЙ ПЕРВИЧНОЙ СЕТИ КУРСКОЙ ОБЛАСТИ

Представлен анализ особенностей проектирования и развития внутризоновой первичной сети электросвязи Курской области.

Первичные сети предназначены для создания коммутируемой инфраструктуры, обеспечивающей автоматическую организацию постоянного канала с двухточечной топологией между пользовательскими устройствами, подключенными к такой сети. В первичных сетях применяется техника коммутации каналов. Каналы, предоставляемые первичными сетями своим пользователям, отли-

чаются высокой пропускной способностью – обычно от 2 Мбит/с до 10 Гбит/с [1].

Еще 15 лет назад первичная сеть области базировалась на симметричных медных кабелях общей протяженностью примерно 1000 км. Подавляющая часть симметричных кабелей внутризоновой первичной сети уплотнялась аппаратурой К-60П-4, К-60П, ИКМ-30 и ИКМ-120.

Согласно планам развития внутризоновых первичных сетей в 2000-х годах произошла замена устаревших линий связи в виде металлических кабелей на волокно-оптические и внедрена совершенно новая технология передачи данных на основе систем синхронной цифровой иерархии (СЦИ – англ. SDH). Этот переход не только позволил многократно увеличить количество каналов, но и поднял уровень надежности.

На рисунке 1 изображена диаграмма, иллюстрирующая прирост пропускной способности сети [2].

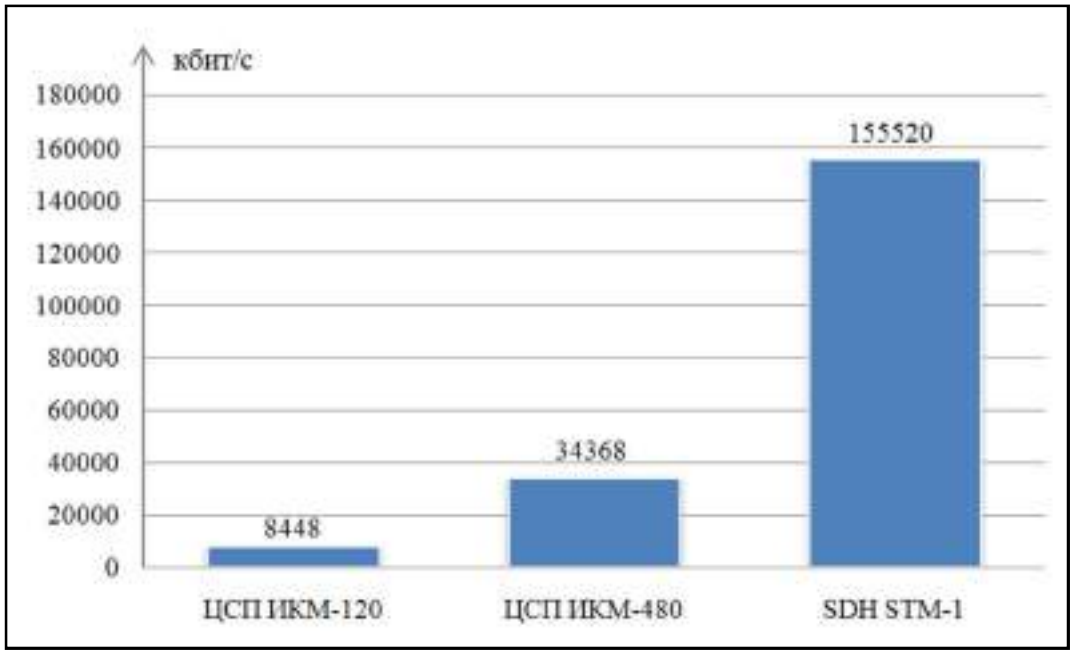


Рис. 1. Диаграмма увеличения скорости

На сегодняшний день первичная сеть области построена по кольцевому принципу с участками уровня STM-4 и STM-1. В результате комплексного анализа требований и реальных технических параметров сети определены территориальные участки, не

обеспечивающие достижение современных требований по пропускной способности и коммутационным возможностям.

Основные количественные значения этих требований представлены в таблице.

Современные количественные значения требований к первичной сети

Техническая характеристика	Требуемое значение
Пропускная способность	1-10 Гбит/с
Количество каналов	1008 E1 / 63 E3
Количество портов ввода/вывода	63 E1 / 1 E3 / 1 GbE
Размер матрицы кросс-коммутации	16 x 16 STM-1 (VC-12 / VC-3 / VC-4)

Так, участок, соединяющий областной центр с развивающимися городами Курчатов и Льгов, имеет самую низкую пропускную способность в 155 Мбит/с, которой явно недостаточно для новых потребителей в лице крупных компаний, банков, муниципальных и ведомственных учреждений, силовых структур. Несомненно, именно этот участок требует первоочередной модернизации.

В общем, программа модернизации может быть направлена на реализацию нескольких направлений:

– замена линейных сооружений;

– замена телекоммуникационного оборудования;

– совершенствование технологии передачи данных.

В ходе исследования и анализа рынка по строительству линий связи установлено, что финансовые расходы на демонтаж и прокладку новой ВОЛС могут составлять сумму до 17 млн руб. При этом могут быть достигнуты следующие новые возможности:

– увеличение количества оптических волокон в кабеле с 8 до 16 и более;

– уменьшение коэффициента затухания оптического сигнала за счет использования более чистого кварцевого стекла в волокне.

Технико-экономическая оценка потенциальных возможностей и расходов показывает нецелесообразность данного направления.

В то же время существующие волокно-оптические линии могут успешно использоваться с перспективным и новым оборудова-

нием, обеспечивающим реализацию современных требований к сети, а именно:

– пропускная способность участка сети более 1 Гбит/с;

– повышенная надежность;

– техническая адаптивность (возможность наращивания производственных мощностей).

Графическое соотношение возможностей линейной и аппаратной составляющей сети представлено на рисунке 2, из которого видно, что именно аппаратная часть ограничивает возможности сети в пропускной способности.

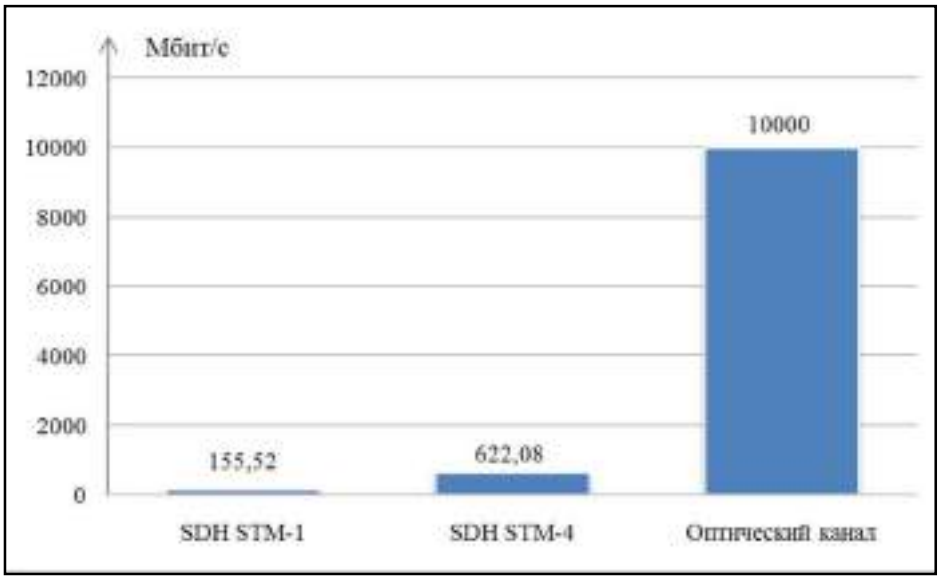


Рис. 2. Соотношение возможностей аппаратной и кабельной частей сети

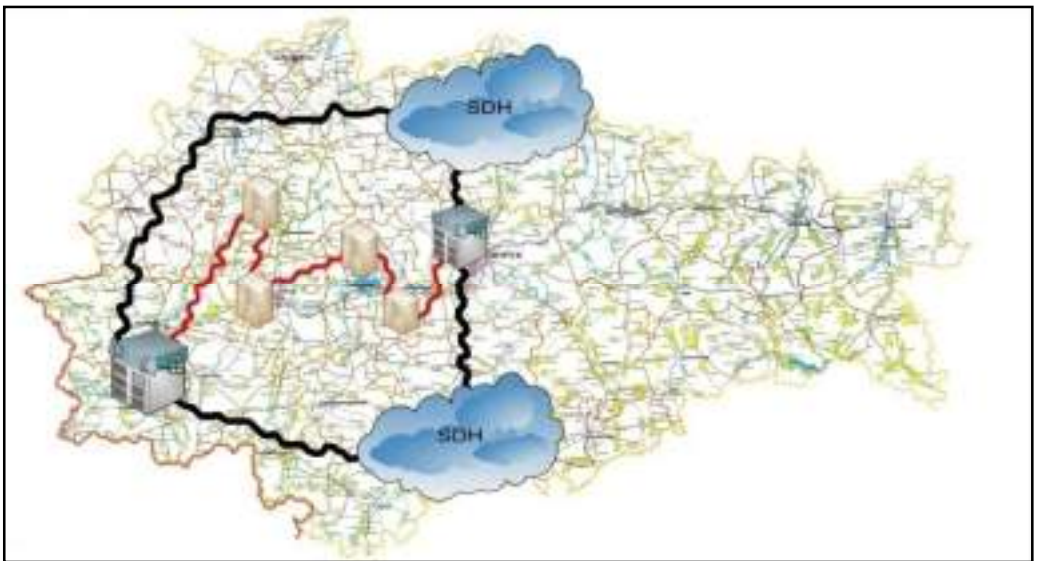


Рис. 3. Структурная схема построения первичной сети Курской области с учетом модернизации

Таким образом, в качестве основного направления модернизации предложена замена станционного оборудования. Затраты могут составить до 10 млн руб. (стоимость оборудования и его монтажа). В результате реализации предложенного направления модернизации структура первичной сети электросвязи Курской области будет иметь вид, представленный на рисунке 3.

С экономической точки зрения такое направление наиболее целесообразно. Кроме того, реализация данного направления обеспечит выполнение перечисленных ранее современных требований.

Основным направлением модернизации сети выбрано направление, связанное с заменой станционного оборудования. Техническая база станционного оборудования должна основываться на технологических решениях компании NokiaSiemensNetworks. Такой выбор обеспечивает информационную совместимость с имеющимися техническими и программными решениями системы управления.

---

1. Андреев В.А., Портнов Э.Л., Кончаловский Л.Н. Направляющие системы электросвязи: учебник для вузов: в 2 т. – Т. 1. – 7-е изд., перераб. и доп. – М.: Горячая линия – Телеком, 2009. – 424 с.: ил.

2. NokiaSiemensNetworks. Концепт реализации схемы управления объединенной компании «РОСТЕЛЕКОМ» (DCN-Концепт для SDH/DWDM-сети). 2002. – 65 с.

УДК 621.391

С.С. Хотынюк

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОСОБЕННОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ХАОТИЧЕСКИХ СИГНАЛОВ

Дано краткое описание хаотических систем связи, рассмотрены их достоинства и недостатки, указаны отличия этих систем от традиционных.

В настоящее время разрабатываются и проходят апробацию системы связи нового вида, в которых в качестве несущей используются не традиционные синусоидальные, а хаотические сигналы. Такие системы получили название хаотических.

В основе использования хаотических сигналов в системах связи лежит возможность управления этими сигналами приложением к генерирующим их системам малых воздействий. Дело в том, что хаотическая система очень чувствительна к начальным условиям, то есть поведение системы в последующие моменты времени сильно зависит от ее состояния в предшествующие, причем малое изменение состояния системы приводит к значительным последствиям. В качестве малых воздействий на систему могут выступать изменения параметров системы в ходе ее работы (например, варьирование электрического сопротивления или емкости в небольшом диапазоне значений), а также внешние воздействия (приложение малого дополнительного напряжения, пропускание небольшого тока).

В общих чертах идея, лежащая в основе построения хаотических систем связи, заключается в следующем. Поскольку хаотические сигналы, воспроизводимые двумя идентичными системами, включенными одновременно, одинаковы в любой момент времени, то если одну из таких систем расположить на передающей стороне, а вторую – на приемной, то сигнал, воспроизводимый хаотическим передатчиком, будет целиком известен хаотическому приемнику, таким образом, этот сигнал можно использовать в качестве несущей. Хаотическая несущая модулируется посредством ее сложения с информационным сигналом, который выступает в качестве управляющих малых воздействий. На приемной стороне из принятого сообщения путем вычитания несущей выделяется информационный сигнал. При этом в связи с хаотическим характером несущей посторонний наблюдатель может даже не понять, что осуществляется сеанс связи.

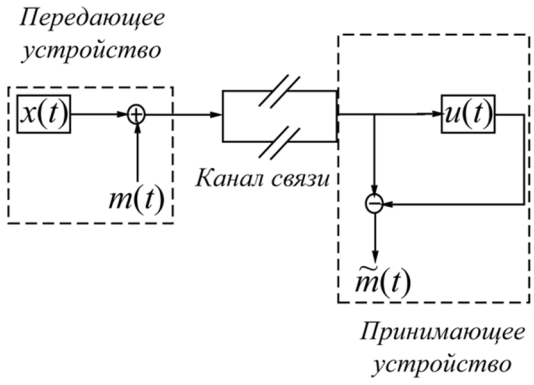


Рис. Схематическое изображение хаотической системы связи

Схематическое изображение хаотической системы связи представлено на рисунке, где $x(t)$ и $u(t)$ – две идентичные хаотические системы, работающие на передающей и приемной сторонах соответственно; $m(t)$ – информационный сигнал; $\tilde{m}(t)$ – детектированный сигнал [1].

Исследование сигналов с хаотической несущей позволило выделить преимущества, которыми обладают такие сигналы по сравнению с традиционными с синусоидальной несущей. В частности, среди этих преимуществ можно назвать следующие [2].

1. Хаотические сигналы являются широкополосными с небольшой спектральной плотностью мощности, то есть обладают всеми достоинствами сигналов с синусоидальной несущей в системах с расширением спектра: большой помехоустойчивостью и высокой пропускной способностью их каналов. Причем хаотические сигналы можно использовать как сами по себе, так и для расширения спектра узкополосных сигналов.

2. Хаотические сигналы трудны для постороннего перехвата – сторонний наблюдатель может даже не узнать о происходящем сеансе связи. Хаотические сигналы хорошо маскируются на фоне шумов, выделить их, не обладая априорной информацией о свойствах конкретно используемого сигнала, задача крайне сложная.

3. Методы преднамеренного подавления сигналов, используемые при осуществлении радиоэлектронной борьбы (РЭБ), гораздо менее эффективны при применении их к хаотическим сигналам, нежели к традиционным синусоидальным.

4. Поскольку хаотические сигналы по их форме слабо отличаются от случайных, то есть предсказание значения сигнала в следующий момент времени является практически не разрешимой задачей, автокорреляционные функции таких сигналов имеют импульсную форму. В связи с этим сигналы, приходящие в одну точку в виде разных лучей с тем или иным запаздыванием друг относительно друга, практически друг на друга не влияют, то есть при использовании хаотических сигналов проблема многолучевого распространения отсутствует в принципе. Более того, такие сигналы, делая каждый свой энергетический вклад, повышают общую энергетику, то есть усиливают друг друга.

5. Многочисленные исследования показывают [2, 3], что восстановление хаотических сигналов, подверженных воздействию шума, происходит более эффективно, нежели традиционных сигналов с синусоидальной несущей, подверженных влиянию шума такого же уровня. Кроме того, применяемые к хаотическим сигналам методы фильтрации шума являются более эффективными.

Таким образом, хаотические сигналы характеризуются рядом привлекательных преимуществ по сравнению с синусоидальными. Вне зависимости от конструкции конкретно взятой хаотической системы связи, такие системы характеризуются следующим рядом общих достоинств и недостатков [2].

1. Синхронизация в цифровых системах связи играет важную роль, т.к. позволяет получить информацию о длительности символов. Кроме того, в случае когерентного приема, когда требуется знание фазы приходящего сигнала, синхронизация используется для восстановления несущей. В отличие от традиционных систем связи с синусоидальными сигналами синхронизация хаотических систем выполняется самостоятельно, без каких-либо дополнительных мер.

2. Экспериментальным путем было определено, что некоторые многопользовательские оптические телекоммуникационные схемы на основе хаоса позволяют подключать более чем на 15% больше пользователей при той же битовой вероятности ошибки.

3. Сильная зависимость хаотических сигналов от начальных условий может использоваться для мультиплексирования, т.к. слабое изменение начальных условий приводит к тому, что развитие хаотической динамики идет по другому «сценарию». Различные «сценарии» развития процесса могут соответствовать различным каналам связи, поэтому возможно осуществлять объединение нескольких информационных каналов в одном.

4. Возможность управления хаотической динамикой можно также использовать для цифрового кодирования информации. Этот подход основан на следующем. Временная развертка хаотических колебаний состоит из перемежающихся положительных и отрицательных пиков. Оказывая на систему воздействия, можно вынудить ее выдавать тот или иной требуемый пик. Ассоциируя, например, положительный пик сигнала с символом «1», отрицательный пик – с символом «0», можно осуществить кодирование сигнала. Достоин-

ства такого способа состоят в том, что посредством маломощных воздействий можно производить кодирование источника, канальное кодирование и шифрование, причем объединяя все это в одном процессе, без привлечения дополнительных ресурсов системы.

Таким образом, можно сделать вывод о том, что управление хаотическими системы требует низких энергозатрат. Возможность осуществления нескольких задач (кодирование источника, канальное кодирование, шифрование) одним физическим процессом приводит к упрощению структуры хаотических систем по сравнению с традиционными. Кроме того, хаотический режим работы возникает при условии нелинейного поведения одного из элементов системы. Поскольку все реальные электронные элементы являются нелинейными с узким линейным участком, то обеспечить нелинейность проще, нежели выполнить условие линейности элемента. Данное обстоятельство также выступает в пользу хаотических систем по сравнению с синусоидальными, требующими принятия специальных мер по обеспечению линейного режима. Последние три фактора обусловливают высокую рентабельность систем связи с хаотическими сигналами.

В качестве недостатка хаотических систем связи необходимо упомянуть их меньшую помехоустойчивость, т.к. по сравнению с традиционными схемами при том же соотношении сигнал/шум в системах связи с хаотической несущей более высока вероятность ошибки.

Учитывая все особенности описываемых систем, их достоинства и недостатки, в качестве возможного целесообразного использования хаотических информационных сигналов можно предположить следующие варианты:

– системы с низким энергопотреблением, в которых затруднено принятие сложных и энергоемких мер для избегания нелинейности;

– оптическая связь, поскольку оптические и другие электронные устройства имеют больший диапазон рабочих параметров (эксперименты по применению хаотических сигналов в системах оптической связи уже проводились [4]);

– сверхширокополосные радиосистемы;

– персональные сети с низкими скоростями передачи данных.

На сегодняшний день разработку систем связи на основе хаоса еще нельзя считать окончательно завершенной, скорее можно говорить о существовании таких систем на уровне перспективной концепции, т.к. слабо разработана или полностью отсутствует элементная база. Однако перспективы хаотических систем заманчивы, эта концепция привлекает множество исследователей, что подтверждается большим количеством печатных работ по этой теме [2, 5]. Все это позволяет высказать уверенность в том, что использование хаоса в системах связи в скором времени выйдет за рамки концепции в область практического применения и прочно займет свою нишу среди современных инфокоммуникационных систем.

Список литературы

1. Короновский А.А., Москаленко О.И., Храмов А.Е. О применении хаотической синхронизации для скрытой передачи информации // Успехи физических наук.– 2009.– Т. 179 (12).– С. 1281–1310.

2. Grzybowski J.M.V., Eisencraft M., Macau E.E.N. Communication Systems: Current Trends and Challenges // Applications of Chaos and Nonlinear Dynamics in Engineering: Vol. 1. Understanding Complex Systems. – Berlin: Springer-Verlag, 2011. – P. 203-230.

3. Williams C. Chaotic communications over radio channels // IEEE Transactions on Circuits and Systems Part I: Fundamental Theory and Applications.– 2001.– Vol. 48(12).– P. 1394-1404.

4. Chaos-based communications at high bit rates using commercial fibre-optic links / Argyris D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcı´a-Ojalvo, C. R. Mirasso, L. Pesquera, K. A. Shore. // Nature. – 2005. – Vol. 438(7066). – P. 343-346.

5. Chaotic Signals in Digital Communications / by ed. M. Eisencraft, R. Attux, R. Suyama. – Boca Raton: CRC Press, 2013. – 504 p.

УДК 621.391

С.С. Хотынюк

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ХАОТИЧЕСКИЕ СИГНАЛЫ: СВОЙСТВА И НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ

Дано краткое описание хаотических сигналов, генерирующих их систем, рассмотрены основные перспективные направления применения таких сигналов.

В начале 90-х годов прошлого века возникло и стало активно развиваться направление исследований систем связи, в основе которых лежит использование в качестве несущего так называемого хаотического сигнала. Ряд ученых и инженеров полагают, что не за горами эра активного использования хаотических сигналов, в связи с чем данное направление является перспективным и современным. Исследования таких сигналов и систем в настоящее время ведутся и освещаются как в зарубежной, так и в российской литературе [1, 2], однако в этой теме присутствует недостаток вводных статей на русском языке, не перегруженных математическим аппаратом и позволяющих новичкам в этой области получить достаточно ясное первоначальное представление об этом интересном и перспективном направлении исследований. Настоящая статья является попыткой восполнить данный пробел.

Хаотические сигналы при определенных условиях формируются нелинейными динамическими системами.

Целью исследования развивающихся во времени процессов (динамических явлений) является нахождение математической модели (уравнения или системы уравнений), достаточно точно описывающей протекание этих явлений. Такие процессы, в случае если математические модели для них найдены, называются детерминированными.

В детерминированном процессе можно предсказать значение переменной величины в любой момент времени. Если же значение величины предсказать нельзя, процесс называется случайным. Как правило, под случайным понимается полностью детерминированный процесс, смешанный с некоторым неизвестным процессом, называемом шумом, в результате чего предсказать поведение исследуемой в таком процессе величины нельзя. Однако во второй половине XX века сформировалось понимание того, что существуют процессы, которые одновременно можно отнести как к детерминированным, так и к случайным. Такие процессы были названы хаотическими.

Для хаотических явлений можно составить точную математическую модель, однако предсказать значение переменной величины в любой момент времени невозможно.

На рис. 1 представлен график изменения величины (в данном случае электрического напряжения) в хаотическом процессе от времени. Процесс представляет собой колебания величины с амплитудой и частотой, изменяющимися без заметной закономерности. В связи с этим хаотические процессы называют хаотическими колебаниями. Как видно из рисунка 1, график хаотических колебаний внешне не отличается от графика случайной величины.

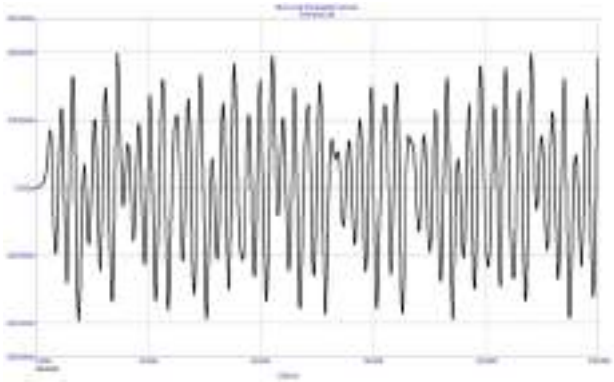


Рис. 1. График зависимости электрического напряжения от времени в хаотическом процессе

Тем не менее подобное впечатление обманчиво. Если при неизменных параметрах системы производить вычисления выходного результата по математической модели этой системы, можно раз за разом получать абсолютно идентичные результаты, а построенные по этим результатам временные графики будут полностью совпадать. Таким образом, в отличие от случайных хаотические сигналы являются возобновляемыми.

Открытие этих фактов привело к возникновению так называемой теории хаоса, которая имеет ряд возможных применений: с помощью хаотических систем моделируют турбулентные движения жидкостей и газов, сложные механические маятники, графики биржевых цен акций, изменение популяций организмов в живой природе, сердечные аритмии и ряд других исследований в различных областях науки. Теорией хаоса также заинтересовались разработчики систем связи, и их исследования принесли интересные результаты. Оказалось, что можно не только описывать уже известные явления хаотическими моделями, но и разрабатывать источники хаотических процессов под их математические модели.

Для того чтобы в системе возникли хаотические колебания, необходимо наличие в ней нелинейного элемента. Возникновение

хаотического режима в электрических цепях можно продемонстрировать на примере одного из наиболее изученных источников хаотических процессов – цепи (или генератор), названной в честь его создателя Чуа [3].

Это электрическая цепь, состоящая из двух конденсаторов C1 и C2, катушки индуктивности L, линейного резистора с проводимостью G и нелинейного резистора с отрицательным сопротивлением (диода Чуа) g, в которой при задании определенных значений ее параметров возникают хаотические колебания токов и напряжений на ее элементах (i_L, V_{C1}, V_{C2}). Схематическое изображение цепи Чуа представлено на рис. 2 [4].

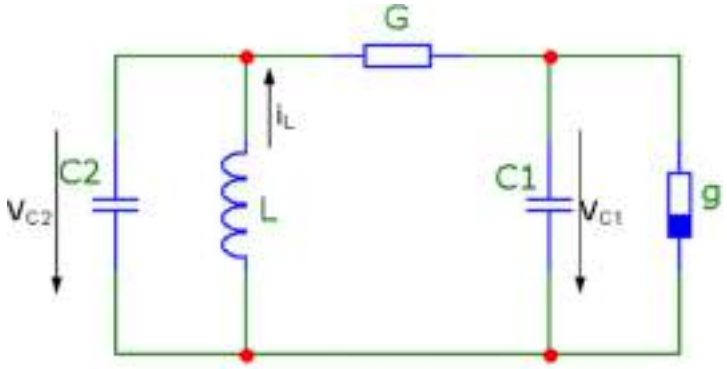


Рис. 2. Схема цепи Чуа, построенная в программном комплексе Micro-Cap

Нелинейным элементом в цепи Чуа является диод Чуа, который в качестве отдельного элемента не выполняется, его можно собрать, например, из двух операционных усилителей. Вольт-амперная характеристика диода Чуа представлена на рис. 3 [4].

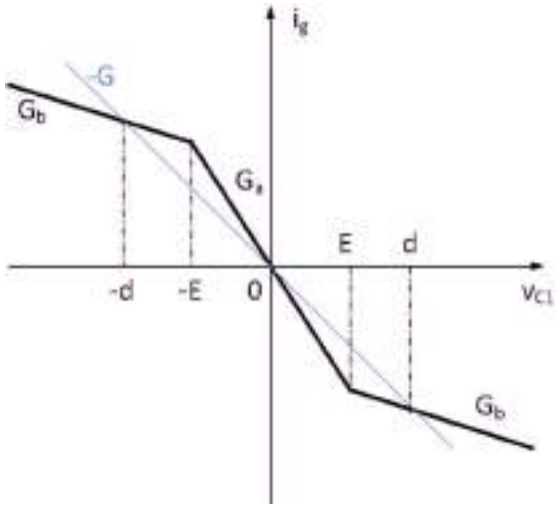


Рис. 3. Вольт-амперная характеристика диода Чуа

Исследования амплитудного спектра частот хаотических сигналов показывают, что эти сигналы относятся к широкополосным и имеют сплошной спектр. В качестве примера на рис. 4 представлен график зависимости спектральной плотности мощности хаотических колебаний от частоты хаотических колебаний, производимых формирователем потока хаотических радиоимпульсов, разработанным в Институте радиотехники и электроники РАН [5].

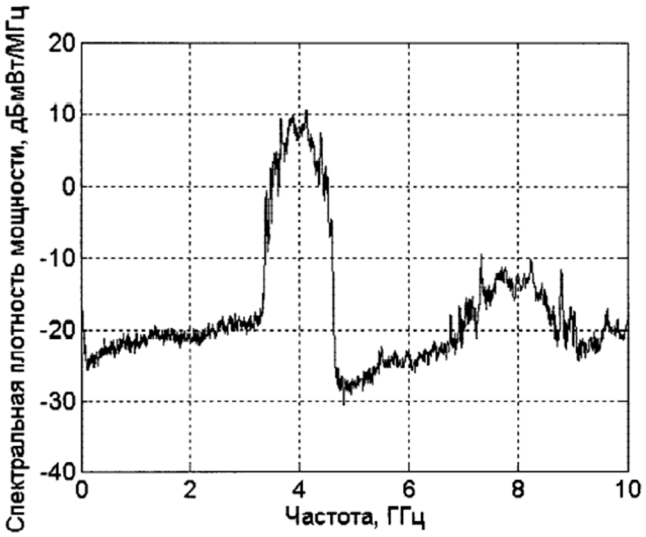


Рис. 4. График зависимости спектральной плотности мощности хаотических колебаний от частоты хаотических колебаний

Особенностью систем, демонстрирующих хаотическое поведение, является их высокая чувствительность к начальным условиям. В качестве демонстрации этого явления на рис. 5 представлена временная реализация напряжения в цепи Чуа V_{C1} для двух значений L, отличающихся друг от друга на 0,01%. На рисунке 5 хорошо видно, как два сигнала, вначале почти точно совпадающие друг с другом сначала постепенно расходятся, а затем становятся существенно непохожими друг на друга [6].

Другой практически значимой особенностью хаотических сигналов является их способность к самосинхронизации. Это означает, что если каким-либо образом организовать взаимосвязь двух идентичных хаотических систем и предоставить им возможность работать в режиме генерирования хаотических процессов, то спустя какое-то время после начала работы сигналы, снимаемые с систем, будут абсолютно идентичными.

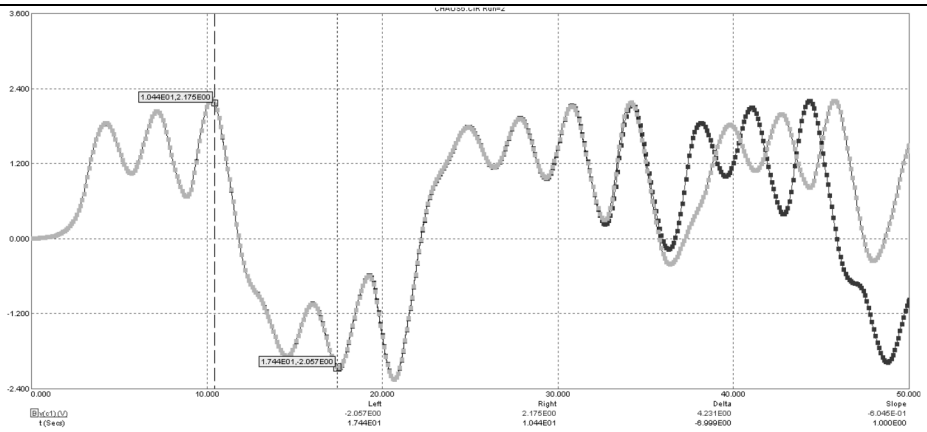


Рис. 5. Временная реализация напряжения в цепи Чуа V_{C1} для двух значений L, отличающихся друг от друга на 0,01%

В качестве примера на рис. 6, 7 соответственно представлены две цепи Чуа, работающие с включенной и выключенной синхронизацией [3]. Нижние осциллографы демонстрируют сигнал, подаваемый с отдельных цепей, а на горизонтальную и вертикальную развертки верхнего осциллографа подаются сигналы с обеих цепей сразу. Из рис. 6 видно, что в режиме синхронизации сигналы в отдельных цепях (нижние осциллографы) выглядят вполне похожими, верхний осциллограф демонстрирует прямую, находящуюся под углом 45º к каждой из осей, что подтверждает вывод о равенстве сигналов, в то время как при отсутствии синхронизации (рис. 7) заметно различие сигналов в разных цепях на нижних осциллографах, об этом же свидетельствует картинка на экране верхнего осциллографа [3].

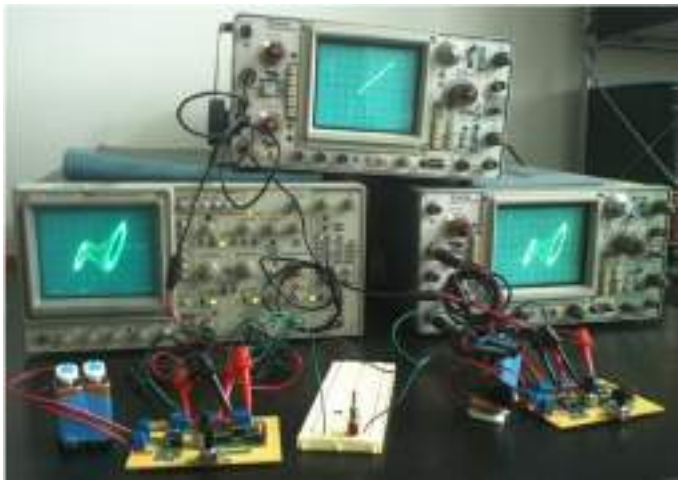


Рис. 6. Две синхронизированные цепи Чуа

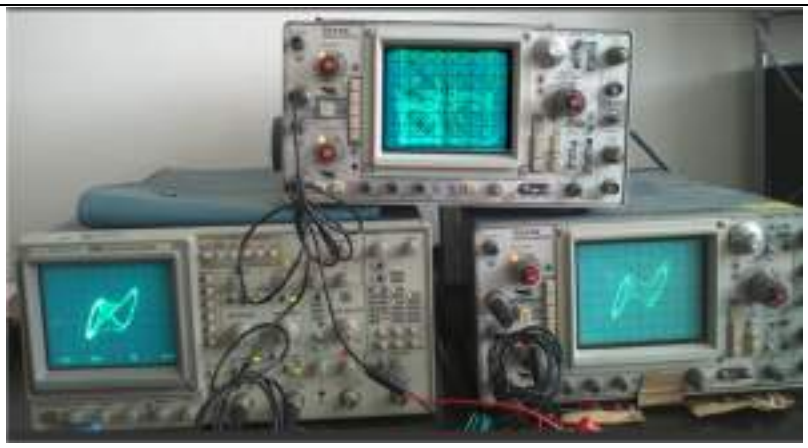


Рис. 7. Две рассинхронизированные цепи Чуа

Описанные свойства хаотических сигналов обусловливают широкие перспективы их применения в системах инфокоммуникаций.

Список литературы

1. Grzybowski J.M.V., Eisencraft M., Macau E.E.N. Communication Systems: Current Trends and Challenges // Applications of Chaos and Nonlinear Dynamics in Engineering: Vol. 1. Understanding Complex Systems. – Berlin: Springer-Verlag, 2011. – P. 203-230.

2. Сверхширокополосная прямохаотическая передача информации в СВЧ-диапазоне / А.С. Дмитриев, Б.Е. Кяргинский, А.И. Панас, Д.Ю. Пузиков, С.О. Старков // Письма в ЖТФ.– 2003.– Т. 29(2). – С. 70-76.

3. SiderskiyV. Сайт о цепи Чуа [Электронный ресурс]. – URL: http://chuacircuits.com.

4. Цепь Чуа [Электронный ресурс]. – URL: http://ru.wikipedia.org/wiki/Цепь_Чуа.

5. Пат. №2429566 Российской Федерации. Способ формирования потока хаотических радиоимпульсов и формирователь хаотических радиоимпульсов / Дмитриев А.С., Ефремова Е.В., Клецов А.В., Кузьмин Л.В., Панас А.И.; заявитель и патентообладатель Юго-Зап. гос. ун-т; Опубл. 2011, Бюл. № 26.

6. Патрушева Т.В., Патрушев Е.М. К вопросу о применимости осцилляторов хаотических колебаний в устройствах контроля физических величин // Ползуновский альманах.– 2009.– №2.– С. 153–155.

УДК 004.031.42

А.Е. Севрюков, О.А. Чернышева

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВЫБОР ОПТИМАЛЬНОГО ВАРИАНТА ПОСТРОЕНИЯ СЕТИ IPTV

Рассмотрена стратегия, подразумевающая создание оптимального варианта архитектуры сети интерактивного телевизионного вещания.

IPTV – это технология передачи телевизионного изображения по сетям передачи данных с помощью IP-пакетов. Просматривать такие каналы можно как на мониторе компьютера или ноутбука, так и на экране обычных телевизоров.

Весь спектр услуг IPTV можно условно разделить на три основные группы:

– базовые (канальные) услуги (BasicChannelService);

– расширенные (избираемые) услуги (EnhancedSelectiveService);

– интерактивные телематические услуги (InteractiveDataService).

Для реализации этих услуг оператор использует следующие режимы передачи информации в IP-сети: unicast, broadcast и multicast.

Unicast используется для предоставления персональных услуг. Этот метод позволяет передавать информацию от источника к конкретному IP-адресу. Абонент заказывает персональный контент, предназначенный только для него и, соответственно, только сам получает заказанную услугу. При одновременном просмотре своих заказов несколькими пользователями их трафик суммируется на участке от источника – файлового сервера, на котором находятся требуемые передачи, до абонентской линии – например, порта на оборудовании DSLAM - xDSLмультиплексере доступа).

Режим broadcast используется для передачи данных из одного источника ко всем получателям в заданной подсети. Информацию получают все без исключения абонентские установки. Для этого режима используются адреса, заканчивающиеся на 255, например 192.168.1.255. Если передавать видео в режиме broadcast, то все пользователи, находящиеся в одной подсети, вынуждены будут

смотреть только этот канал. Поэтому данный режим применяется только для передачи каких-либо служебных сообщений.

Режим передачи, который можно назвать самым важным в IPTV – это multicast. Он предназначен для доставки данных группе абонентов и применяется при организации телетрансляций и других услуг массового пользования. Для идентификации групп каналов используется специально зарезервированный для этих целей при разработке протокола IP диапазон адресов – от 224.0.0.0 до 239.255.255.255 (класс D). Multicast предусматривает передачу информации от источника к абонентским мультиплексерам или коммутаторам одним потоком, транслируя далее ее только на те порты, которые эту информацию заказывали. Multicast позволяет существенно сэкономить полосу пропускания в транспортной сети, не требуя отдельного потока для каждого канала к каждому зрителю.

Внедрение IPTV предполагает кардинальную модернизацию инфраструктуры существующих сетей связи. Среди наиболее значимых этапов – создание инфраструктуры сети доступа.

В настоящее время сети доступа развиваются в четырех направлениях:

– беспроводные сети;

– гибридные волоконно-коаксиальные сети (HFC);

– сети на основе существующих медных витых телефонных пар с применением технологии xDSL;

– волоконно-оптические сети.

Технология xDSL – один из самых простых и недорогих способов увеличения численности абонентов по кабельным системам на базе медных витых линий связи. Такой путь считается для операторов одним из самых оправданных и экономичных при предоставлении скорости от 1 до 8 Мбит/с. Но задача предоставления скоростей передачи в несколько десятков Мбит/с на таких системах является не самым простым решением, учитывая плохое качество меди и большие расстояния передачи. Следующим традиционным решением является гибридная волоконно-коаксиальная сеть (HFC, HybridFiber-Coaxial). Главным минусом таких систем считается ограниченная полоса пропускания. При возникновении

трудностей в прокладке кабеля привлекательным считается решение беспроводных сетей. За последние годы все большую популярность получает технология WiFi, которая имеет общую полосу до 300 Мбит/с. Минусом считается то, что для получения данной скорости необходимо минимальное расстояние от данной точки до клиента.

Сеть должна иметь такие характеристики, как широкополосность, гибкость, надежность, управляемость, масштабируемость, удобство в эксплуатации. Только временным выходом из сложившейся ситуации можно считать применение на СД модемов xDSL. При экономии в использовании существующих линейных сооружений существенно ограничивается скорость передачи цифровых потоков. С точки зрения скорости передачи даже самые современные модемы ADSL-2 ADSL-2+ уже сейчас находятся «на грани» требований пользователей. Для потокового видео со стандартным разрешением (SDTV) необходима скорость 17 Мбит/с (в MPEG-2), при передаче же сигналов HDTV потребуется обеспечение скорости передачи 20 Мбит/с (в MPEG-2) или 9 Мбит/с (в MPEG-4). Что касается применения гибридных волоконно-коаксиальных технологий (HFC), то они достаточно хорошо себя проявили только в сетях кабельного телевидения (КТВ).

Из всего вышесказанного можно сделать вывод, что наибольшую привлекательность имеют оптические линии связи, которые способны предоставить максимальные скорости абонентам.

Используется множество вариантов выбора волоконно-оптической технологии доступа:

– использование решений на основе оптических модемов;
– оптического Ethernet;
– технологии Micro SDH;
– на основе пассивных оптических сетей PON.

К наиболее приоритетным на сегодняшний день относят два стандарта PON-сетей:

1) GPON (Gigabit PON), транспортный протокол GFP (generic framing protocol). Нисходящий поток – 1490 нм, 2,4 Гбит/с, восходящий поток – 1310 нм, 1,2 Гбит/с;

2) GEPON (Gigabit Ethernet PON), транспортный протокол – Ethernet. Нисходящий поток – 1490 нм, 1,2 Гбит/с, восходящий поток – 1310 нм, 1,2 Гбит/с.

Учитывая, что услуга IPTV разумно предоставляется пакетом, стоит отметить следующее.

Достаточно мощный профиль услуги можно сформулировать так: одному конечному пользователю должны быть доступны три канала IPTV – один HDTV (15 Мбит/с) и два SDTV (2x4 Мбит/с), доступ в Интернет (2 Мбит/с), доступ к локальным ресурсам (1 Мбит/с), три линии VoIP (0,3 Мбит/с). То есть общий ресурс на одного пользователя составляет порядка 28 Мбит/с при условии, что он пользуется всеми сервисами одновременно. Такой профиль услуг может поддерживаться в одном PON-дереве как для 32 пользователей GEPON, так и для 64 пользователей GPON. На самом же деле передаваемый в многопользовательском режиме (Multicast) трафик, включающий трафик IPTV, в дереве PON для каждого пользователя не дублируется, поэтому все абоненты одного дерева PON могут одновременно смотреть все транслируемые в нем IPTV-каналы (рис. 1). В результате услуги IPTV фактически не налагают ограничений на коэффициент разветвления, а реальная полоса, доступная абоненту, значительно шире.

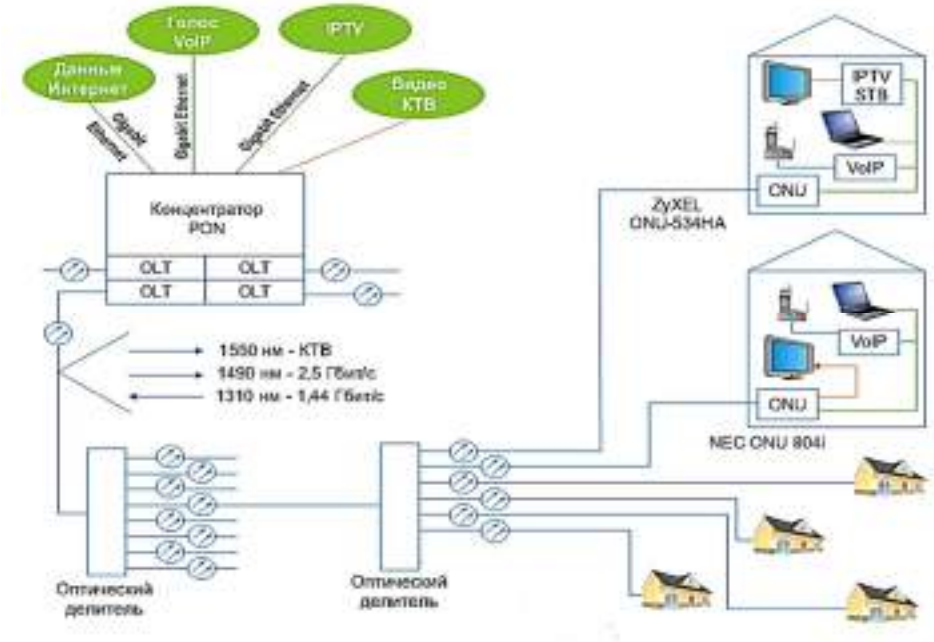


Рис. 1. Мультисервисная сеть GEPON

В GEPON реализация режима Multicast в дереве PON, стандартизованная IEEE, базируется на обработке пакетов с Multicast-адресами и близка к технологиям, применяемым в Ethernet-сетях.

В GPON поддержка Multicast в дереве PON стандартизована ITU-T только для ATM-протокола. При использовании GEM каждый производитель GPON реализует режим Multicast, базируясь на различных дополнениях к протоколу GEM, разрабатываемых самостоятельно либо на основе сторонних патентов.

Решения GEPON используют достаточно простые процедуры конфигурирования и управления, во многом аналогичные процедурам, выполняемым в обыкновенных Ethernet-сетях. Специалистов, занимающихся администрированием Ethernet-сетей, на рынке труда достаточно, и они легко могут освоить администрирование решений PON (рис. 2). Решения GPON, в свою очередь, базируются на совокупности технологий SDH, ATM/GEM и Ethernet, что предъявляет повышенные требования к администрированию сетевой инфраструктуры в целом и к эксплуатирующему персоналу в частности.

X-ки	APON (BPON)	EPON	GPON	GEPON
Институты стандартизации / альянсы	ITU-T SG15 / FSAN	IEEE / EFMA	ITU-T SG15 / FSAN	IEEE / EFMA
Дата принятия стандарта	октябрь 1998	июль 2004	октябрь 2003	Сентябрь 2004
Стандарт	ITU-T G.981.x	IEEE 802.3ah	ITU-T G.984.x	IEEE 802.1ah
Скорость передачи, прямой/обратный поток, Мбит/с	155/155622/155622/622	1000/1000	1244/155,622,12442488/622,1244,2488	1250 / 1250
Базовый протокол	ATM	Ethernet	SDH	Ethernet
Линейный код	NRZ	8B/10B	NRZ	8B/10B
Максимальный радиус сети, км	20	20 (>30)	20	20
Максимальное число абонентских узлов на одно волокно	32	16	64 (128)	64
Коррекция ошибок FEC	предусмотрена	нет	необходима	предусмотрена

Рис. 2. Характеристики PON

Таким образом, выбор в пользу решения GPON или GEPON в условиях конкретной сети связи весьма условен и должен определяться не только параметрами пропускной способности, но и рядом

других аспектов, которым на начальном этапе придают мало значения, что затем негативно сказывается на эксплуатации и развитии сети.

Для российских операторов той минимальной полосы, что предоставляет, например, GPON (30 Мбит/с), с избытком хватит для обычного домашнего пользователя: 12-15 Мбит/с для HDTV (или 2-4 Мбит/с для SDTV, что намного более вероятно), 128 кбит/с для VoIP, а вся остальная полоса – для доступа в Интернет. Если посмотреть на все это в перспективе, то, конечно же, появление нового контента потребует и достаточно объемных каналов, поэтому многие крупные мировые операторы связи уже анонсировали стратегии развития своих сетей. Стоит отметить, что с каждым годом рост потребностей абонентов вынудит операторов переходить на грядущие 10GGPON и 10GEPON.

Список литературы

1. Мир телекома // Сети абонентского доступа на базе технологии PON. –2012. – №1. С. 2-72.

2. Алексеев Е.Б. Оптические сети доступа: учебное пособие. – М.: ИПК при МТУСИ, 2005. – 140 с.

3. Петренко И.И., Убайдулаев Р.Р. Пассивные оптические сети PON. – Ч. 1. Архитектура и стандарты // LightwaveRussianedition. – 2004. – №1. – С. 22-28

УДК 004.738.52

А.Е. Севрюков, А.А. Шабельников

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СПОСОБ УВЕЛИЧЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ UMTSB КУРСКОЙ ОБЛАСТИ

Рассмотрен метод увеличения пропускной способности сети UMTS, в результате которого доходы операторов могут возрасти и покрыть все финансовые издержки, связанные с внедрением технологии.

Сегодня стремительно возрастает спрос на высокоскоростной доступ в Интернет. Количество пользователей глобальной сети неуклонно растет, в том числе пользователей мобильным Интернетом. У абонентов повышается спрос на качественный просмотр видеоматериалов, проведение видеоконференций, быструю загрузку

мультимедийных файлов. Однако невысокие скорости передачи данных не могут в достаточной мере удовлетворить эти запросы. Кроме того, при существующем состоянии UMTS-сетей региона уровень обслуживания будет неуклонно ухудшаться с увеличением количества пользователей услугами сетей.

Одним из путей устранения предложенных недостатков выступает модернизация существующей сети. Основным этапом модернизации может служить внедрение в систему UMTS технологии MIMO.

В этой связи технология MIMO является актуальной и представляет практический интерес.

Общие результаты тестирования UMTS-сетей операторов по г. Курску представлены в таблице.

Результаты тестирования UMTS-сетей по г. Курску

Операторы	Средняя скорость, Мбит/с	Максимальная скорость, Мбит/с	Максимальная скорость
Мегафон	1,0	2,1	HSPA+(21,6 Мбит/с)
Билайн	0,9	2,4	HSPA(14,4 Мбит/с)
МТС	2,0	4,7	HSPA+(21,6 Мбит/с)

Из таблицы видно, что средняя скорость каждого из операторов существенно отстает от заявленной скорости.

Подводя итоги по скоростям, лучший результат как по средней, так и по пиковым скоростям был получен у МТС, далее по средней скорости идет Мегафон, на третьем месте – Билайн, а по пиковым скоростям – сначала Билайн, а затем Мегафон.

Такое качество обслуживания сети явно нельзя назвать удовлетворительным в современных условиях. Сегодняшние запросы пользователей могут удовлетворить средние скорости передачи данных порядка 10 Мбит/с, т. е. модернизация сетей UMTS до 20 категории обслуживания.

Обновив программное обеспечение на оборудовании сети, возможно модернизировать сеть UMTS операторов до этого уровня.

Соответственно, для дальнейшего повышения скорости передачи данных необходимо внедрение принципиально новых техно-

логий. Рабочая группа 3GPP в данном случае предлагает наиболее функциональную технологию – технологию MIMO.

Технология MIMO (MultipleInputMultipleOutput) – множественный вход множественный выход) – это технология, используемая в беспроводных системах связи (WIFI, WI-MAX, сотовые сети связи), позволяющая значительно улучшить спектральную эффективность системы, максимальную скорость передачи данных и емкость сети. Главным способом достижения указанных выше преимуществ является передача данных от источника к получателю через несколько радиосоединений, откуда данная технология и получила свое название.

Для работы технологии MIMO необходимы некоторые изменения в структуре передатчика по сравнению с обычными системами.

В первую очередь, на передающей стороне необходим делитель потоков, который будет разделять данные, предназначенные для передачи на несколько низкоскоростных подпотоков, число которых зависит от числа антенн.

Подробно рассмотрим на примере технологию MIMO 2x2, представленную на рисунке.

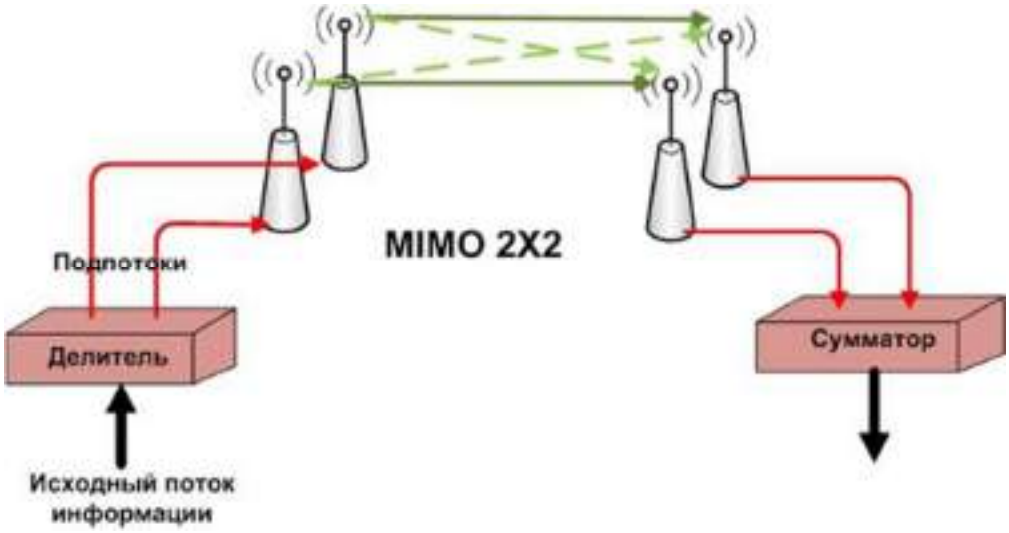


Рис. Принцип работы MIMO

Для MIMO 2x2 и скорости поступления входных данных 100 Мбит/с делитель будет создавать два потока по 50 Мбит/с каждый. Далее каждый из данных потоков должен быть передан через свою антенну. Обычно антенны на передаче устанавливаются с не-

которым пространственным разнесением, чтобы обеспечить как можно большее число побочных сигналов, которые возникают в результате переотражений. В одном из возможных способов организации технологии MIMO сигнал передается от каждой антенны с различной поляризацией, что позволяет идентифицировать его при приеме. Однако в простейшем случае каждый из передаваемых сигналов оказывается промаркированным самой средой передачи (задержкой во времени, затуханием и другими искажениями).

В современных условиях в Курской области можно внедрить только технологию MIMO. Несмотря на высокую экономическую стоимость этого проекта, его внедрение принесет выгоду операторам UMTS-сетей области. В результате модернизации существующих сетей доходы операторов могут возрасти и покрыть все финансовые издержки, связанные с внедрением технологии.

---

1. Бакулин М.Г., Крейнделин В.Б., Шлома А.М. Новые технологии в системах мобильной радиосвязи. – М.:Инсвязьиздат, 2005.

УДК 621.395.4

О.В. Ефимова, Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

БАНК ФИЛЬТРОВ ОРТОГОНАЛЬНОГО РЕЧЕВОГО КОДИРОВАНИЯ

Проводится анализ структуры существующего кодера MPEG с целью применения в речевом кодировании, расчет импульсной характеристики и АЧХ полифазного фильтра.

Актуальным вопросом в разработке указанной темы является эффективное использование выделенного частотного ресурса. Одним из наиболее применяемых решений в сжатии медиапотока с потерями является семейство кодеров MPEG [1]. Данное семейство принадлежит к разновидности ортогональных кодеров. Структура кодера MPEG – 1/AudiolayerIII содержит в себе полифазный банк фильтров, состоящий из 32 цифровых полосовых фильтров. Главной задачей блока фильтрации является подготовка временного потока к частотному ортогональному преобразованию. Режим работы кодера MPEG подразумевает сжатие полосы потока в диапазоне 20–20000 Гц. Ввиду того, что эффективная полоса речи со-

ставляет около 20% данного диапазона, актуально провести расчет и синтез модифицированного банка фильтров для речевого кодирования.

В данной работе представлена методика расчета цифрового полосового фильтра, применяемого в ортогональном речевом кодировании. Так как эффективно передаваемая полоса частот речи составляет 300 – 3400 Гц, то нет необходимости в применении 32-полосного банка фильтров, достаточно провести расчет 14 барков, куда входят 4-17 диапазоны изначального полифазного фильтра.

Методика расчета банка фильтров заключается в следующем. В общем случае принцип работы дискретного фильтра можно представить в виде разностного уравнения импульсной характеристики (1) [1]:

$$y(k) = b_0 x(k) + \ldots + b_m x(k-m) - a_1 y(k-1) - \ldots - a_n y(k-n), \quad (1)$$

где a_i и b_j – вещественные коэффициенты;

k – отчет на выходе фильтра $y(k)$.

В силу особенностей ФЧХ цифровых фильтров для построения полифазного фильтра необходимо использовать КИХ фильтры. Для КИХ фильтра выходные отчеты $y(k)$ зависят только от входных отчетов, поэтому он имеет конечную импульсную характеристику, а отсчеты импульсной характеристики фильтра КИХ полностью совпадают с коэффициентами b_j.

Для расчета импульсной характеристики необходимо выбрать количество коэффициентов КИХ фильтра с целью обеспечения заданной переходной полосы, а также синтезировать оконную функцию с целью обеспечения заданного подавления в полосе заграждения [2]:

$$h_n = \begin{cases} \dfrac{\psi \times p_n \times (\sin(\omega_2 \times n) - \sin(\omega_1 \times n))}{\pi \times n} & if \ \ n \geq 1 \\ \omega_0 \ \text{otherwise} \end{cases}, \quad (2)$$

где ψ – коэффициент передачи фильтра;

p_n – весовая функция, противодействующая явлению Гиббса [2]:

$$p_n = 1 - \frac{n}{\theta \times N}, \quad (3)$$

где n – количество входных временных отсчетов;

θ – весовой коэффициент;

N – сглаживающий коэффициент.

Методика расчета импульсной характеристики приведена ниже. Нижняя частота с учетом масштаба дискретизации определяется выражением (4). Верхняя частота с учетом масштаба определяется согласно формуле [4]:

$$f_1 := \frac{f_н}{8000}; \qquad f_2 := \frac{f_в}{8000}. \tag{4}$$

Циклическая частота, определяется формулой для нижней и верхней частоты [3]:

$$\omega_1 := 2 \times \pi \times f_1; \quad \omega_2 := 2 \times \pi \times f_2. \tag{5}$$

Нулевой отчет импульсной характеристики фильтра определяется выражением [3]

$$\omega_0 := \frac{(\omega_2 - \omega_1)}{\pi}. \tag{6}$$

Для каждого из фильтров коэффициенты подбираем индивидуально. Проведем расчёт коэффициентов цифрового нерекурсивного фильтра на примере следующего критического интервала частот:

Диапазон 4 [3], центральная частота 350 Гц, ширина 300 – 400 Гц:

$f_1 := \frac{300}{8000}$ Гц, нижняя частота с учетом масштаба;

$f_2 := \frac{400}{8000}$ Гц, верхняя частота с учетом масштаба;

Определим циклические частоты для f_1 и f_2:

$\omega_1 := 2 \times \pi \times f_1$,

$\omega_1 = 0.236$ Рад/с,

$\omega_2 := 2 \times \pi \times f_2$,

$\omega_2 = 0.314$ Рад/с.

Нулевой отчет импульсной характеристики фильтра:

$$\omega_0 := \frac{(\omega_2 - \omega_1)}{\pi}.$$

Частота дискретизации определяется согласно выражению $f = \frac{1}{\Delta t}$, $\Delta t = 125 \times 10^{-6}$, тогда $f = 8 \times 10^{3}$ Гц; $n = 0...31$ – диапазон отчетов.

Для данного фильтра индивидуально подбираем следующие коэффициенты:

$N = 61$ – сглаживающий коэффициент;

$\Psi = 38$ – коэффициент передачи фильтра;

$\Theta = 0{,}6$ – весовой коэффициент.

Импульсная и амплитудно-частотная характеристики цифрового фильтра приведены на рисунке.

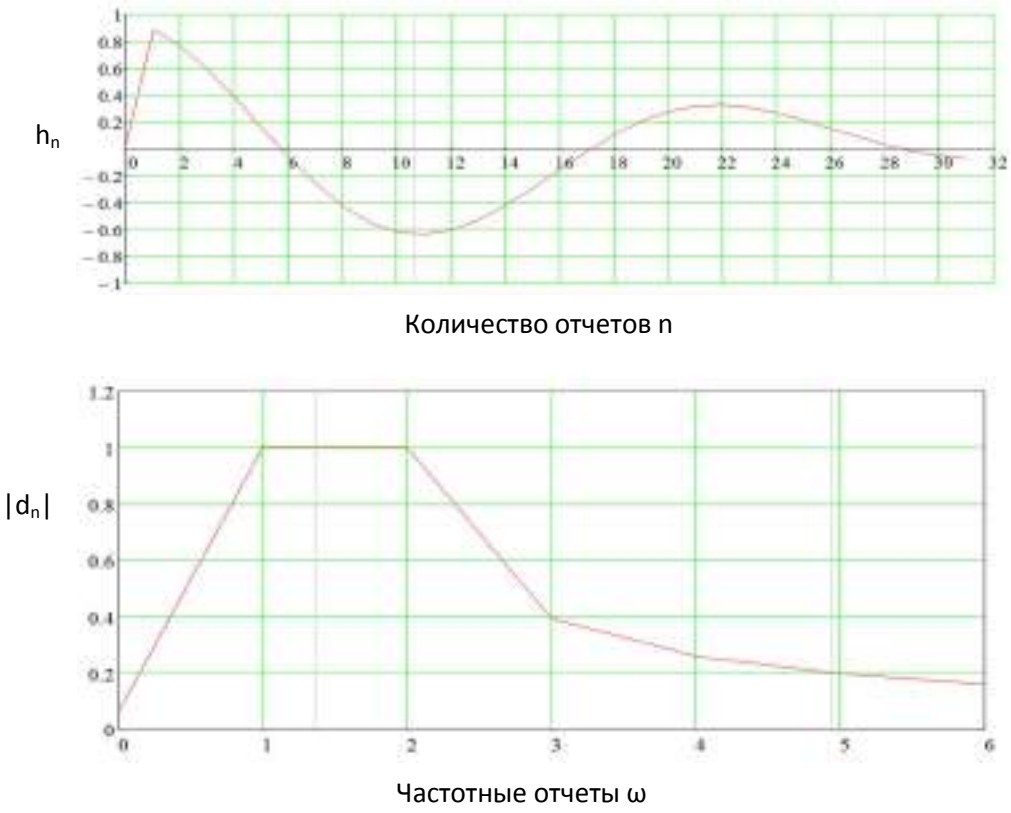


Рис. Импульсная характеристика h_n и АЧХ(БПФ) $|d_n|$

Для данной импульсной характеристики число коэффициентов КИХ фильтра представлено в таблице.

Значения коэффициентов КИХ фильтра
для диапазона частот 300 – 400 Гц

№ п/п	0	1	2	3	4	5	6
Значение коэффициента	0,025	0,889	0,765	0,591	0,383	0,159	-0,062
№ п/п	7	8	9	10	11	12	13
Значение коэффициента	-0.062	-0.063	-0429	-0.551	0.622	-0.64	0.608
№ п/п	14	15	16	17	18	19	20
Значение коэффициента	-0.532	-0.424	-0.294	-0.155	-0.019	0.104	0.203
№ п/п	21	22	23	24	25	26	27
Значение коэффициента	0.274	0.315	0.324	0.307	0.267	0.212	0.149
№ п/п	28	29	30	31	-	-	-
Значение коэффициента	0.086	0.028	-0.018	-0.069	-	-	-

По приведённой методике рассчитываются коэффициенты фильтров всего диапазона речи, конкретно для каждого барка. Весовые и сглаживающие коэффициенты функции, ослабляющей эффект Гиббса, выстроить в строгую математическую последовательность не представляется возможным, поэтому каждый барк определяется индивидуально исследователем. Результатом синтеза является набор временных коэффициентов импульсной характеристики для каждого поддиапазона.

Список литературы

1. Сергеенко А.Б. Цифровая обработка сигналов. – СПб.: Питер, 2003.– 604 с.

2. Расчет КИХ фильтра с линейной фазочастотной характеристикой методом частотной выборки с применением оконного сглаживания [Электронный ресурс]. – URL: http://www.dsplib.ru/content/filters/firwin/firwin.html.

3. Применение цифровой фильтрации в медико-биологической практике. Общие понятия цифровой фильтрации [Электронный ресурс]. – URL: http://do.gendocs.ru/docs/index-214103.html.

УДК 621.395.4

Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА ДЕСКРИПТОРА ДАННЫХ ПО ДИНАМИЧЕСКОМУ СЛОВАРЮ

Представлена алгоритмическая последовательность дескрипции формата динамического Deflate.

Восстановление динамически сжатого Deflate (первый и второй бит первого байта – 10) происходит посредством построения трёх деревьев Хаффмана, каждое из которых определяет последующий код символов и, главное, код окончания. В данном случае он в каждом блоке различен и, не определив деревья, невозможно обнаружить конец блока.

Особенностью динамического словаря является не только уникальность кодов символов для каждого блока, но и двойное кодирование по Хаффману. Сжатию подвержена также и размерность кода для литералов длин/символов и дистанций. С целью более компактного размещения кодов словаря неиспользуемые литералы и дистанции не входят в систему деревьев. Их точное количество определяют первые байты блока.

№ байта	1								2								3							
№ бита	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
алфавиты	HLIT					тип		б	HCLEN			HDIST												HCLEN
№ бита	4	3	2	1	0				2	1	0	4	3	2	1	0								3

Методика нахождения размера алфавитов следующая.

1. Читать пять бит в прямом порядке. Вычислить размер алфавита длин/символов по формуле HLIT = 257 + {5 бит}.

2. Читать пять бит в прямом порядке. Вычислить размер алфавита дистанций по формуле HDIST = 9 + {5 бит}.

3. Читать 4 бита в прямом порядке. Вычислить размер алфавита длин кодов Хаффмана HCLEN = 4 + {4 бита}.

Первыми необходимо определить размеры кодов для дерева длин кодов Хаффмана.

Последовательность нахождения следующая.

1. Размеры кодов считывать подряд по три бита (количество трёхбитных чисел определено в HCLEN, максимум 19), переводить в декартовое счисление и последовательно вносить в порядке, показанном в таблице 1. Максимальное значение длины кода равно 7.

Таблица 1

Нахождение размера кодов Хаффмана

Символ алфавита длин	16	17	18	0	8	7	9	6	10	5
Длина кода символа	{3}	{3}	{3}	{3}	{3}	{3}	{3}	{3}	{3}	{3}
Символ алфавита длин	11	4	12	3	13	2	14	1	15	
Длина кода символа	{3}	{3}	{3}	{3}	{3}	{3}	{3}	{3}	{3}	

2. Выполнить поиск значений кодов Хаффмана в лексикографическом порядке: значению младшего кодового значения соответствует высший литерал алфавита.

Методика нахождения кодов по известным длинам происходит следующим образом:

1. Найти самый длинный код и задать все его разряды единицами. Например, если длина кода 5, то – 11111.

2. Назначить все последующие коды данной длины, декрементировав каждый относительно предыдущего (количество кодов взять из таблицы 1).

3. При переходе на более короткую длину кода произвести побитный сдвиг вправо на один бит.

4. Перейти в пункт 2, если не все коды длин найдены, иначе – перейти в пункт 5.

Пример нахождения 4 кодов дерева по длине 5:

Длина кода 5	1	1	1	1	1	Декрементировать
Длина кода 5	1	1	1	1	0	Декрементировать
Длина кода 5	1	1	1	0	1	Декрементировать
Длина кода 5	1	1	1	0	0	Сдвинуть на бит вправо и декрементировать
Длина кода 4		1	1	0	1	Декрементировать…

5. Перестроить таблицу 1 в лексикографическом порядке: младшей длине кода соответствует меньший код, но, не нарушая соответствия столбцов таблицы 1 и длины кода. Это и есть первое дерево.

Таблица 2

Нахождение кодов размера большого алфавита

Символ алфавита длин	1	2	3	4	5	6	7	8	9	10
Длина кода символа	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC
КодХаффмана	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN
Символ алфавита длин	11	12	13	14	15	16	17	18	19	
Длина кода символа	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	
КодХаффмана	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	

Интерпретация 19-ти значений длин кодов:

0 – 15: Представляют длины кодов 0 – 15 для большого алфавита литералов.

16: Копировать предыдущую длину кода от 3 до 6 раз. Следующие 2 бита в прямом порядке указывают длину повторения.

17: Повторить длину кода 0 от 3 до 10 раз. Следующие 3 бита в прямом порядке указывают длину повторения.

18: Повторить длину кода 0 от 11 до 138 раз. Следующие 7 бит в прямом порядке указывают длину повторения.

Теперь, зная коды Хаффмана для длин большого алфавита литералов, находим размеры их кодов:

№ литерала длины/символа	Размер кода из табл.6	Код Хаффмана по дереву
0	DEC	{BIN}
1	DEC	{BIN}
2	DEC	{BIN}
3	DEC	{BIN}
… …	… …	… …
285	DEC	{BIN}

1. Читать первый бит и последующие (согласно дереву Хаффмана каждый последующий бит точно определят сам код и его размер), определить код длины из модифицированной таблицы 2. Если символ оказывается 16, 17 или 18, читать дополнительные биты. Установить соответствующие нулевые (если 17 или 18) и повторные значения длин кода (если 16) для большого алфавита литералов.

2. Читать следующие биты и устанавливать соответствия литералов длинам их кодов до последнего, определенного HLIT. Максимальное значение 285.

3. Найти все коды Хаффмана для HLIT, зная их длины, по методике, описанной выше.

4. Установить лексикографическое соответствие между литералами и кодами Хаффмана, найденными в пункте 3. Получим дерево для основного алфавита литералов.

5. Читать следующий бит, найти длины кодов алфавита дистанций согласно модифицированной таблице 2. Максимальное значение HDIST 29.

6. Установить лексикографическое соответствие для кодов Хаффмана по их длинам. Получим третье дерево алфавита дистанций:

Символ алфавита дистанций	0	1	2	3	4	5	6	7	8	9
Длина кода символа	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC
КодХаффмана	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN
Символ алфавита дистанций	10	11	12	13	14	15	16	17	18	19
Длина кода символа	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC
КодХаффмана	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN
Символ алфавита дистанций	20	21	22	23	24	25	26	27	28	29
Длина кода символа	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC	DEC
КодХаффмана	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN	BIN

Первое дерево для длин кодов Хаффмана, состоящее из 4-19 значений (табл. 1), больше не понадобится. Далее последовательно читаем в обратном порядке коды исходных символов их повторений:

1. Читать в обратном порядке биты и искать соответствие в таблице литералов/длин.

а) Если найден литерал (0-255), записать в результат.

б) Если длина повтора (257-285), читать дополнительные биты в прямом порядке. Определить длину повтора. Далее читать в обратном порядке биты и искать соответствие в алфавите дистанций, читать дополнительные биты для дистанций. Определить ди-

станцию. Отсчитать влево от последнего найденного байта дистанцию, копировать количество символов соответственно длине повтора и вставить в конец, вслед за последним найденным.

в) Если найден код Хаффмана для символа 256 – это означает конец блока.

---

1. Deutsch P. GZIP file format specification version 4.3 [Electronic resource]. – URL: ftp://ftp.uu.net/graphics/png/documents /zlib/zdoc-index.html/

УДК 621.394.74

Д.А. Калабин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВЛИЯНИЕ УСЛОВИЙ ЭКСПЛУАТАЦИИ НА ПАРАМЕТРЫ ТЕРМОЭЛЕКТРИЧЕСКИХ ИСТОЧНИКОВ АЛЬТЕРНАТИВНОГО ЭЛЕКТОРОПИТАНИЯ

В настоящее время автономные источники электрической энергии на основе термоэлектрических генераторных модулей находят применение для питания маломощных передатчиков.Они обладают такими уникальными качествами, как полная автономность, высокая надежность, простота эксплуатации, бесшумность и долговечность, но только соблюдение условий эксплуатации позволяет использовать их наиболее эффективно.

Для получения наибольшей эффективности и надежности работы ТГМ необходимо руководствоваться следующими ключевыми принципами.

Горячая и холодная поверхности, на которые будет установлен модуль, должны иметь высокую плоскостность: не хуже 20 мкм в базовом варианте. При этом для получения наилучшей эффективности, особенно в случае применения модулей с улучшенной плоскостностью и параллелизмом (L2 и L3), рекомендуемое значение плоскостности – от 10 до 5 мкм. Плоскостность влияет на качество контакта горячей и холодной поверхности со сторонами модуля.

Генераторный модуль должен быть соответствующим образом установлен между источником тепла и холодным радиатором. Для достижения наилучшего результата и сохранения работоспособности генераторного модуля в течение срока эксплуатации

необходимо обеспечить усилие сжатия порядка 1–1,5 кН для модуля размером 40×40 мм. Для оптимизации нагрузки в период эксплуатации целесообразно использовать пружины совместно с резьбовыми соединениями. Недостаточное усилие сжатия приводит к уменьшению мощности, выдаваемой модулем.

Температура горячей стороны ТГМ не должна превышать заданную в спецификации.

Край металлической поверхности источника тепла, соприкасающейся с ТГМ, должен выходить за границы модуля, желательно на 10 мм и более с каждой стороны. Данная мера способствует более равномерному распределению потока тепла на краях модуля.

Температура поверхности модуля должна быть максимально равномерной. В случае если источник тепла и/или радиатор холодной стороны изготовлены не из меди, рекомендуется применять промежуточные медные пластины для предотвращения неравномерного температурного поля.

Для увеличения потока тепла, проходящего через модуль, диаметр стягивающих болтов конструкции ТЭГ должен быть по возможности минимальным. Материал болтов желательно выбирать с минимальной теплопроводностью (например, нержавеющая сталь).

Для обеспечения наилучшего теплового контакта ТГМ с источником тепла и радиатором холодной стороны необходимо применять теплопроводную пасту. Слой термопасты должен быть по возможности минимальным для сохранения прямого контакта между керамической поверхностью модуля и металлом.

Для получения максимальной генерируемой мощности конкретный тип модуля должен быть выбран с учетом характеристик элементов конструкции ТЭГ, радиатора, интерфейсных материалов и др.

Важной характеристикой модуля является его тепловое сопротивление R_t, выбирать которое следует исходя из следующего соотношения:

$$R_t \sim k \times \left(R_c + R_h\right), \qquad (1)$$

где k – численный коэффициент, равный 1–1,5;

R_c – тепловое сопротивление между охлаждаемой стороной и окружающей средой, К/Вт;

R_h – тепловое сопротивление между нагреваемой стороной ТГМ и источником теплоты с заданной температурой, К/Вт.

Выводы

Эксплуатация ТГМ, несмотря на внешнюю простоту, имеет ряд правил и важных нюансов, несоблюдение которых ведет к понижению эффективности и надежности его работы. А это, в свою очередь, ведет к снижению мощности, выдаваемой ТГМ, и увеличению количества сбоев подключенной к модулю аппаратуры.

Все принципы эксплуатации ТГМ направлены на обеспечение наилучшего механического и теплового контакта горячей и холодной поверхности со сторонами модуля, максимально равномерной температуры поверхности модуля и на увеличение потока тепла, проходящего через модуль.

---

1. Бурштейн А. И. Физические основы расчета полупроводниковых термоэлектрических устройств. – М: Физматгиз, 1962. – 383 с.

2. Тахистов Ф. Ю. Оптимизация параметров термоэлектрического генераторного модуля с учетом эффективности теплообмена на сторонах модуля. – СПб.: Изд-во ФТИ, 2008. – 272 с.

УДК 004.75

И.О. Харитонов, А.А. Гуламов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РАСШИРЕНИЕ СФЕР ПРИМЕНЕНИЯ ОДНОМОДОВЫХ ВОЛС ЗА СЧЕТ ПРЯМОГО ПОДКЛЮЧЕНИЯ НЕПОСРЕДСТВЕННО К АТМОСФЕРНЫМ ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ

Рассмотрена перспективность применения АОЛС при прямом подключении непосредственно к ВОЛС в городских условиях.

Технология атмосферных оптических линий связи (АОЛС) основана на использовании атмосферы в качестве среды распространения светового излучения и позволяет передавать любые потоки данных на ограниченные расстояния.

Передача сигнала происходит по лучу, имеющему высокую направленность. Перехватить его практически невозможно, что обеспечивает высокую безопасность каналов связи. Наибольший выигрыш от использования инфракрасных каналов достигается там, где необходимо установить соединение без больших затрат, в короткие сроки или на временной основе. Уже сегодня преимуще-

ства АОЛС-технологии помогают сотовым операторам при оперативном подключении базовых станций, особенно эффективно проявив себя при подключении микростанций в торговых комплексах, бизнес-центрах, гостиницах.

В АОЛС на основе лазера с дифракционно-ограниченным пучком реализуется вариант передачи–приема сигнала напрямую одномодовой ВОЛС, что позволяет создать многогигабитный канал класса точка-точка. АОЛС, как показано на рис. 1 и 2, обладают несколькими особенностями, такими как гибкость эксплуатации, легкость установки, отсутствие необходимости лицензирования, и являются линиями связи прямой видимости [1,2].

Рис. 1. Применение АОЛС в городских условиях

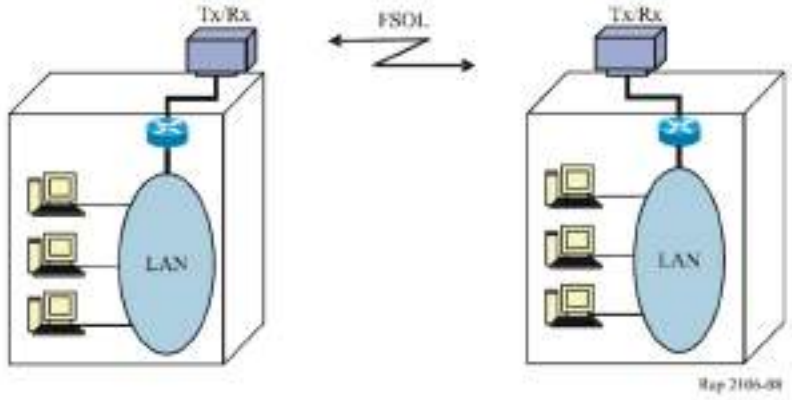


Рис. 2. Соединение или расширение локальных сетей двух зданий при помощи АОЛС

В типичных условиях наземной линии бесшовное соединение АОЛС между несколькими одномодовыми ВОЛС позволяет создавать беспроводные широкополосные каналы связи не только для фиксированных терминалов, но также для мобильных пользователей, таких как спутники, автомобили, поезда, корабли и самолеты, для связи с которыми невозможно использовать ВОЛС.

При использовании одномодовых ВОЛС в сочетании с АОЛС существующие ВОЛС с технологиями спектрального уплотнения и оптических усилителей на волокне, легированном эрбием, а также мультиплексоров и демультиплексоров, использующих решетки на основе массива волноводов, могут применяться без модификаций АОЛС.

Однако АОЛС подвержены воздействию неблагоприятных погодных условий, а климат сильно отличается в разных странах и регионах. Следовательно, очень важно знать характеристики широкополосных атмосферных оптических каналов для поддержки дальнейшего изучения совместимости с различными погодными условиями и оценки характеристик до перехода к стадии эксплуатации.

На рисунке 3 показана базовая конфигурация терминала, который напрямую соединяет две одномодовые ВОЛС по атмосферному каналу [1]. Преломляющая оптическая система используется как оптическая антенна (ОА) для фокусировки в коллимированный пучок луча на длине волны 1550 нм. Апертура ОА может быть изменена в пределах от 10 мм до 42 мм, в зависимости от протяженности атмосферного канала связи. Внутренний диаметр коллимированного пучка остается при этом неизменным и равен 2 мм.

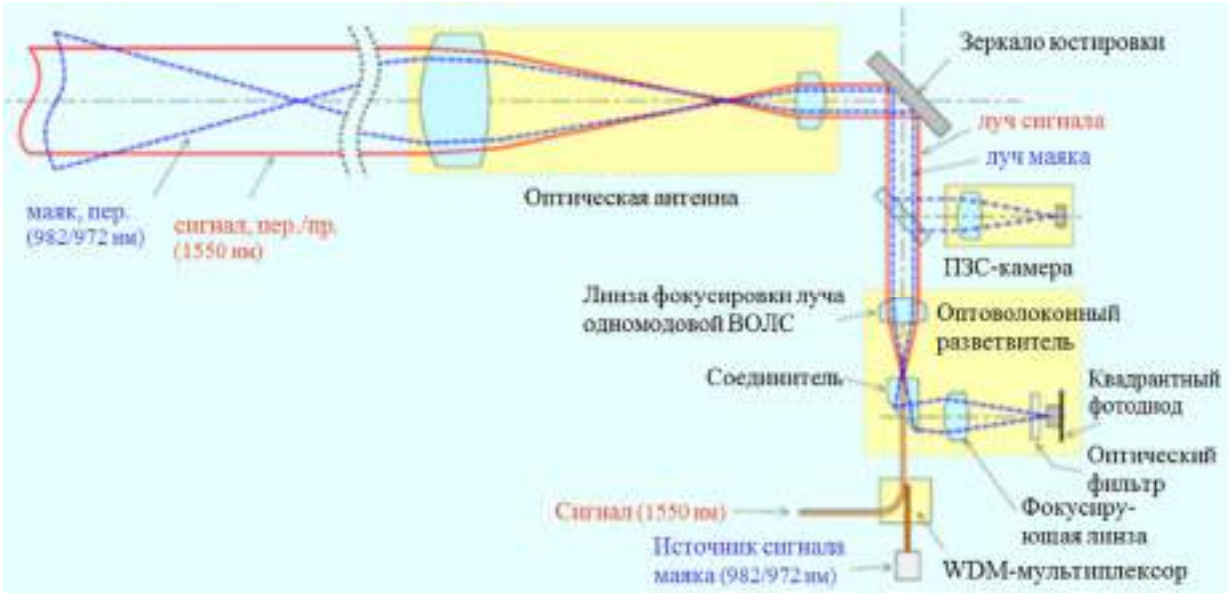


Рис. 3. Устройство терминала АОЛС-одномодовая ВОЛС

На выходе ОА установлено юстировочное зеркало, перемещаемое в двух плоскостях, что позволяет стабилизировать наклон луча, вызванный вибрациями, тепловой деформацией опорных кон-

струкций, атмосферными турбулентностями. Отъюстированный луч фокусируется на апертуре одномодового оптоволокна в оптическом разветвителе. Для обнаружения положения пятна луча сигнала маяка используется квадрантный фотодиод (КФ). В соответствии с сигналами ошибок от квадрантного фотодиода аналоговый пропорционально-интегрально-дифференциальный (ПИД) сервоконтроллер управляет юстировочным зеркалом, чтобы свести к минимуму влияние отклонения угла приходящего сигнала.

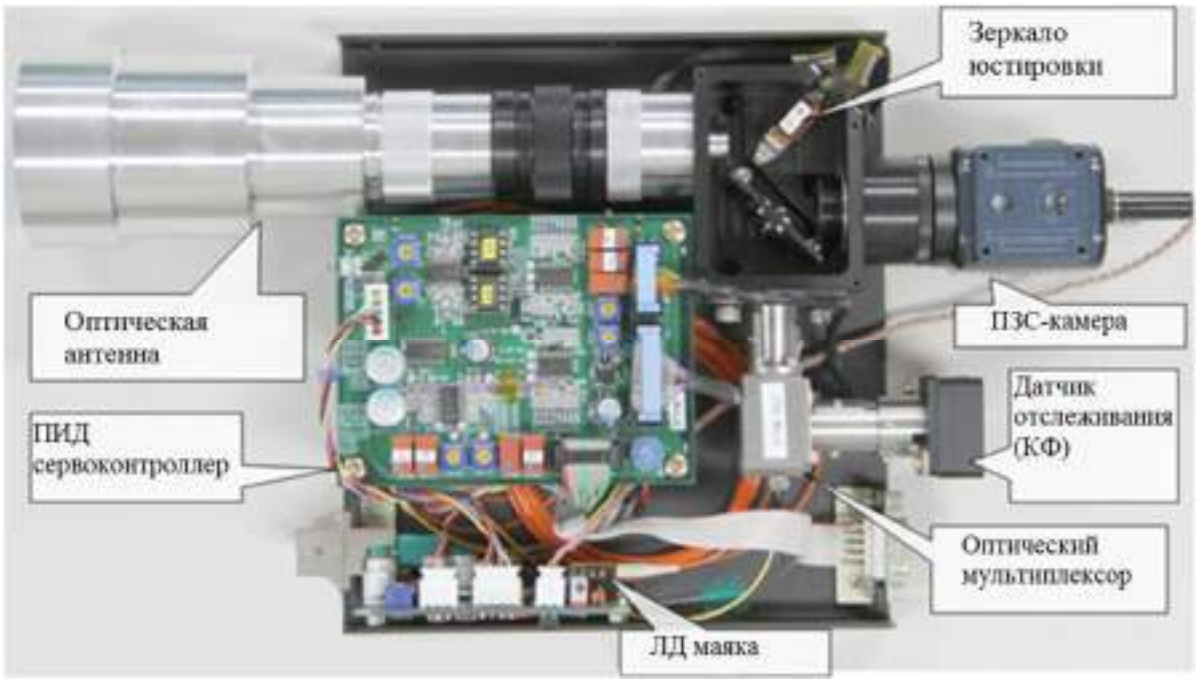


Рис. 4. Внутреннее устройство терминала АОЛС-одномодовая ВОЛС [1]

После цикла работы сервоконтура передаваемый сигнал мультиплексируется с сигналом маяка в WDM-мультиплексоре. Затем сигнал передается на оптическую антенну для отправки к противоположному терминалу. Данная технология позволяет достигать скоростей передачи до 1,28 Тбит/с.

---

1. Apt report. Direct single-mode-fiber coupled free-space optical communications to expand the flexibility in fiber-based services. No. APT/ASTAP/REPT-9 / Edition: March 2013 / Document: ASTAP-21/OUT-11. – Bangkok (Thailand), 2013.

2. Технология АОЛС (FSO) и решение проблемы последней мили [Электронный ресурс].– URL: http://www.micromax.ru/about/faq/dict-2.shtml.

СЕКЦИЯ 2
ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

УДК 004.091

С.Н. Михайлов, К.И. Агапченко

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СПОСОБ ИНФОЛОГИЧЕСКОЙ ОБРАБОТКИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН ДЛЯ ОЦЕНКИ ПОДОБИЯ ТЕМАТИЧЕСКОГО СОДЕРЖАНИЯ ЛЕКЦИОННЫХ КУРСОВ

Представлен разработанный способ смысловой обработки текста для выявления дублирования информации в лекционных материалах кафедры ЗИ и СС и последующей оптимизации учебного процесса.

В настоящее время инфологические системы находят применение в различных областях структурирования знаний. Основной особенностью инфологической системы является ее возможность выявления и наглядного представления пользователю смыслового содержания документа.

Инфологическая обработка текстового документа в общем случае предполагает строго упорядоченную последовательность действий, направленных на выявление семантического содержания выбранных текстов.

На первом этапе выполняется нормализация текста, представляющая собой приведение его к виду, в котором все слова приведены в нормальную (базовую) форму и исключены стоп-слова (союзы, местоимения и т.д.).

На втором этапе осуществляется сегментация на синтаксические единицы и определение рейтинга связок слов с целью формирования иерархических понятий текста.

На последующих этапах осуществляется процедура наглядного представления иерархии понятий текста путем отображения понятийного графа текста, в узлах которого находятся термины, а дугами обозначаются связи между ними. Таким образом, в результате инфологической обработки документа может быть сформирована понятийная иерархия текста, отражающая компактное компьютерное представление семантики текста, строго соответствующее семантическому содержанию исходного документа. Визуальный

граф понятийной иерархии, представляемый оператору, является аналогом иероглифической записи документа, позволяющим воспринимать содержимое текста не последовательно, а моментально.

Описанная процедура инфологической обработки текста может быть положена в основу создания нового способа оценки подобия тематического содержания лекционных курсов путем сравнения понятийных иерархий рабочих программ дисциплин выбранного направления подготовки студентов.

Таким образом, разработка способа инфологической обработки рабочих программ дисциплин для оценки тематического подобия содержания лекционных курсов является актуальной и представляет практический интерес.

В условиях перехода высших учебных заведений на выполнение требований и стандартов третьего поколения указанный способ может быть использован для автоматизации процесса выявления степени отражения компетенций в конкретных дисциплинах направления подготовки.

В ходе разработки способа инфологической обработки для оценки тематического подобия содержания лекционных курсов был сформирован методологический подход, содержащий 8 этапов:

Этап 1 – Выбор информативных документов, наиболее интенсивно используемых в деятельности кафедры и хранящихся в информационных ресурсах.

Этап 2 – Структурная декомпозиция тематического содержания документов.

Этап 3 – Нумерация документов и содержащихся в них тем.

Этап 4 – Создание архива документов и приведение их к единому формату.

Этап 5 – Инфологическая обработка документов архива на основе формирования упорядоченной совокупности тематических запросов.

Этап 6 – Последовательный анализ признаков обнаружения подобия тематического содержания запроса в имеющихся архивных данных.

Этап 7 – Принятие решения о тематическом сходстве содержания в различных обработанных документах.

Этап 8 – Идентификация тематик, содержащих семантическое подобие в различных документах.

Данная методология легла в основу создания технологии, в которой авторами была определена последовательность операций, необходимых для оценки подобия тематического содержания рабочих программ дисциплин по направлению подготовки 210700.62 «Инфокоммуникационные технологии и системы связи».

Апробация разработанной технологии проводилась в ходе выполнения эксперимента, задачей которого была оценка возможности применения инфологической системы для реализации автоматизированного процесса выявления тематического подобия содержания документов, хранящихся в информационных ресурсах. В качестве информационного ресурса выбрана электронная библиотека сервера кафедры ЗИ и СС.

В качестве документов отобраны шестнадцать программ дисциплин профессионального направления подготовки бакалавров кафедры. При этом каждому из N документов был присвоен идентификационный номер (от 1 до 16) для последующего удобства администрирования данных ресурсов (N_i, i=1,2…16).

В каждом N_i документе проведена структурная декомпозиция содержащегося в нем тематического материала. В результате каждой теме конкретной дисциплины присвоен оригинальный идентификационный номер Ti.I, где i – номер дисциплины, I– номер темы, которая изучается в i-й дисциплине. Таким образом был создан нумерованный список тем лекционных материалов по каждой дисциплине. Первая дисциплина содержала 14 тем (номера T1.1 – T1.14), вторая – 6 тем (T2.1 – T2.6), в третьей имелось 5 тем (T3.1 – T3.5) и, наконец, в четвертой 20 тем (T4.1 – T4.20).

Все 16 полученных документов были сохранены в едином формате с расширением «doc», так как это принципиально при использовании имеющегося макета инфологической системы.

На рисунке 1 представлен сформированный список.

На очередном этапе эксперимента сформирован архив документов, который будет использоваться непосредственно инфологической системой для смысловой обработки.

Загрузив архив из 16 документов в программный макет инфологической системы, пользователь получает возможность отображения понятийного окружения каждого документа визуального графа понятийной иерархии.

На рисунке 2 показан вариант визуального графа понятийной иерархии.

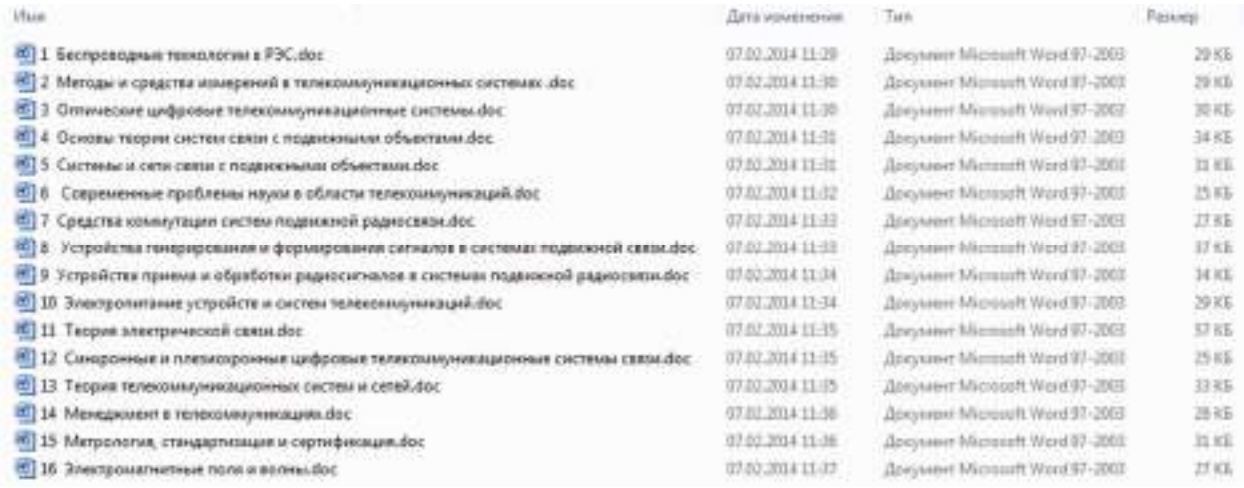


Рис. 1. Нумерованный список документов, участвующих в эксперименте

Рис. 2. Визуализация семантического окружения текста для документа 1 – «Беспроводные технологии в РЭС»

На следующем этапе эксперимента реализована инфологическая обработка документов архива на основе упорядоченной совокупности тематических запросов. В данном случае в качестве запроса принимается одна тематическая единица документа, т.е. одна нумерованная тема лекционных материалов каждой дисциплины.

Для создания запросов использованы первые четыре архивных документа, представляющие собой РПД:

1. Беспроводные технологии в РЭС.
2. Методы и средства измерений в телекоммуникационных системах.
3. Оптические цифровые телекоммуникационные системы.
4. Основы теории систем связи с подвижными объектами.

Такой подход обеспечил формирование 45 запросов.

Сформированные запросы последовательно вводились в окно поиска инфологической системы, после чего производилась смысловая обработка всех документов архива на предмет оценки тематического подобия запроса в содержании каждого из документов. Документы, в которых обнаружено семантическое сходство с тематикой запроса, представлялись в виде перечня в окне поиска, как это показано на рисунке 3.

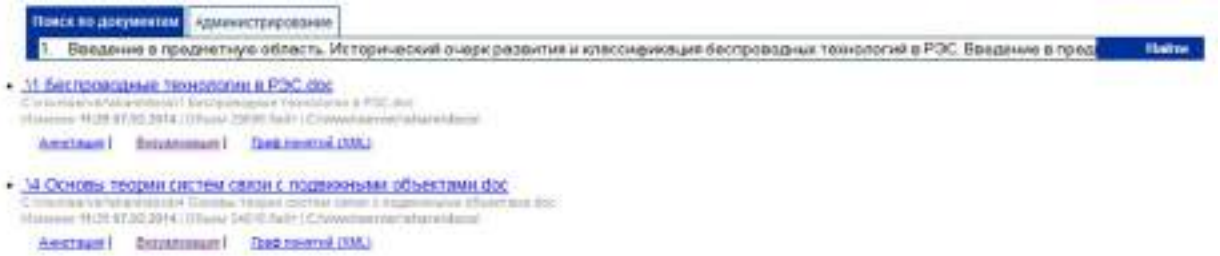


Рис. 3. Результат тематического запроса к документам архива на предмет семантического подобия по теме 1.1

Выполняя последовательный поиск по каждому запросу, пользователь получает возможность определить полный перечень дисциплин, в которых освещается та или иная тема по всему направлению подготовки.

Обобщенные результаты инфологической обработки 16 РПД по четырем темам из 45 представлены в таблице.

Анализ представленных результатов показывает, что отдельные темы имеют смысловое подобие в 7 и более дисциплинах. Указанный результат подтверждает тот факт, что отдельные темы одной дисциплины в ходе учебного процесса могут иметь многократное дублирование в нескольких других дисциплинах.

На рисунках 4 и 5 графически представлены обобщенные результаты эксперимента, отражающие количественные и качественные характеристики обнаруженных дублирований.

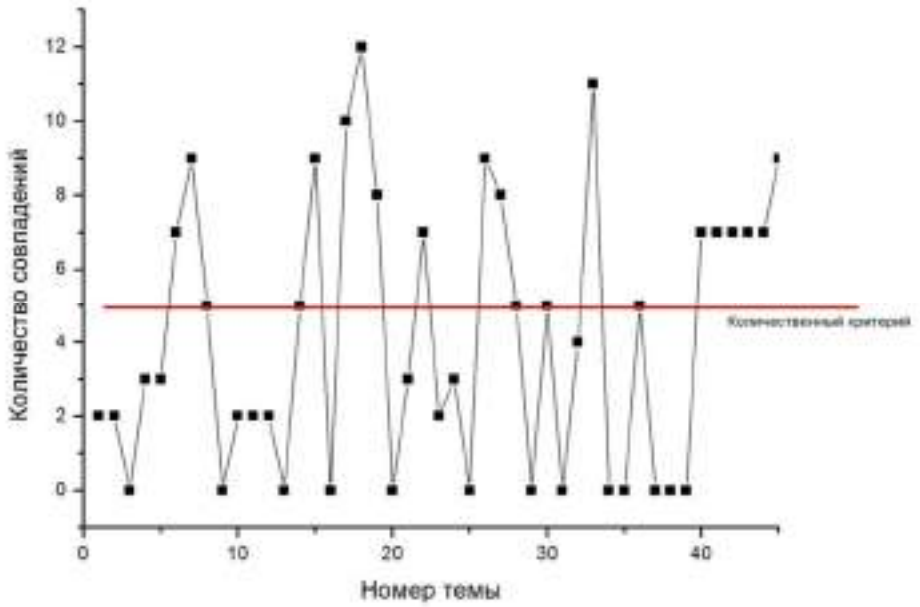


Рис. 4. Количество обнаруженных смысловых подобий тем в разных дисциплинах

Результаты произведенных в эксперименте запросов

№ дисци-плины	№ темы	Кол-во совпавших	Номера совпавших дисциплин
1	1.1	2	1, 4
	1.2	2	1, 4
	1.3	0	-
	1.4	3	1, 3, 4
	1.5	3	1, 4, 5
	1.6	7	1, 2, 4, 5, 11, 12, 13
	1.7	9	1, 2, 3, 4, 7, 9, 11, 12, 15
	1.8	5	1, 3, 4, 5, 13
	1.9	0	-
	1.10	2	1,10
	1.11	2	2,11
	1.12	2	1,4
	1.13	0	-
	1.14	5	1, 3, 4, 5, 6
2	2.1	9	2, 5, 6, 7, 9, 10, 11, 13, 15
	2.2	0	-
	2.3	10	2, 3, 4, 5, 6, 8, 11, 12, 13, 15
	2.4	12	2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 15
	2.5	8	2, 3, 4, 5, 8, 11, 13, 15
	2.6	0	-

Окончание табл.

№ дисциплины	№ темы	Кол-во совпавших	Номера совпавших дисциплин
3	3.1	3	1, 2. 3, 4, 8, 11, 12, 13, 15
	3.2	7	2, 3, 6, 8, 9, 11, 15
	3.3	2	3, 13
	3.4	3	5, 8, 12
	3.5	0	-
4	4.1	9	1, 4, 5, 8, 9, 10, 11, 12, 15
	4.2	8	1, 4, 5, 9, 10, 11, 12, 13
	4.3	5	1, 2, 4, 9, 10
	4.4	0	-
	4.5	5	3, 4, 8, 11, 12
	4.6	0	-
	4.7	4	4, 11, 14. 15
	4.8	11	1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 13
	4.9	0	-
	4.10	0	-
	4.11	5	4, 8, 11, 13, 14
	4.12	0	-
	4.13	0	-
	4.14	0	-
	4.15	7	2, 4, 5, 11, 12, 13, 14
	4.16	7	2, 4, 5, 11, 12, 13, 14
	4.17	7	2, 4, 5, 12, 13, 14, 15
	4.18	7	2, 4, 5, 12, 13, 14, 15
	4.19	7	2, 4, 5, 12, 13, 14, 15
	4.20	9	2, 4, 5, 8, 9, 12, 13, 14, 15

Если в качестве критерия дублирования выбрать пять и более совпадений тематического подобия, то получим перечень из 21 рассмотренных тем, представленных на рисунке 4. По этим темам, используя данные, представленные на рисунке 5, достаточно просто определяется перечень дисциплин, содержащих тематическое подобие.

Выявленные по тематическому подобию дисциплины могут быть представлены руководству кафедры для последующего анализа их тематического содержания и уточнения изучаемых вопро-

сов с целью исключения возможности дублирований дидактических единиц.

При этом указанная информация может быть использована для поддержки принятия организационных и управленческих решений, направленных на оптимизацию использования учебного времени.

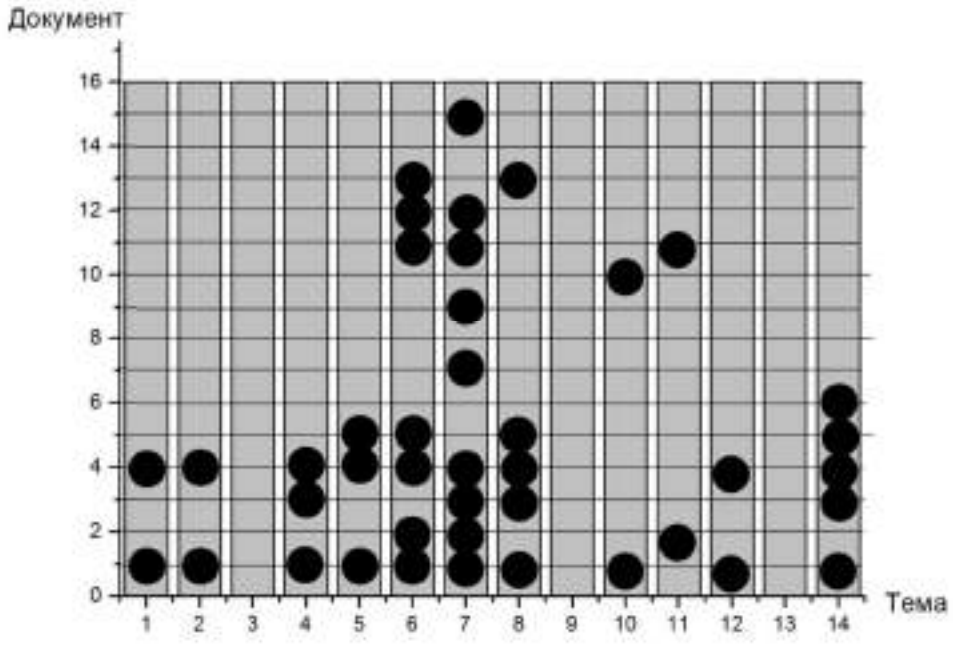


Рис. 5. Отображение возможных дублирований отдельных тем в содержании изучаемых дисциплин

Оценка временных затрат, необходимых для проведения анализа возможных тематических дублирований в 16 РПД ручным способом и автоматизированно с применением инфологической обработки, показывает, что во втором случае оперативность достижения результата может быть повышена до 5 раз.

Таким образом, представленный способ инфологической обработки РПД для оценки подобия тематического содержания лекционных курсов позволяет автоматизировать процесс выявления тематических дублирований в различных дисциплинах отдельного направления подготовки студентов.

Экспериментальные исследования по оценке тематического сходства 16 РПД показали возможность применения разработанного способа в системе поддержки принятия управленческих решений выпускающей кафедры, направленных на оптимизацию использования учебного времени.

1. Компьютерная лингвистика и перспективные информационные технологии. Теория и практика построения систем автоматической обработки текстовой информации / Г.Г. Белоногов [и др.]. – М.: Русский мир, 2004. – 264 с.

2. Васильев В.Г., Кривенко М.П. Методы автоматизированной обработки текстов. – М.: ИПИ РАН, 2008. – 301с.

УДК 004.932.75’1

А.М. Потапенко, М.В. Алёшечкин, А.С. Якушев

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВАРИАНТ СТРУКТУРЫ НЕЙРОННОЙ СЕТИ ДЛЯ РАСПОЗНАВАНИЯ ПРОСТЕЙШИХ ЗАПРОСОВ (СЛОВ) ПРИ ИНФОРМАЦИОННОМ ПОИСКЕ

Рассмотрена базовая структура нейронной сети для распознавания слов, а также принцип её обучения.

Одной из важнейших, но нерешенных с должным качеством проблем является автоматизация информационного поиска в сети Интернет. Из всей совокупности задач, посвященных этой проблеме, немаловажное место должно быть отведено задаче подготовки информационных запросов, представленных в «нестандартизованных» форматах (рукописный, графический и т.п.), к заданным стандартам кодирования. В данной работе рассматриваются вопросы решения задачи распознавания символов рукописного текста на основе нейросетевых устройств и выбора их основных параметров.

Основные требования к алгоритму распознавания символов в рукописном тексте, а следовательно, к составу и структуре нейросети, его реализующей, сводятся к следующему.

На вход системы распознавания символов поступает последовательность кодовых слов, отображающих элементы символов анализируемого текста и их положение в нем. Результатом работы системы распознавания является исходный текст, представленный в виде структурированной последовательности символов в заданном формате. Количество распознаваемых символов в рамках одного языка ограничено и может составлять несколько сотен единиц. В то же время количество вариантов начертания искомых

символов в рукописных текстах многократно превосходит размерность любого исходного алфавита, что делает малоэффективными системы распознавания на основе эталонных описаний распознаваемых образов. Требуется самообучающаяся система, накапливающая «опыт» правильных решений.

Последовательность кодовых слов разбивается на группы (облака, семейства), объединяемые принадлежностью к тому или иному символу текста. Граница группы в контексте задачи распознавания символов могут иметь, например, явные знаки пунктуации и неявные (например, пробелы) признаки. Однако в исходной последовательности кодовых слов эти признаки в явном виде отсутствуют и могут появиться лишь как результат работы системы распознавания. Отсюда следует, что результаты работы системы с точки зрения подзадачи выделения совокупности кодовых слов, образующих символ текста, должны использоваться для их корректировки, то есть система должна иметь обратные связи и работать итерационно.

Очевидно, что в значительном числе случаев существенно улучшить точность распознавания символов позволяет использование априорной информации по правилам словообразования и синтаксиса, используемых в тексте естественных языков. Отсюда следует, что система распознавания символов должна включать в себя, как минимум, процедуры формирования элементов слов и слов в целом. Количество таких процедур определяется особенностями языка. В частности, для русского к ним можно отнести: процедуры формирования приставок, корней, суффиксов, окончаний, а также взаимодействия слов с местоимениями и предлогами.

Возможных вариантов решения поставленной задачи на основе нейросетевых подходов достаточно много. Среди основных – нейронные сети Хопфилда и Хэмминга, сети Кохонена, сети Джордана, многослойные персептроны и другие.

При выборе основы для построения базовой структуры нейронной сети для распознавания слов более других соответствуют предъявленным требованиям 2 варианта: сеть Хопфилда и сеть Хэмминга. Вместе с тем сеть Хемминга имеет ряд важных преимуществ. Во-первых, данная сеть рассчитана на неуправляемое обучение, то есть сеть может самоорганизовываться. Сеть Хэммин-

га, в отличие от других, обеспечивает возможность построения ассоциативной памяти. Кроме того, её реализация требует меньших, по сравнению с сетью Хопфилда, затрат вычислительных ресурсов, более проста в программной реализации и имеет максимально упрощенный алгоритм обучения. Структура сети Хэмминга позволяет проектировать достаточно сложные нейронные сети, число и сложность распознаваемых образов которых ограничивается только объемом оперативной памяти.

Структурная схема сети Хэмминга приведена на рисунке 1.

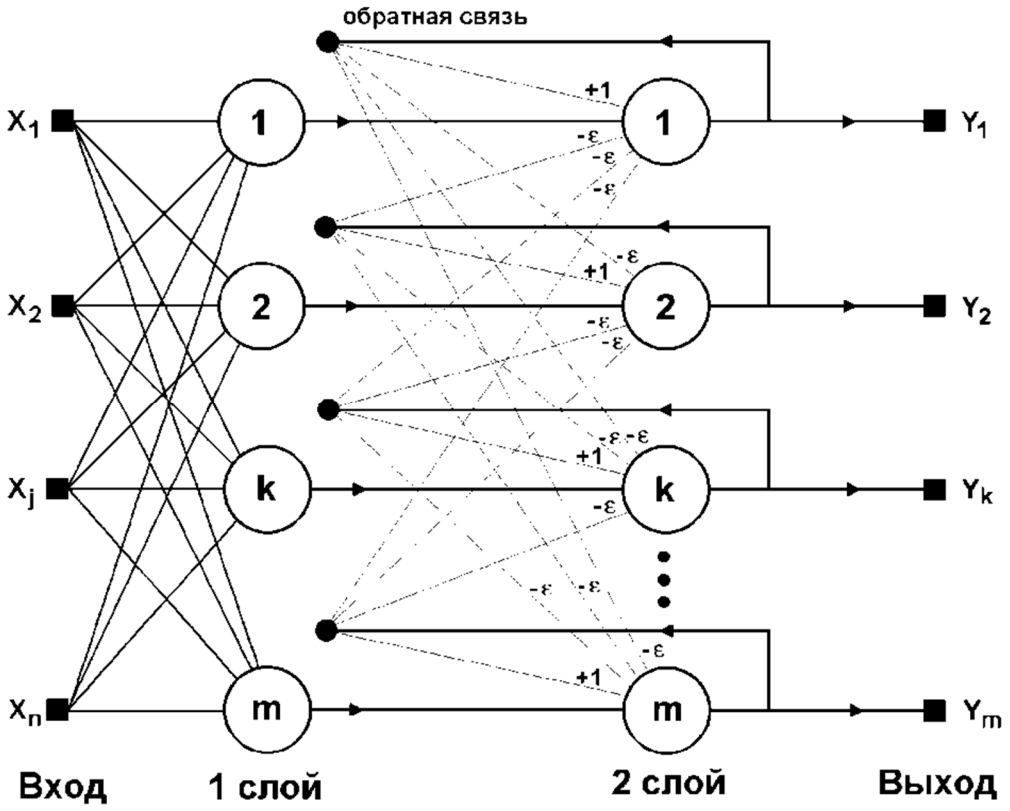


Рис. 1. Структурная схема сети Хэмминга

Структурная схема сети Хэмминга состоит из двух слоёв нейронов. Первый и второй слои имеют по m нейронов, где m – число образцов. Нейроны первого слоя имеют по n синапсов, соединенных со входами сети (образующими фиктивный нулевой слой). Нейроны второго слоя связаны между собой отрицательными обратными синаптическими связями. Единственный синапс с положительной обратной связью для каждого нейрона соединен с его же аксоном (выходом).

Суть проблемы в распознавании слов заключается в распознавании и классификации входных данных для нейронной сети, в нашем случае букв, цифр, символов, самих слов и их элементов в виде изображений. Учитывая все требования, предлагается многослойная структура, основанная на сетях Хэмминга, состоящая из семи слоёв. Каждый слой предлагаемой сети является по отдельности сетью Хэмминга, состоящей из двух слоёв, выходы которых являются входами для последующего слоя. Все слои сети также объединены обратными связями для самообучения и уточнения принятых решений. Семь – минимальное количество слоёв, необходимое для распознавания символа, которое основано на итерационной обработке нескольких уровней данных: буквы, символы, цифры, все части слов, сами слова, а также отдельный слой нейронов для определения границ символов в изображении.

Назначение слоев сети применительно к русскому языку состоит в следующем:

1. Входной слой обеспечивает анализ поступивших данных и определение границ символа в изображении.

2. Второй слой предназначен для распознавания букв, цифр и других символов.

3. Четыре последующих слоя, обеспечивают обработку частей слов:

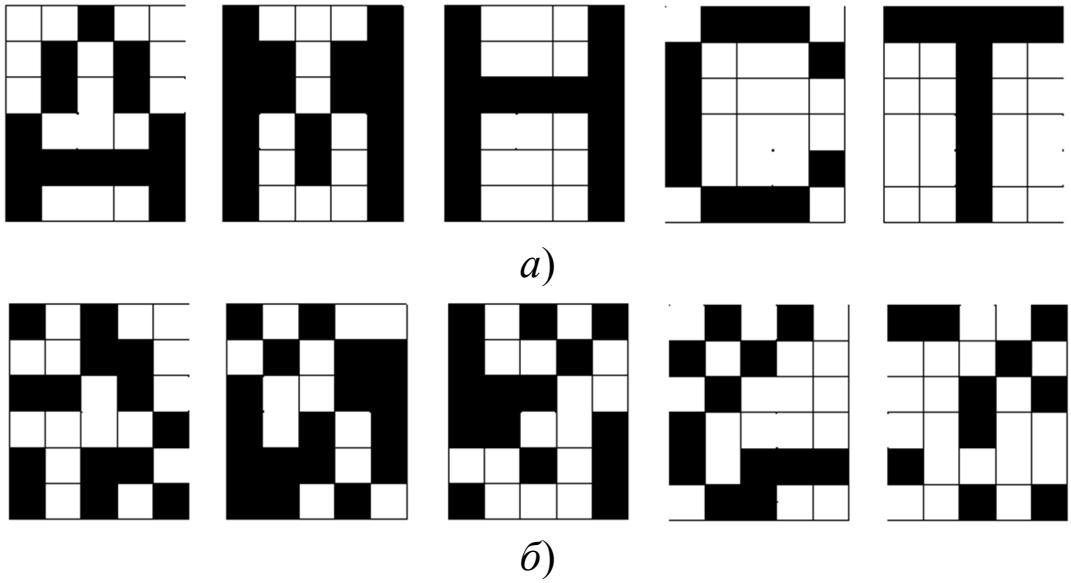
   3.1) приставок;
   3.2) корней слов;
   3.3) суффиксов;
   3.4) окончаний.

4. Седьмой – последний выходной слой, который анализирует комбинации результатов и формирует слова.

Вывод о значении анализируемого символа на основе решений всех семи уровней сети осуществляется следующим образом. На входной слой подаётся образ той или иной буквы, цифры или символа, в нашем случае элементы изображения. Само изображение запоминается как расстановка пикселей, тёмных и светлых, на определенной площади. Происходит процесс определения границ строк, слов и, наконец, символов, например, путем анализа процентного соотношения светлых и тёмных пикселей на определенном отрезке. Если количество тёмных пикселей превышает некото-

рое значение, система принимает решение о том, что данное поле пикселей образует строку. Данные о границах слов и символов могут определяться аналогично, например, за счет анализа вертикальных «границ» из светлых пикселей внутри определенной ранее строки.

Далее производится распознавание самого символа, процедура которого иллюстрируется на рисунках 2, *а* и 2, *б* для идеальных и реальных условий соответственно.



а)

б)

Рис. 2. Пример распознавания букв

В общем виде в качестве форм входных данных могут применяться не только изображения, но и другие двоичные сигналы: звуковые оцифровки, прочие данные, описывающие некие объекты или характеристики процессов.

Затем результаты работы второго слоя в виде гипотез о значении символов последовательно обрабатываются последующими слоями сети. Целью этих этапов обработки является проверка правомерности выдвинутых гипотез, которая основана на допустимости комбинаций символов в словах и их элементах. Все слои сети должны быть между собой взаимосвязаны. Если один из слоёв не дал положительного результата, то это является основанием для опровержения прежних и выдвижения новых гипотез.

Обобщенный алгоритм функционирования данной структуры сети наглядно представлен на рисунке 3.

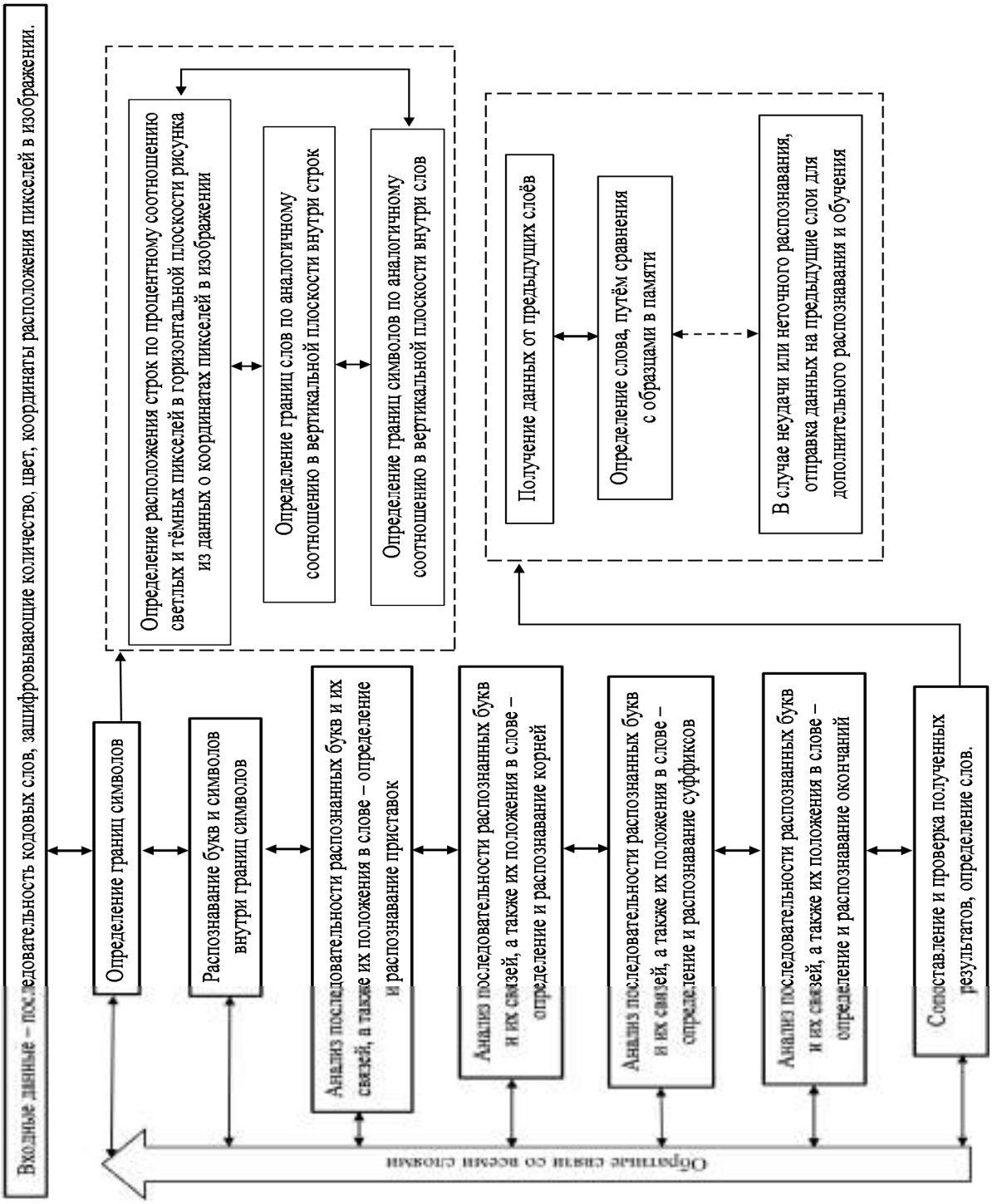


Рис. 3. Обобщенный алгоритм функционирования структуры сети

Что касается количества необходимых нейронов для каждого слоя, то оно определяется уже русским языком. Для входного слоя будет достаточно для начала примерно 100 нейронов. За счет такого количества определяется некое «плавающее окно» – поле, в котором идет процесс распознавания границ строк, слов и символов в

подаваемом на вход тексте. Для второго слоя необходимо около 255 выходных нейронов подсети Хэмминга. В это количество входят абсолютно все возможные символы, включая цифры, буквы и любой другой символ кодировки ASCII. Для третьего – приблизительно 23 нейрона, так как именно столько основных приставок в русском языке. Для суффиксов русского языка потребуется примерно 131 нейрон, для окончаний – примерно 25, а для корней и самих слов – около 30000, если брать весь словарный запас русского языка. Структура сети позволяет добавлять или удалять неиспользуемые нейроны, что дает возможность легко учитывать опыт решения практических задач и адаптировать сеть под реальные условия.

Предложенная структура является начальной и имеет возможность доработки и расширения функции распознавания запросов не только на русском, но и на других языках.

---

1. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика. – М.: Мир, 1992.

2. Боровиков В.П. Нейронные сети STATISTICANeuralNetworks: Методология и технологии современного анализа данных. – 2-е изд., перераб. и доп. – М.: Горячая линия – Телеком, 2008.

УДК 621.396

И.Г. Бабанин, К.М. Керимбаева

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВАРИАНТ ПОСТРОЕНИЯ НАУЧНО-ПРОИЗВОДСТВЕННОГО КОМПЛЕКСА ДЛЯ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ СОВРЕМЕННЫХ УСТРОЙСТВ ГЕНЕРИРОВАНИЯ И ФОРМИРОВАНИЯ РАДИОСИГНАЛОВ НА БАЗЕ ПЛИС В ЦИФРОВЫХ ВЫСОКОСКОРОСТНЫХ ПОДВИЖНЫХ СИСТЕМАХ СВЯЗИ

Показана необходимость построения научно-производственного комплекса для автоматизированного проектирования современных устройств генерирования и формирования сигналов на базе ПЛИС в цифровых высокоскоростных подвижных системах связи.

Информация играла и играет немалую роль в жизни человека. В связи с началом научно-технической революции первой полови-

ны XX века объемы информации стремительно возросли, что привело к информационному взрыву. Таким образом, увеличилась необходимость обмена различного рода информацией и, как следствие, способов обмена необходимой информацией. Актуальность и необходимость решения данной задачи является главным фактором, мотивирующим ученых на поиск путей её решения.

В таблице представлено развитие скоростей передачи данных для различных поколений подвижной системы связи.

Темпы развития скоростей передачи данных в подвижных системах телекоммуникаций

Поколения	Стандарты	Скорость передачи	Тип модуляции	Тип разделения канала
1G	D-AMPS	1,9 кбит/с	π/4-DQPSK	FDMA
2G	GSM	9,6-14,4 кбит/с	GMSK	TDMA, CDMA
2,5G	GPRS,EDGE(2,75G), 1XrTT	115 - 384 кбит/с	GMSK	CDMA
2,75G	WSDMA, CDMA2000,UMTS	2 Мбит/с	BPSK, QPSK	CDMA2000 1X
3G	HSDPA,HSUPA, HSPA,HSPA+	3-14 Мбит/с	QAM-16, -64	CDMA2000 1xEV-DO
4G	LTE-Advanced, WiMax Release 2 (IEEE802.16m), WirelessMAN-Advanced	100Мбит/с – 1Гбит/с	QAM-16, -64	OFDM

Стремительный рост подтверждает закон Мура: «За каждые 5 лет происходит увеличение объема информации втрое». Кроме того, в таблице отображена тенденция к применению линейных высокопозиционных видов модуляции.

Вышеприведенные данные свидетельствуют об актуальности построения научно-производственного комплекса для автоматизированного проектирования современных устройств генерирования и формирования радиосигналов на базе FPGA, CPLD в цифровых высокоскоростных подвижных системах связи.

Для осуществления данной задачи необходимо использование соответствующего оборудования. В данном случае приемлемо два варианта: персональный компьютер (при модуляции не выше QAM-1024) или же несколько компьютеров, объединенных в вычислительный кластер посредством сетевого оборудования. Обязательным является наличие устройства для программирования ПЛИС (для микросхем altera – USBBlaster; для микросхем Xilinx-PlatformCabelUSB). Кроме того, комплекс должен содержать программное обеспечение (ПО), необходимое для исправной работы системы. В перечень такого ПО входят «общие» программы:

1) Matlab/Simulink(не ниже R2013b);
2) GNURadio (не ниже 3.7.0).

«Специализированные» программы от компании Xilinx:

1) Xilinx ISE;
2) Plan Ahead;
3) XPower Analiser;
4) Schematic Viewer;
5) Liming Analiser;
6) Core Generator;
7) iMPACT.

«Специализированные» программы от компании Altera:

1) Quartus II;
2) Model Sim;
3) Nios II.

Для обеспечения взаимодействия «общих» программ со «специализированными» необходима их установка на компьютер (вычислительный кластер) по схеме, представленной на рисунке 1.

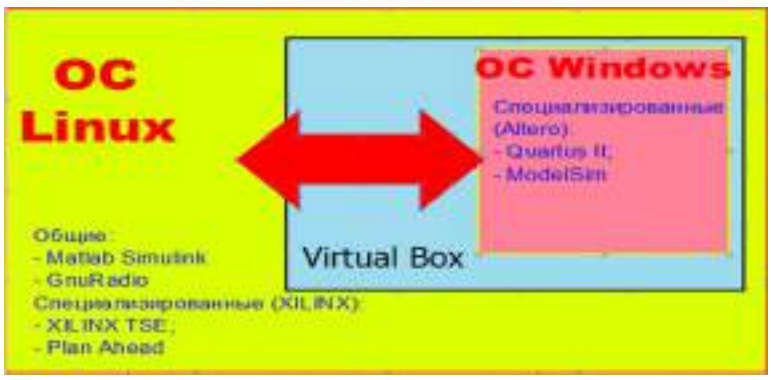


Рис. 1. Структурно-функциональная схема взаимодействия программного обеспечения автоматизированного комплекса

Причина использования такого структурно-функционального взаимодействия заключается в том, что программное обеспечение GNURadio может работать только с операционной системой (ОС) Linux, а «специализированные» программы компании Alterac ОС Windows. Исходя из этого целесообразно в качестве основной системы использовать ОС Linux с установленной на нее «специализованных» компанией Xilinx «общих» программ, а в качестве гостевой ОС Windows – со «специализированными» программами Altera.

Вышепредставленное оборудование и ПО не позволяет в полной мере создать комплекс автоматизированного проектирования передатчиков высокоскоростных цифровых линий связи. Для полного функционирования комплекса необходим разработанный файл имитационной универсальной модели формирователя радиосигналов систем связи с повышенной кратностью модуляции. Состав модели представлен на структурно-функциональной схеме (рис. 2, 3).

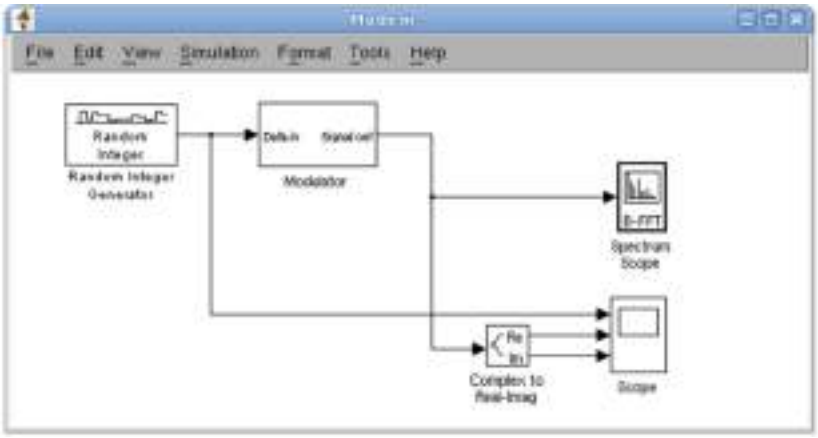


Рис. 2. Структурно-функциональная схема устройства формирования радиосигналов в системе динамического моделирования Matlab/Simulink

Из рисунков 2 и 3 видно, что данная модель включает в свой состав перекодировочную таблицу (LUT), формирующий фильтр с характеристикой приподнятого косинуса (Raised Cosine Receive Filter), усилитель для обеспечения средней потребляемой мощности (Gain), индикаторы отображения выходного амплитудного спектра, констеляционной, глазковой, временных диаграмм на выходе «LUT»и «Gain» [1].

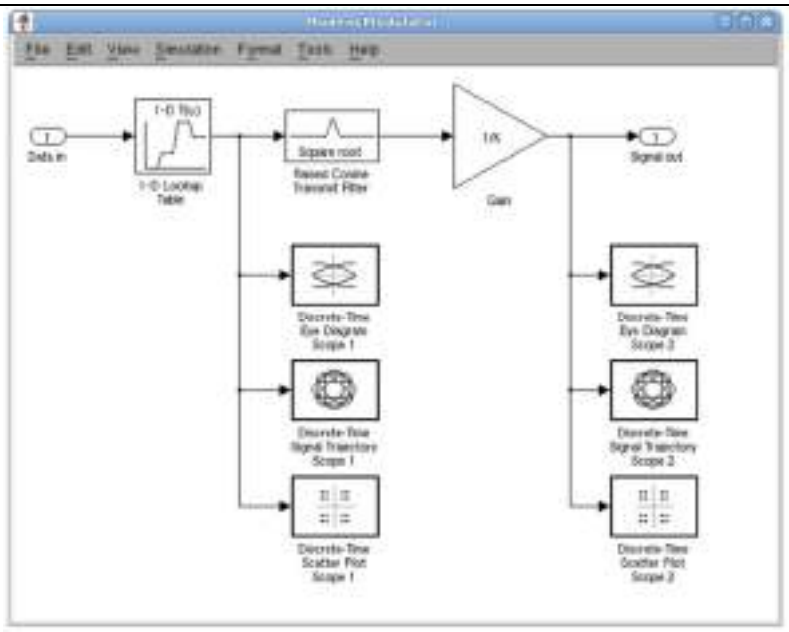


Рис. 3. Структурно-функциональная схема универсального модулятора

Так, формирующий фильтр необходим в данной системе для ограничения спектра сигнала передатчика и повышения его спектральной эффективности. Необходимость использования данного устройства возникает в условиях постоянно возрастающих требований к цифровым системам связи по скорости передачи данных. Пример задания параметров формирующего фильтра: тип фильтра (Filter Type) – корень из приподнятого косинуса (Square Root); групповая задержка, определяющая длину импульсной характеристики (ИХ) фильтра, (Group Delay) – 5 символов; коэффициент скругления (Rolloff Factor) –0,8; коэффициент повышения частоты дискретизации (Upsamplingfactor) – 8; характер обработки сигнала (Input Processing) – samplebased. С выхода формирующего фильтра комплексный сигнал поступает на усилитель с коэффициентом передачи 1/К, где выполняется его нормировка. Индикаторы отображения выходного амплитудного спектра, констеляционной, глазковой, временных диаграмм необходимы для наглядного представления поведения сигнала в создаваемой модели. Анализатор спектра, как и другие составляющие модели, необходимо задать также соответствующими параметрами: необходимо выставить размер окна БПФ 1024 и включить буферизацию входного сигнала с размером буфера 1024 отсчета (рис. 4, 5).

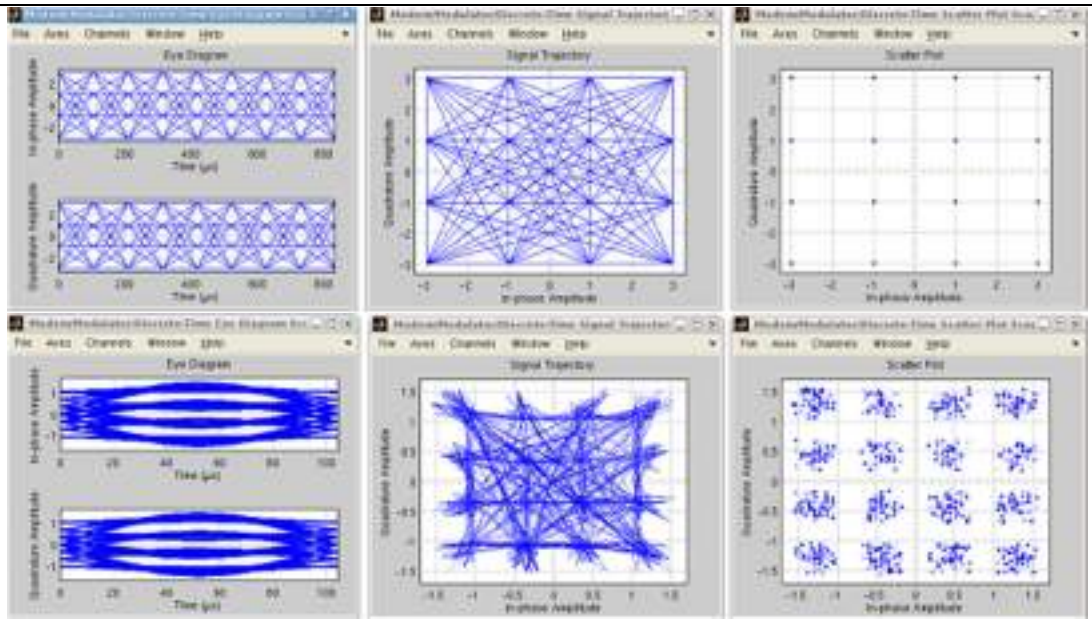


Рис. 4. Блоки отображения информации о сигнале

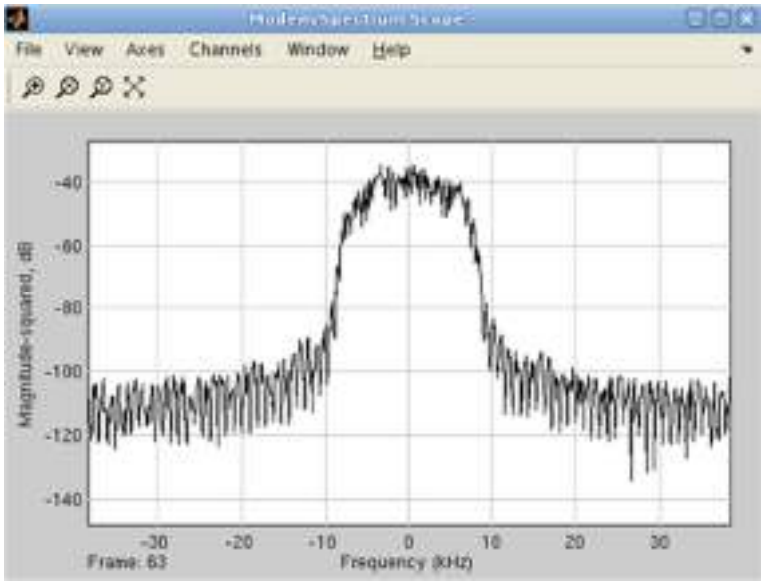


Рис. 5. Спектр формируемого сигнала

Для проведения операций по тестовому испытанию, настройке, отладке необходим научно-производственный комплекс для автоматизированного проектирования устройств приёма и обработки радиосигналов высокоскоростных линий связи. Совместное использование данных комплексов позволит оценивать качество передаваемых данных по радиотракту, исследовать влияние потерь шумового, нешумового характера в структурно-функциональных узлах цифровых телекоммуникационных систем.

Таким образом, построение научно-производственного комплекса для автоматизированного проектирования современных устройств генерирования и формирования сигналов на базе ПЛИС в цифровых высокоскоростных подвижных системах связи является важной и необходимой задачей, поскольку спрос на данное устройство стремительно набирает обороты. Происходит это в связи с увеличением требований к системам передачи информации, так как ее объемы значительно растут – возникает необходимость в более высокой скорости и качестве передачи. Более того, уникальные возможности, большой объем логических, специализированных и трассировочных ресурсов ПЛИС, выпускаемых фирмой Xilinx, Altera, значительно облегчают задачу и позволяют разрабатывать высокопроизводительные цифровые устройства различного уровня сложности.

Список литературы

1. Системы связи. Подвижные системы связи: учебно-методическое пособие для лабораторных работ [Электронный ресурс] / сост. Н.М. Боев. – Электрон. дан. – Красноярск: Сиб. федер. ун-т, 2013.

2. Официальный сайт компании Xilinx [Электронный ресурс]. – URL: http://www.xilinx.com.

3. Официальный сайт компании Altera [Электронный ресурс]. – URL: http://www.altera.com.

УДК 004.418

А.Л. Марухленко, А.А. Кваскov, И.А. Петровский

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РАСПРЕДЕЛЕННАЯ СИСТЕМА КОНТРОЛЯ ПРОМЕЖУТОЧНЫХ ЗНАНИЙ СТУДЕНТОВ ВУЗА

В масштабах кафедры проведен анализ динамики выполнения студентами практических работ, обоснована актуальность и предложен вариант системы, способствующей более равномерному режиму выполнения индивидуальных заданий.

Целенаправленное взаимодействие преподавателей и обучающихся, в ходе которого решаются задачи образования, развития и воспитания, является актуальным и предполагает организацию

обучения во взаимосвязи всех компонентов. Особое внимание следует уделять развитию практических навыков, которые формируются по ходу выполнения расчётных и практических работ. Практические работы включают комплекс заданий, в которых необходим регулярный контроль корректности полученных результатов на каждом этапе выполнения. Для повышения эффективности таких работ необходимо предоставить обучающимся возможность верификации результатов.

Данную проблему целесообразно решать с использованием средств, обеспечивающих студенту возможность в произвольный момент времени провести самоконтроль. Учитывая факторы необходимости ограничения доступа и заданной периодичности приема данных, работа системы должна удовлетворять следующим требованиям:

– доступ всех участников к данной системы без установки дополнительного программного обеспечения;

– обязательная регистрация с подтверждением по email (минимизация спама, обратная связь);

– ответ на задание можно вводить только раз в 24 часа (с целью исключения перебора ответов).

Анализ учебного процесса в ЮЗГУ в 2013 по дисциплине «Основы информационной безопасности» позволил сформировать зависимость успешного выполнения практических работ по времени в течение семестра (рис. 1).

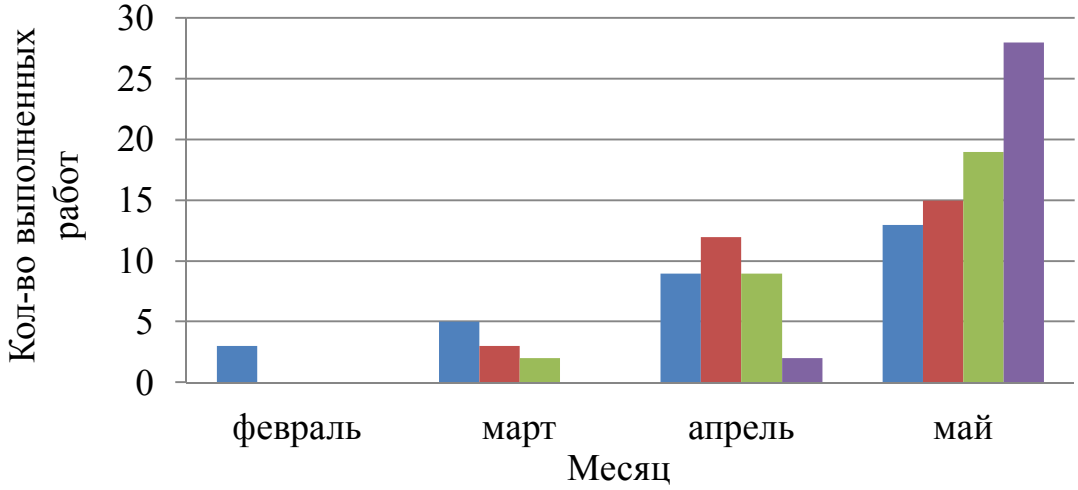


Рис. 1. Диаграмма защиты практических работ

Обзор современных средств по созданию автоматизированных систем учета и обработки статистических данных выявил целесообразность использования языка программирования PHP и системы управления базами данных MySQL. Так как подобная система будет использоваться как студентом, так и преподавателем, необходимо два варианта организации ресурса (модель взаимодействия элементов системы для обучаемых показана на рисунке 2, для преподавателей – на рисунке 3).

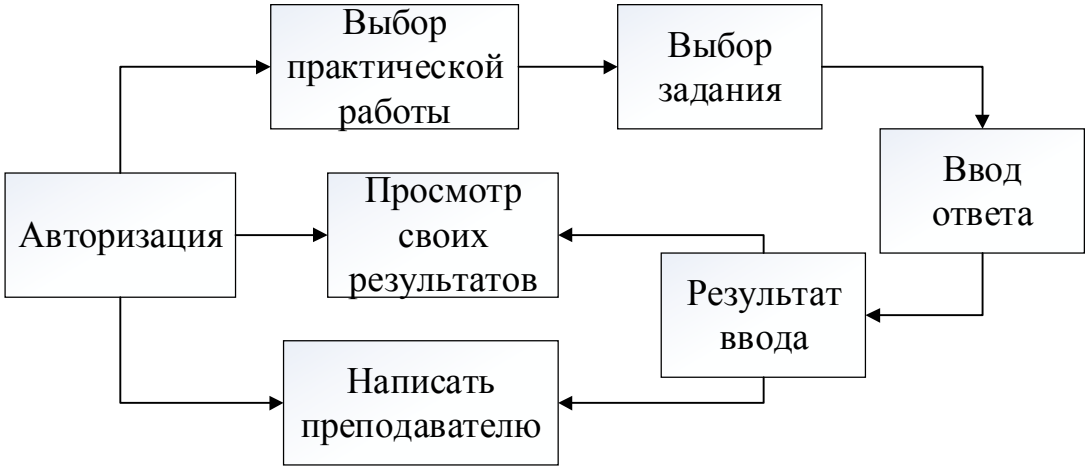


Рис. 2. Схема взаимодействия объектов системы (студент)

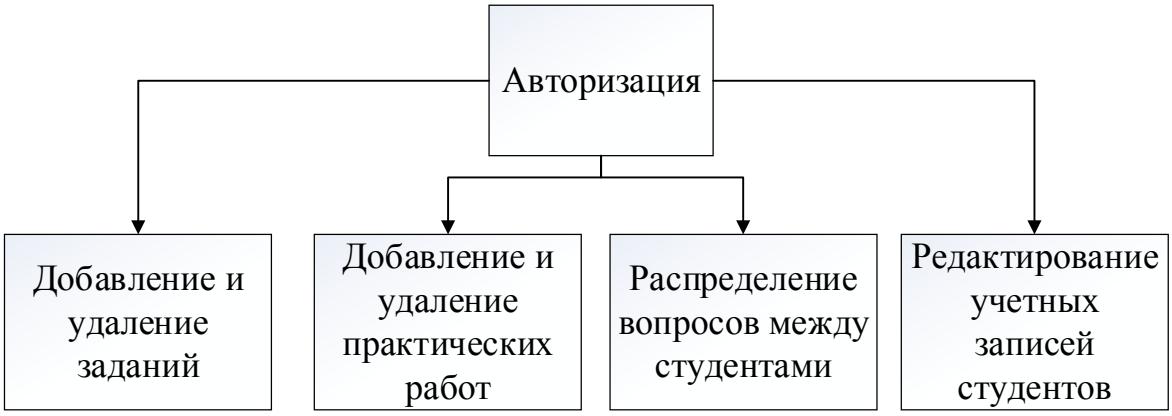


Рис. 3. Схема взаимодействия объектов системы (преподаватель)

На основе данного исследования был реализован сайт «Labtab», который был размещен на хостинге. Студенты в течение осеннего семестра в 2013 году проверяли результаты практических работ по дисциплине «Основы информационной безопасности». Динамика защиты работ с использования сайта «Labtab»показана на рисунке 4.

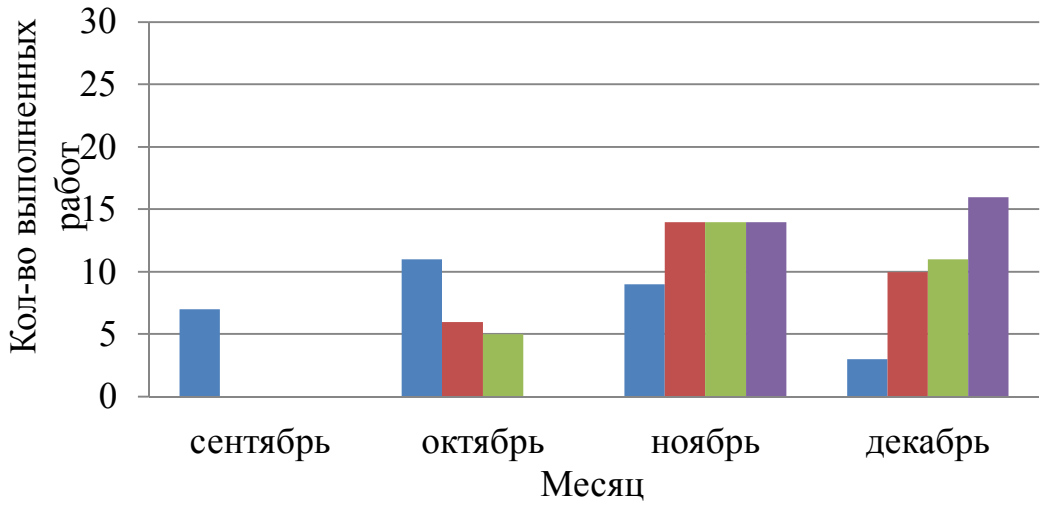


Рис. 4. Диаграмма защиты практических работ после внедрения системы

После внедрения системы получилось более равномерное распределение результатов успешного выполнения индивидуальных заданий, снизилась пиковая нагрузка в последние месяцы семестра.

Использование разработанного сервиса предоставит обучающимся возможность верификации, а преподаватели смогут получать статистику в масштабе реального времени.

---

1. Богомолов В.А. Обзор бесплатных систем управления обучением [Электронный ресурс]. – URL: http://ifets.ieee.org/russian/depository/v10_i3.

2. Евтушенко К.Н., Корнаков Д.С. Виртуальные лабораторные работы в образовани // Проблемы и перспективы развития образования в России: сб. матер. X Междунар. конф. / под общ. ред. С.С. Чернова. – Новосибирск: Изд-во НГТУ, 2011. – 403 с.

УДК 004.771

А.Л. Марухленко, А.А. Кваскова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВАРИАНТ ОРГАНИЗАЦИИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ ПРОВЕДЕНИЯ КОНФЕРЕНЦИЙ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СРЕДСТВ

Рассматривается способ организации видеоконференций в компании, работающей с удаленными сотрудниками, произведены расчеты канала связи.

Согласно исследованию маркетингового агентства Discovery Research Group рынок консалтинговых услуг в 2013 году увеличился на 28% и достиг 3 млрд $. Российский рынок консультационных услуг развивается за счет роста сектора консалтинга в сфере информационных технологий, на который приходится более половины объема российского рынка консультационных услуг [1]. В данной сфере и специализируется компания «Телекомновации», которая занимается оптимизацией телекоммуникационных служб Интернет-провайдеров.

Характеристика решаемых задач включает в себя: встречи с клиентами, консультирование клиентов, удаленные проекты, совещания между собственными сотрудниками. Статистика показывает, что 95% рабочего времени сотрудники проводят вне собственного офиса, 30% сотрудников никогда не были в главном офисе. Таким образом, целесообразно использование сервиса, который позволил бы проводить групповые конференции, работать с документами в реальном времени, демонстрировать рабочий стол, что позволит сократить транспортные расходы, сэкономить рабочее время сотрудников, повысить эффективность совещаний. Для обеспечения вышесказанного необходимо внедрить систему, которая бы использовалась для связи удаленных сотрудников. Анализ особенностей деятельности компании «Телекомновации» позволил сформулировать ряд требований к подобной системе:

– одновременная работа до 20 участников;

– возможность адаптации внутреннего и внешнего интерфейса (гибкость администрирования);

– использование собственного сервера (вся информация находится в масштабах организации и может носить конфиденциальный характер);

– возможность показа рабочего стола в реальном времени (конференция, обучение персонала);

– обмен файлами между пользователями;

– совместная работа над документами.

На сегодняшний день для реализации данных требований можно выделить два типа сервисов по организации видеоконференций: 1) сервер, который устанавливается на отдельную платформу внутри организации, и мы имеем внутрикорпоративный сервер видеоконференций; и 2) серверы, которые находятся в Интернете. Анализ подобных систем показан в таблице.

Сравнение решений по поведению видеоконференций

Название	Цена, тыс.руб/год	Выделенный сервер	Использование документов	Демонстрация рабочего стола	Обмен файлами	Установка клиентского ПО	Кол-во участников
webinar.ru	35,9	-	+	+	-	-	25
Skype	4,8	-	-	+	+	+	10
WebEXcisco	40	-	+	+	+	+	100
Big blue button	-	+	+	+	+	-	-
Trueconf	84	-	+	+	+	+	120
Acrobat ConnectPro	155,7	-	+	+	-	-	100
Apache Open Meetings	-	+	+	+	+	-	-

Учитывая, что необходимым требованием является наличие выделенного сервера, предпочтительнее внедрение Big blue button, так как при схожем функционале с Apache Open Meetings система обладает гибкостью настройки и масштабирования. Анализ трафика показал снижение нагрузки до 9 % на канал в момент пиковой нагрузки работы 5 в режиме видеоконференций [4].

К серверу предъявляются следующие требования: ОС UbuntuServer 10.04 64-bit, 4 ГБ ОЗУ, Dual-core 2.6 ГГЦ, открытые порты 80, 1935, 9121; порт 80 не должен использоваться другим приложением.

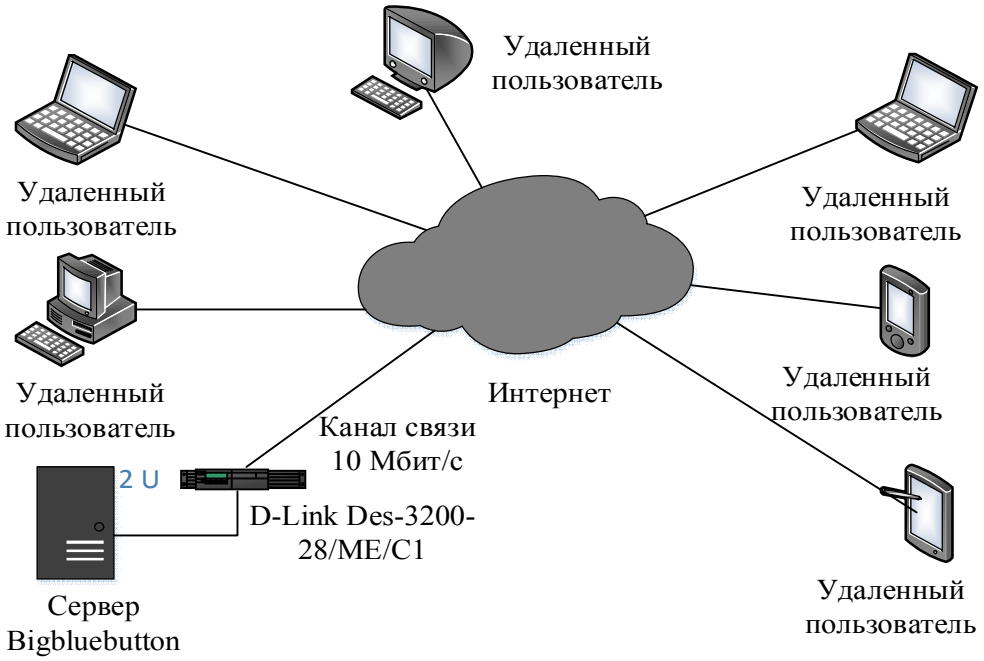


Рис. Схема взаимодействия пользователей

На рисунке показана схема взаимодействия пользователей, 1 помечен анализируемый канал связи.

Требования к каналу связи:

- входящий канал для сервера рассчитывается по формуле

$$B = W \cdot Y; \quad (1)$$

- исходящий канал для сервера рассчитывается по формуле

$$C = W \cdot (U - 1) \cdot Y; \quad (2)$$

- пропускная способность сервера рассчитывается по формуле:

$$A = B + C, \quad (3)$$

где Y = 400 Кбит/с – скорость видеопотока;

W = количество веб-камер;

U = количество пользователей.

Рассчитаем какое количество участников могут принимать участие. Для это воспользуемся формулами 1, 2 и 3. Количество веб-камер возьмем равным количеству пользователей.

В результате расчетов при ширине канала 10 Мбит/с, максимальное количество участников равняется 5.

Применение полученных результатов позволит повысить эффективность работы компании благодаря снижению временных и финансовых затрат на подготовку и проведение совещаний, конференций, рабочих встреч.

Список литературы

1. DiscoveryReseachGroup. Анализ рынка консалтинговых услуг в России в 2013 г. – М., 2014. – 74 с.

2. Чернышев В.О. К вопросу выбора инструментальной среды современных информационных технологий. – Минск, 1998. – Вып. 2. – Т. 1. – 35 с.

3. Газизов Т. Т., Корнеев Ю. О., Афанасьев Д. И. Технологическая площадка для организации учебно-методических мероприятий в режиме веб-конференции // Новые информационные технологии в образовании: матер. Всерос. заоч. электрон.науч.-практ. конф., 15–16 ноября 2012 г. / Сев.-Вост. гос. ун-т. – 2012. – С. 12.

УДК 681.3

С.С. Шевелев, К.А. Акимов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

УСТРОЙСТВО ПАРАЛЛЕЛЬНОГО ПОИСКА И ЗАМЕНЫ ВХОЖДЕНИЙ В ОБРАБАТЫВАЕМЫХ СЛОВАХ

Рассмотрено устройство параллельного поиска и замены вхождений в обрабатываемых словах, которое может быть применено в шифрации и дешифрации текстовой информации.

Алгоритмы шифрования текстовой информации становятся востребованными, они получили широкое распространение в передаче информации в социальных сетях. Информация нуждается в шифровании для передачи ее по незащищенным каналам связи, а также для хранения ее в незащищенных источниках. Операция шифрования применяется для соблюдения конфиденциальности передаваемой информации. Любой алгоритм шифрования использует ключ, который создает конкретное преобразование из всех возможных для данного алгоритма.

Шифрование методом замены основано на алгебраической операции, называемой подстановкой. Методы шифрования заменой основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом. Получатель сообщения расшифровывает его путем обратной замены. В криптографии различают четыре разновидности шифров замены: простая замена, сложная замена, блочная замена, многоалфавитная замена. При аппаратной реализации все процедуры шифрования и расшифрования выполняются специализированными устройствами. При этом непременным компонентом всех аппаратно-реализуемых методов является гаммирование. Этот метод сочетает в себе высокую криптостойкость и простоту реализации.

Предложено специализированное устройство и алгоритм его работы. Это устройство выполняет операции поиска вхождений и подстановку символов в словах текста. В обрабатываемом слове процессы поиска вхождений можно выполнить как в параллельном, так и в последовательном режимах символьной обработки.

Новые слова можно формировать с помощью операций поиска и замены вхождений, а также выполнений операций левой и правой конкатенаций. Необходимо достигнуть высокой скорости поиска и замены при выполнении операций поиска вхождений в обрабатываемом слове. Поиск вхождений в обрабатываемом слове может осуществляться в двух режимах работы устройства: определение вхождений, имеющих общие части, и определение вхождения без общих частей.

В устройстве применяются оперативные запоминающие устройства, в которых хранится информация. Обрабатываемое слово, вхождение и замена переписываются из памяти в сдвигающие регистры. Процессы записи и считывание информации в регистры могут быть следующие: параллельный ввод – параллельный вывод используется в регистре для хранения вхождений; последовательный ввод – последовательный вывод используется в регистре для хранения замены; последовательный ввод – параллельно-последовательный вывод используется для хранения в регистре обрабатываемого слова.

При осуществлении поисковых функций вхождения могут быть представлены различными комбинациями букв в обрабатываемом слове: нет повтора одинаковых букв (итерации) в обрабатываемом слове; повтор одинаковых букв есть в середине обрабатываемого слова; итерация существует в конце слова; итерация в обрабатываемом слове существует в начале слова; итерация в обрабатываемом слове присутствует и в начале слова, и в конце; обрабатываемое слово состоит полностью из итераций. В зависимости от вида итераций применяются различные алгоритмы, осуществляющие поисковые операции вхождений в обрабатываемых словах.

В предлагаемом устройстве поиск вхождения в обрабатываемом слове выполняется в параллельном режиме. Все символы вхождения параллельно поступают на первые входы компаратора. На вторые входы узла сравнения также параллельно поступают символы обрабатываемого слова. В устройстве применены три регистра – регистр вхождения, регистр обрабатываемого слова и регистр замены. Длина регистров, в которых хранятся вхождение и обрабатываемое слово, а также количество компараторов, в которых происходит сравнение символов, одинаковая. Если произошло

положительное сравнение, то на выходе компаратора формируется единичное значение. В этом случае в обрабатываемом слове найдено вхождение. В случае работы устройства в режиме поиска определяется адрес вхождения. Если устройство работает в режиме поиска и замены, то в регистр замены записывается цепочка символов – замена. Обрабатываемое слово не изменяется в процессе замены. Если произошло отрицательное сравнение, то необходимо сдвинуть обрабатываемое слово на один разряд влево и сравнить следующую серию символов, равную по количеству символам вхождения. Процесс сдвига обрабатываемого слова в регистре выполняется до определения признака конца обрабатываемого слова. Символ в результате левого сдвига записывается в регистр замены. В регистр замены записываются символы обрабатываемого слова в результате операции левого сдвига регистра или буквы замены в режиме работы устройства поиска и замены. В устройстве осуществляются операции левой и правой конкатенаций. Структурная схема устройства параллельного поиска и замены вхождений в обрабатываемых словах изображена на рисунке.

Блок памяти вхождений (БПВХ) служит для записи, хранения и выдачи вхождений – цепочки символов, которые необходимо обнаружить в обрабатываемом слове. Блок памяти обрабатываемых слов (БПОС) служит для записи, хранения и выдачи обрабатываемых слов, с которыми необходимо проводить поисковые операции. Блок анализа поиска (БАП) служит для анализа поисковой операции, определения способа поиска вхождений в обрабатываемом слове, а также определения адреса вхождения. Блок памяти замены (БПЗМ) служит для записи, хранения и выдачи замены в регистры блока регистров результата замены. Блок замены (БЗАМ) служит для выполнения операций: записи символа обрабатываемого слова в случае отрицательного сравнения, записи замены в регистры блока регистров результата замены, если произошло положительное сравнение в блоке компаратора. Блок хранения результатов (БХР) служит для записи и хранения в нем адресов вхождений в обрабатываемых словах и результатов выполнения операций замены. Блок управления (БУ) служит для генерации управляющих сигналов устройства.

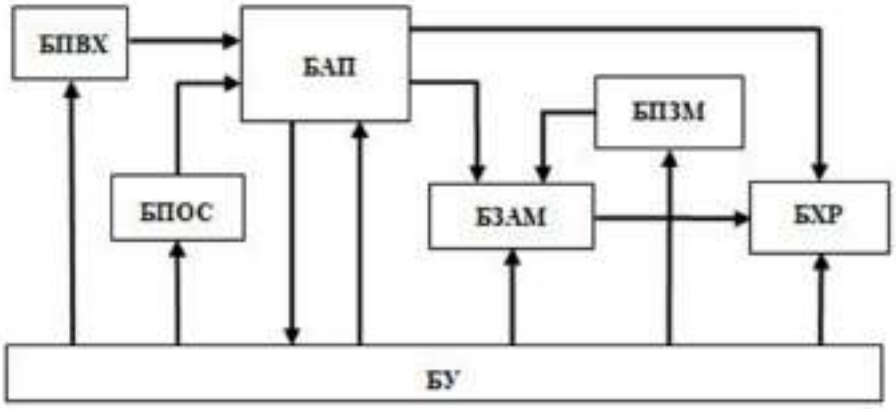


Рис. Устройство параллельного поиска и замены вхождений в обрабатываемых словах

В операциях шифрования и дешифрования информации роль специализированных устройств трудно переоценить. Во-первых, аппаратная реализация обладает лучшими скоростными характеристиками, использование специальных чипов приводит к тому, что они позволяют оптимизировать многие математические операции. Во-вторых, аппаратные средства защиты информации обладают несравнимо большей защищенностью как от побочных электромагнитных излучений, так и от непосредственного физического воздействия на устройство. В-третьих, аппаратные средства более удобны в эксплуатации, так как позволяют осуществлять операции кодирования и декодирования для пользователя в прозрачном режиме. В-четвертых, аппаратные средства используются для защиты телефонных переговоров, для отправки факсимильных сообщений и других видов передачи информации, где невозможно использовать программные средства.

В связи с тем что шифрование и другие информационные технологии проникают в наш быт, растет число компьютерных преступлений. Зашифрованная информация, так или иначе, представляет собой объект защиты. Различия в правилах и ограничениях по шифрованию компьютерной информации могут создать определенные трудности в плане обеспечения конфиденциальности общения. В связи с этим в любом государстве поведение в отношении передачи и шифрования информации регулируется различными правовыми нормами.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / под ред. А. Б. Васильева. – М.: Триумф, 2002. – 816 с.

2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

3. Пат. 2296366 Рос. Федерация, G06F17/30, G06F17/21. Устройство параллельного поиска и замены вхождений в обрабатываемых словах / Шевелев С.С. – № 2005125327/09; заявл. 09.08.2005; опубл. 27.03.2007, Бюл. №9. – 33 с.

УДК 681.3

С.С. Шевелев, Е.Ю. Дорошенко

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ТРОИЧНЫЙ СУММАТОР-ВЫЧИТАТЕЛЬ

Цифровое устройство сумматор-вычитатель в троичной системе счисления выполняет арифметическую операцию суммирования двоичных разрядов по правилам сложения чисел в троичной системе счисления.

Троичная система счисления является наиболее экономичной из всех целочисленных систем счисления с точки зрения плотности записи информации, т.е. при одинаковом количестве аппаратных затрат позволяет хранить больше информации. Троичная система бывает симметричной (цифры “0”, “1”, “-1”) и несимметричной (цифры “0”, “1”, “2”). Для кодирования троичных цифр в двухуровневых схемах используется два двоичных разряда. Для кодирования троичной несимметричной системы используются следующие обозначения: “00” – для цифры “0”; “01” – для “1”, “10” – для “2”.Троичная позиционная несимметричная система счисления по затратам числа знаков наиболее экономична из позиционных несимметричных систем счисления.

Для выполнения операции суммирования в троичной симметричной системе счисления было разработано специализированное устройство. Структурная схема данного устройства изображена на рисунке.

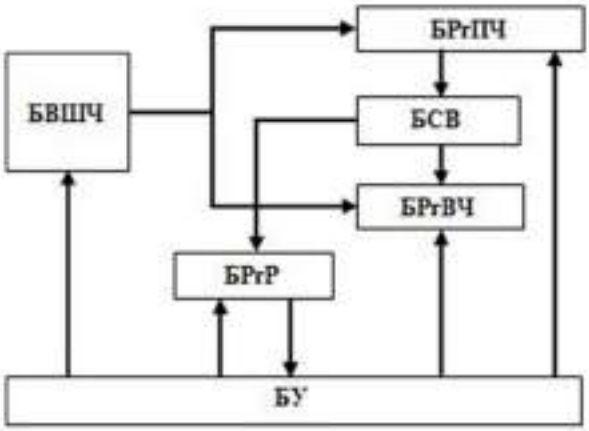


Рис. Структурная схема сумматора-вычитателя в троичной системе

Троичный сумматор-вычитатель в симметричной системе содержит блок ввода и шифрации чисел (БВШЧ), блок суммирования (БСВ), блок регистра первого числа (БРгПЧ), блок регистра второго числа (БРгВЧ), блок регистра результата (БРгР), блок управления (БУ).

БВШЧ используется для ввода значений операндов и кода операции.

В блоке вычисляется признак перевода числа ППЧ в обратный код:

$$ППЧ = ЗнРА \vee (КО \oplus ЗнРВ), \qquad (1)$$

где ЗнРА – знаковый разряд первого числа;

КО – код операции;

ЗнРВ – знаковый разряд второго числа.

Операция перевода числа в обратный код осуществляется путем перестановки бит в каждом троичном разряде и приводит к изменению знака числа на противоположный. Выдача значений за пределы блока ввода и шифрации чисел осуществляется по шине. Управление блоком происходит подачей сигналов и обнуления, и разрешения записи в элементы памяти блока.

Блок регистра первого числа БРгПЧ служит для хранения значений первого операнда. Блок регистра второго числа БРгВЧ служит для хранения значения второго операнда. Управление блоками осуществляется подачей сигналов по информационным шинам из блока управления.

Блок суммирования БСВ предназначен для выполнения операции сложения двоичных кодов по правилам троичной системы счисления. Результат сложения чисел по информационному сигналу поступает на вход блока регистра результата. Основным блоком устройства является трехразрядный сумматор. Функция трехразрядного сумматора заключается в получении суммы младшего и старшего разрядов входных чисел, определения кодовых ситуаций, при которых необходимо введение коррекции результата для получения окончательной суммы, формирование младшего и старшего разрядов переноса в старший разряд. Этот блок содержит три полных троичных одноразрядных сумматора. Одноразрядный сумматор вычисляет младший S_0 и старший S_1 разряды предварительной суммы двоичных сумматоров, а также перенос в следующий разряд P_1 с учетом переноса из предыдущего разряда P_0.

Вычисление разряда суммы происходит в несколько этапов.

Сначала вычисляются младший S_0 (2), затем межразрядный перенос P_0 и старший S_1 (3) разряды суммы без учета коррекции, т.е.

$$S_0 = A_0 \oplus B_0 \oplus P_{00} \; ; \tag{2}$$

$$P_0 = P_{00}A_0VA_0B_0VB_0P_{00} \; ; \tag{3}$$

$$S_1 = P_0 \oplus P_{01} \oplus A_1 \oplus B_1 \tag{4}$$

Первый дешифратор устройства определяет комбинацию суммы чисел S_0 и S_1, равную 11, при которой необходимо ввести коррекцию для получения окончательного результата.

На выходе этого дешифратора формируется управляющий сигнал $УС_1$ по формуле (4):

$$УС_1 = S_0 \& S_1 \; . \tag{5}$$

Второй дешифратор определяет комбинацию входных чисел, при которых сумма операндов S_0 и S_1 будет равна двоичному коду 00, в этом случае также необходимо ввести коррекцию.

На выходе этого дешифратора формируется управляющий сигнал $УС_2$ по формуле

$$\begin{gathered} УС_2 = A_1\bar{A}_0B_1\bar{B}_0\overline{P0}_1\overline{P0}_0V\bar{A}_1A_0B_1\bar{B}_0\overline{P0}_1P0_0V \\ VA_1\bar{A}_0\bar{B}_1B_0\overline{P0}_1P0_0V\;\bar{A}_1\bar{A}_0B_1\bar{B}_0P0_1\overline{P0}_0\;V \\ V\bar{A}_1A_0\bar{B}_1B_0P0_1\overline{P0}_1\;V\;A_1\bar{A}_0\bar{B}_1\bar{B}_0P0_1\overline{P0}_0 \end{gathered} \tag{6}$$

Третий дешифратор определяет комбинацию входных чисел, при которых сумма чисел S_0 и S_1 будет равна двоичному коду 01, в этом случае также необходимо ввести коррекцию.

На выходе этого дешифратора формируется управляющий сигнал $УС_3$ по формуле

$$УС_3 = A_1\bar{A}_0B_1\bar{B}_0\overline{P0}_1P0_0\ V\ \bar{A}_1A_0B_1\bar{B}_0P0_1\overline{P0}_0\ V\ V A_1\bar{A}_0\bar{B}_1B_0P0_1\overline{P0}_0 \quad (7)$$

Четвертый дешифратор определяет комбинацию входных чисел A_0, B_0, P_{00}, A_1, B_1, P_{01}, при которых сумма чисел S_0 и S_1 будет равна двоичному коду 10, в этом случае также необходимо ввести коррекцию.

На выходе этого дешифратора формируется управляющий сигнал $УС_4$ по формуле

$$УС_4 = A_1\bar{A}_0B_1\bar{B}_0P0_1\overline{P0}_0 \quad (8)$$

Результатом суммирования входных чисел являются младший разряд суммы S_{10}, старший разряд суммы S_{11}, младший разряд переноса P_{10} и старший разряд переноса P_{11}. Разряды суммы S_{10} и S_{11} являются выходными разрядами, разряды переносов P_{10} и P_{11} вычисляются согласно выражениям (9), (10), (11) и (12) соответственно, являясь входными разрядами для последующих комбинационных схем сумматоров:

$$S_{10} = S_0 \oplus (УС_1 V\ УС_2 V\ УС_3) \quad (9)$$

$$S_{11} = S_1 \oplus P_1 \oplus \quad (10)$$

$$P_{10} = A_1\bar{A}_0B_1\bar{B}_0\overline{P0}_0\overline{P0}_1V\bar{A}_1\bar{A}_0B_1\bar{B}_0\overline{P0}_0P0_1V\ V\ A_1\bar{A}_0\bar{B}_1\bar{B}_0\overline{P0}_0P0_1VA_1\bar{A}_0B_1\bar{B}_0\overline{P0}_0P0_1 \quad (11)$$

$$P_{11} = \bar{A}_1A_0\bar{B}_1B_0\overline{P0}_0\overline{P0}_1\ V\bar{A}_1\bar{A}_0\bar{B}_1B_0P0_0\overline{P0}_1\ V\ V\ \bar{A}_1A_0\bar{B}_1\bar{B}_0P0_0\overline{P0}_1V\bar{A}_1A_0\bar{B}_1B_0P0_0\overline{P0}_1 \quad (12)$$

Блок регистра результата БРгР служит для хранения значений результатов, полученных при сложении входных чисел. Управление блоком осуществляется подачей информационных сигналов из блока управления. Блок управления БУ служит для генерации управляющих сигналов, поступающих на входы блоков устройства.

Представленный арифметический процессор можно использовать в вычислительной системе в виде специализированного модуля. Операции суммирования выполняются в прямых кодах, что значительно повышает быстродействие вычислительного процесса. Разработанная структурная схема сумматора-вычитателя может быть использована при построении универсальной троичной вычислительной машины.

Список литературы

1. Нейрокомпьютеры и интеллектуальные роботы / под ред. Н.М. Амосова. – Киев: Наукова думка, 1991.

2. Уоссермен Ф. Нейрокомпьютерная техника. – М.: Мир, 1992.

3. Пат. 2453900. Рос. Федерация, МПК G06 F7/505, G06 F7/49, F7/00. Параллельный сумматор-вычитатель в троичной системе счисления на нейронах / Шевелев С.С. – №2010108106/08; заявл. 04.03.2010; опубл. 20.06.2012, Бюл. №17. – 41 с.: ил.

УДК 004.053

А.С. Якушев, Д.Н. Караколючка, М.В. Алешечкин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКИ АВТОМАТИЧЕСКОГО ОПРЕДЕЛЕНИЯ ЯЗЫКА

Рассмотрены методы определения языка или смеси языков в документах. Производится описание принципов работы и алгоритм распознавания языков в существующих программных продуктах.

При стандартизации (приведении к универсальному виду) представления документов в интересах их информационной обработки одной из важных является задача определения языка или языков, на которых написан документ. Данный вопрос не является новым, и в настоящее время не составит труда найти программный комплекс, выполняющий распознавание языка. Но в задачах отбора информации по смыслу требуется дополнительное рассмотрение этого вопроса. Производя поиск информации с большей точностью, пользователь желает получить более точный и правильный ответ на его поисковый запрос. В некоторой степени этого можно добиться, распознав язык, использующийся в документе. Например, одна и та же статья может быть написана на нескольких языках, с точки зрения кодовых конструкций это две разные статьи, но

с точки зрения смысла – одна и та же. Тем самым, определив язык, мы уменьшаем количество выдаваемой информации и увеличиваем качество поисковой машины. Принципы определения языка незначительно различаются. Основные отличия заключаются в количестве введенных символов, способах выбора нужного языка из всех, заложенных в программу, количестве имеющихся в базе языков и словарной базой в каждом языке. Далее будут рассмотрены основные методики распознавания языка.

Технологии автоматического определения языка:

1. Технология guesser:

Автоматический определитель языка называют иногда guesser, что в переводе означает угадывающий. Он позволяет по введенным нескольким словам определить язык, на котором они написаны. Технически определение языка реализуется при помощи словаря.

Введенный текст разбивается на слова, и они сравниваются со словами из базы определителя. В определении языка участвуют не все слова. Например, алгоритм исключает предлоги, союзы и слова длиной менее 4-х символов. В результате подсчитывается количество совпадений слов разных языков и выводится отчет в виде названия одного языка или списка языков, которые были признаны наиболее подходящими.

Однако работа автоматического определителя языка не так проста: система должна учитывать лексические особенности языков, правила построения предложений, различия в диалектах и другие особенности. Поэтому сервисы автоматического определения языка предоставляются обычно разработчиками систем машинного перевода. Результат определения языка не может быть 100% точным. Обычно определитель языка также сообщает, с какой вероятностью ему удалось определить язык [1].

2. Библиотека PHPLangautodetect

Процесс автоматического определения языка неточен и принципиально является вероятностным. То есть всегда результат даётся с какой-либо вероятностью, особенно это касается языков, которые имеют очень схожий либо даже идентичный алфавит (в написании). При этом качество распознавания зависит от длины строки исследуемого текста: чем меньше материала для исследования, тем

сложнее или даже невозможно такое определение. Поэтому первым ограничением метода анализа используемого алфавита является длина текста, при этом чем она больше, тем точнее анализ.

Этот метод имеет две разновидности. Вариант «процента использования алфавита» использует подсчёт количества использованных уникальных символов алфавита и расчёт их доли в общем объёме текста. Второй вариант измеряет количество символов в тексте, которое совпадает с алфавитом, при этом некоторые символы могут попадать в разные алфавиты и засчитываться нескольким языкам.

Второй метод основан на использовании заранее сформированных правил, которые устанавливают идентичность текста при помощи уникальных или типичных для грамматики языка последовательностей букв (например, артикли в английском, буквы "ъ" и "ё" в русском или "є" в украинском). Хотя, если заранее известно, какие языки надо определять, то между ними может быть больше уникальных сочетаний, чем если использовать все языки.

Отдельно следует остановиться на случае, когда в тексте смешиваются слова разных алфавитов. Например, имена или названия компаний и товаров могут быть написаны на оригинальном языке, чаще всего английском, однако всё предложение сформулировано по-русски. Здесь поможет только вариант подсчёта общего количества символов, которые принадлежат алфавиту и на основе того, чьих символов больше, принимать решения.

Принцип работы:

Первым делом программа приводит полученную строку к стандартной форме, пытаясь её перекодировать, потом удаляет лишние знаки и проверяет длину. Минимальный объём текста 50 символов, максимальный – 1680.

Пользователь может задать различные варианты детектирования. Библиотека может использовать анализ алфавитов, при этом смотреть или на общий объем текста, или же на процент используемых букв каждого алфавита. Порог принятия решения также настраивается, по умолчанию это 75% (в зависимости от подсчёта это или 75% букв алфавита, или же в тексте общее количество символов этого языка больше 75%). Для более быстрой работы, особенно на больших объёмах текста или большом количестве

языков, можно использовать только правила, их обычно намного меньше, чем символов в алфавитах.

Возвращает библиотека после детектирования или значение false, что означает невозможность определения, или же то, что используемого языка нет в базе данных. В случае успеха пользователь получает массив с двухбуквенным кодом языка (для примера: "en", "ru" или "ua").

Для оптимизации работы автоматического определителя лучше всего заранее ограничить набор языков самыми вероятными и удалить те, которые не являются подходящими – таким образом сократится значительное число циклов и алгоритм будет работать быстрее [2].

Списки программных продуктов, производящие автоматическое определение языка:

1) guesser;
2) Xerox;
3) Talenknobbel;
4) TextCat;
5) Verbix;
6) TranslatedLabs;
7) Полиглот 3000 [3].

Достоинства и недостатки программных продуктов, производящих автоматическое определение языка, представлены в таблице.

Достоинства и недостатки программных продуктов, производящих автоматическое определение языка

Параметр	Программный продукт					
	guesser	Xerox	Talenknobbel	TextCat	Translated Labs	Полиглот 3000
Кол-во языков	58	81	20	69	102	Более 400
Режим работы: онлайн	+	+	+	+	+	–
Режим работы: установка на ПК	–	–	–	–	–	+
Показ точности	+	–	+	–	–	+

Наиболее распространенная и развитая среди данных программ – определитель языка Полиглот 3000, так как:

1) распознаёт более 400 языков;

2) полностью поддерживает Уникод;

3) быстрое и точное определение языка;

4) возможность определения языка среди наиболее популярных;

5) программа работает в операционных системах Windows 95/98/NT/ME/2000/XP/2003/Vista/2008/7/8 [4].

Также серьезной задачей является не только определение языка, но и повышение правильности и качества определения языка.

Для решения этой задачи можно воспользоваться следующими рекомендациями:

1) использование не менее 20-ти слов (чем больше, тем лучше);

2) проверка текста на ошибки перед определением языка;

3) ввод в определитель части текста, которая позволит более эффективно определить язык (например, слова с наличием нестандартных букв, надстрочных и подстрочных символов, и т.д.);

4) для более точного результата воспользоваться несколькими сервисами распознавания языка;

5) отбрасывание языков, которые точно не подходят для данного текста;

6) расширение количества параметров при распознавании языковой конструкции.

Произведя рассмотрение и анализ автоматических определителей языка, можно сделать вывод, что принцип работы идентичен и различия незначительны у всех программных продуктов. Главными показателями в распознавании являются количество символов и уникальные или типичные для данного языка символы или последовательности. Определение производится вероятностными методами и получение 100% точного результата невозможно. Для получения более точного результата необходимо к вероятностным методам добавлять последовательный анализ большего числа параметров, таких как более сложный грамматический, морфологический и синтаксический анализы.

Список литературы

1. Автоматический определитель «Guesser.ru» [Электронный ресурс] // Автоматический определитель. – URL: http://guesser.ru/.

2. Alpha-Beta-Release Blog [Электронный ресурс] // Автоматическое определение языка произвольного текста на PHP – библиотека PHPLangautodetect. – URL: http://abrdev.com/?p=346.

3. Онлайн-переводчики и онлайн-словари для всех языков мира [Электронный ресурс] // Автоматические определители языков. – URL: http://mrtranslate.ru/guessers.php.

4. Likasoft – лингвистические технологии будущего [Электронный ресурс] // Полиглот 3000. – URL: http://www.polyglot3000.com/ru/index.shtml.

УДК 004.622

А.С. Якушев, Д.Н. Караколючка, М.В. Алешечкин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АЛГОРИТМ ПРИВЕДЕНИЯ ИНФОРМАЦИИ К СТАНДАРТИЗОВАННОМУ ВИДУ

Рассмотрены вопросы стандартизации описания и адресации структурных элементов, приведения разноформатных файлов к заданному виду.

Одной из важных технологических задач при построении систем селекции информации является задача приведения входной информации к некоторым стандартным видам и формам.

Актуальность задачи связана, с одной стороны, с большим разнообразием применяемых на практике форматов представления информационных документов и, с другой стороны, тем фактом, что документы, поступающие на вход системы, как правило, содержат различные по типам и видам составляющие элементы. В этой связи необходимо определить рациональный состав процедур определения и преобразования форматов элементов входных документов к стандартным видам и формам и алгоритм их выполнения. С точки зрения технологий такого преобразования, исходя из общности принципов их последующей информационной обработки, во всей совокупности возможных форматов входных документов следует выделить следующие группы: текст, аудио, видео, формальные языки, графика, архивы и сжатые файлы.

Как показано в работе [1], в принципиальном плане на входе поисковой системы может быть до нескольких десятков форматов представления документов. Исходя из общей логики построения

документов, каждый из них может быть как моно, так и полиформатным. Отсюда следует, что в итоговом описании документа для последующей информационной селекции мы должны сохранить, с одной стороны, его информационную логику, а с другой стороны, выделить в каждом из них все технологические группы, образующие информационные элементы документа.

Исходя из вышеизложенного общая процедура преобразования входного документа в стандартную форму должна включать следующие функции: определение формата и языка, выявление сопроводительной и реквизитной информации, произведение классификации файлов по форматам и отнесение их к соответствующей группе, приведение файла к стандартному виду. Алгоритм их выполнения представлен на рисунке 1.

Определив формат файла, классифицируем его и делаем выводы о том, к какой из групп он относится. Классификация на группы форматов зависит от того, в какой форме информация заложена внутри документа. Первоначально определяется тип языка документа или его элемента: естественные и искусственные языки. При этом под естественным языком понимается язык в собственном смысле слова, человеческий язык [2]. А под искусственным языком понимается знаковая система, создаваемая специально для использования в тех областях, где применение естественного языка менее эффективно или невозможно. Сконструированные языки различаются по специализации и назначению, а также по степени сходства с естественными языками [3].

Последующее деление внутри каждого класса на группы, связанные с технологическими особенностями последующей обработки, производится следующим образом:

1) текст;
2) графика;
3) формальные языки (Delphi, C++, AutoCAD и др.);
4) текст + графика;
5) архивы и сжатые файлы;
6) PDF, DejaVu, рукописные материалы и др.;
7) мультимедиа (аудио, видео и др.).

Произведя классификацию и отнесение файла к соответствующей группе, возможно приступить к детальному описанию составляющих частей и структуры документ. Поскольку имеются

различные виды содержащейся внутри документа информации, то и методы обработки различны. Например, метод обработки архивов и сжатых файлов заключается в том, что при анализе их формата следует учитывать, что внутри данного типа файлов будут документы, относящиеся к другим группам. Для решения данной проблемы необходимо перед классификацией сделать раскрытие архива и только потом производить обработку содержащихся внутри документов.

Последующая работа с текстовыми файлами заключается в том, что текст необходимо разложить на составляющие его элементы и выявить сопроводительную и реквизитную информацию.

Целью данного рассмотрения является алгоритм, учитывающий следующие аспекты:

– подготовка текста с точки зрения видов сообщений, т.е. технологий отбора;

– отбор информации по признаковым значениям (по смыслу);

– отбор информации по кодовым конструкциям.

Текстовый файл требует выявления и описания его информационной структуры. На рисунке 2 представлена схема подготовки текста для дальнейшего преобразования и обработки.

Из имеющегося текста выделяются первоначальные и главенствующие данные, а именно: название, автор, количество страниц, рецензенты, содержание, дата публикации и другое.

Определение вышеуказанных данных позволяет нам производить отбор информации при поиске по первичной информации, этот принцип использует действующие поисковые системы. Поиск и выделение в тексте ссылок на литературу и сайты позволяет расширить круг искомой информации. При поиске нам выдается, так называемая аннотация к файлу. Выделенную основную информацию из текста подвергают разложению на составляющие части для последующей работы с текстом. Входящий текст раскладывается на структурные элементы: оглавление, разделы, главы, подглавы, параграфы, абзацы, предложения, слова, а слова в свою очередь проходят морфологический разбор. Для каждого структурного элемента текста должна производиться адресация или нумерация элементов. Это позволит в дальнейшем производить более легкое сравнение нескольких текстов при отборе информации по смыслу.

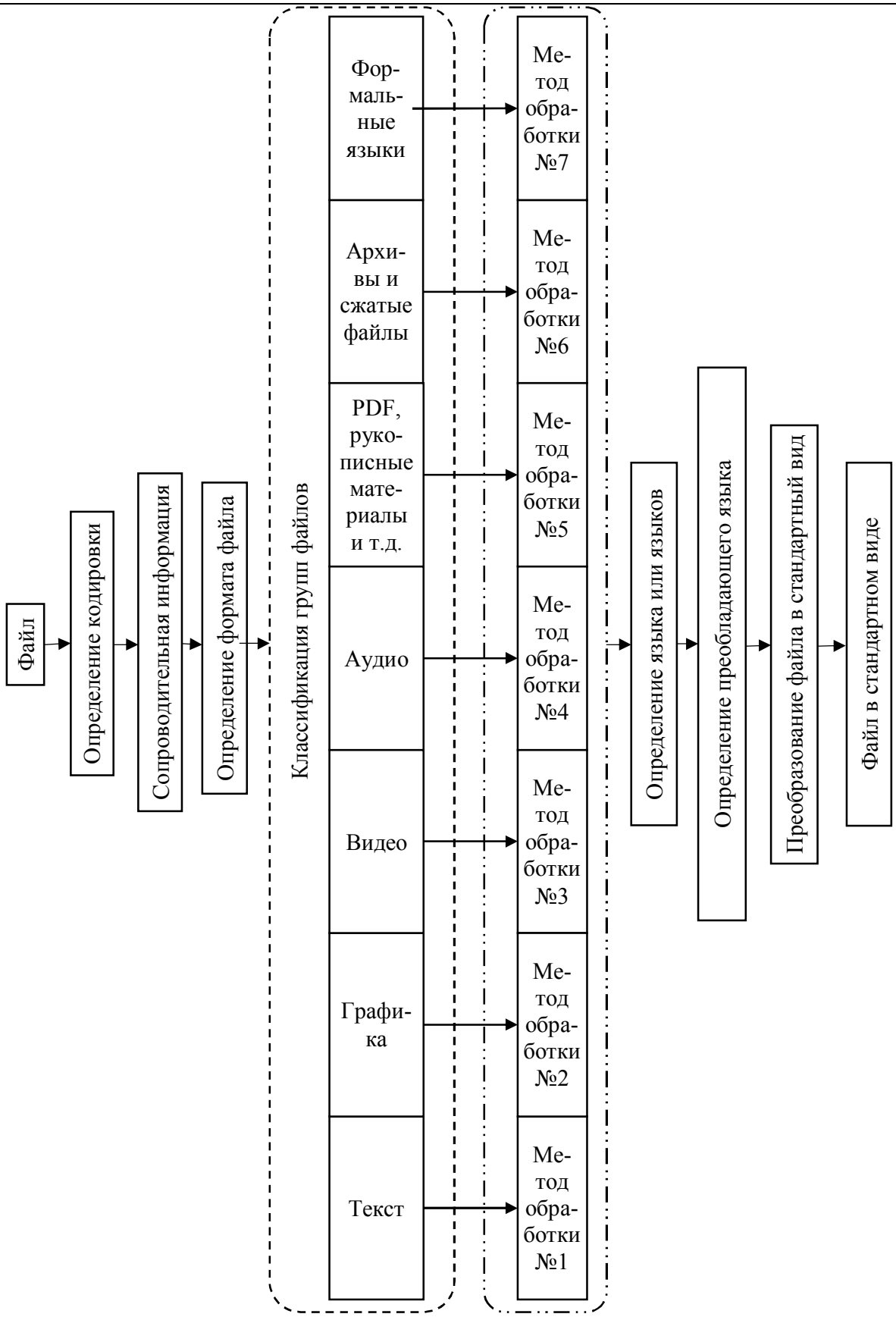


Рис. 1. Обобщенная схема приведения файла к универсальному виду

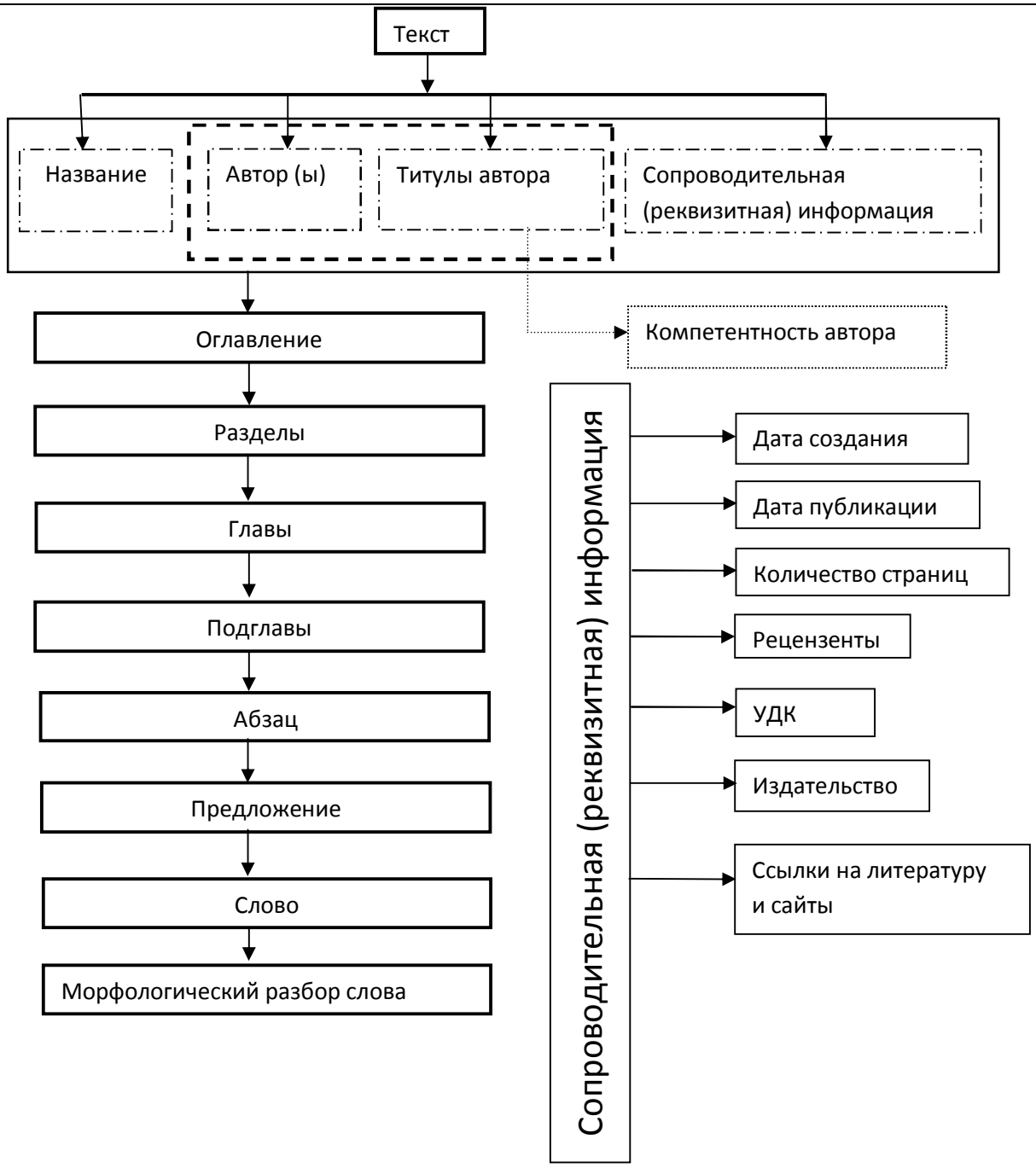


Рис. 2. Разбиение текста на структурные элементы

Метод обработки файлов типа PDF, DejaVu и рукописные материалы предусматривает вмешательство человека в процесс обработки, поскольку зачастую проблематично, а в некоторых ситуациях и невозможно произвести автоматическую обработку документа в связи с его особенностями.

Выполнив промежуточную обработку и разложение документа на структурные элементы, системе необходимо осуществить

определение языка, на котором написан документ, или преобладающего языка при наличии смеси языков.

Конечным этапом является преобразование исходного документа в стандартный вид.

Поскольку для достижения поставленных выше целей необходимо каждому элементу и свойству файла присвоить свои значения, то возникает необходимость в программном продукте, позволяющем это сделать. С точки зрения связывания различных типов данных и структурирования информации в документе целесообразно использовать язык XML. В первую очередь, эта технология может оказаться полезной для разработчиков сложных информационных систем, с большим количеством приложений, связанных потоками информации с самой различной структурой. В этом случае XML-документы выполняют роль универсального формата для обмена информацией между отдельными компонентами большой программы. Это связано с тем, что:

– XML является базовым стандартом для нового языка описания ресурсов, RDF(ResourceDescriptionFramework — модель описания ресурсов), позволяющим упростить многие проблемы в Web, связанные с поиском нужной информации, обеспечением контроля за содержимым сетевых ресурсов, созданием электронных библиотек и т.д.

– язык XML позволяет описывать данные произвольного типа и используется для представления специализированной информации.

– XML может использоваться в обычных приложениях для хранения и обработки структурированных данных в едином формате.

– XML-документ представляет собой обычный текстовый файл, в котором при помощи специальных маркеров создаются элементы данных, последовательность и вложенность которых определяет структуру документа и его содержание.

Основным достоинством XML-документов является то, что при относительно простом способе создания и обработки (обычный текст может редактироваться любым тестовым процессором и обрабатываться стандартными XML-анализаторами) они позволяют создавать структурированную информацию, которую хорошо «понимают» компьютеры [5].

Список литературы

1. Словарь лингвистических терминов [Электронный ресурс] // Словарь лингвистических терминов (естественный язык). – URL: http://dic.academic.ru/dic.nsf/lingvistic/410/естественный.

2. Словарь лингвистических терминов [Электронный ресурс] // Словарь лингвистических терминов (искусственный язык). – URL: http://sociolinguistics.academic.ru/240/Искусственный_язык.

3. CodeNet – все для программиста [Электронный ресурс] // Язык XML. Описание технологии. – URL: http://www.codenet.ru/webmast/xml/part2.php.

УДК 621.398

Н.В. Воронков, В.Ю. Демьяненко

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СЕТЕВАЯ ОРГАНИЗАЦИЯ РЕЦЕПТОРНО-ИСПОЛНИТЕЛЬНОЙ СРЕДЫ АВТОМАТИЗИРОВАННОГО ЗДАНИЯ

Проведен анализ существующих технологий организации системы «Умный дом» в различных условиях жилья, выявлены их достоинства и недостатки.

Современное общество предъявляет очень высокие требования к комфортности среды обитания. В результате инженерное оснащение квартир и коттеджей неуклонно усложняется, растет количество устройств, участвующих в формировании этой среды. Возлагать на хозяина жилья управление всеми системами становится неудобно, невыгодно и небезопасно. Поэтому сейчас все больше внимания уделяется комплексной системе управления жилищем «Умный дом». Данная система берет на себя всю рутинную работу по решению этой сложной задачи, оставляя человеку только принятие главных, базовых решений [1].

Система «Умный дом» предусматривает наличие большого количества электрических и слаботочных коммуникаций, коммутаторов, датчиков (сенсоров), исполнительных механизмов (актуаторов). В среднем на реализацию бюджетного варианта «Умного дома» в квартире необходимо около 70 датчиков и столько же исполнительных устройств, а при реализации в полноценном коттедже это количество увеличивается примерно вдвое (табл.) [2]. Но и в том, и другом случае следует охватить все системы жизнеобеспе-

чения, начиная от отопления и водоснабжения и заканчивая системой безопасности и мультимедийной системой. Поэтому существует проблема, заключающаяся в организации простой и надежной связи большого количества датчиков и исполняющих механизмов с центральным вычислительным элементом системы. Причем эта связь должна эффективно работать в разных условиях жилья (от отдельного коттеджа до квартиры в многоэтажном доме).

Ориентировочное количество датчиков, используемое при реализации «Умного дома» в коттедже

Подсистема «Умного дома»	Количество датчиков
Климат-контроль: – вентиляционная система – отопительная система – кондиционирование	 10 10 10
Водоснабжение	4
Управление освещением	20
Система безопасности: – охранно-пожарная сигнализация – пожаротушение – контроль доступа – видеонаблюдение	 10 10 12 5
Мультимедийная система	15
Управление электропитанием	5
Телевидение и связь	7
Придомовая инфраструктура	7
Система общего управления	15
Всего	140

На физическом уровне система «Умный дом» может быть организована с помощью проводных, беспроводных технологий, а также технологий, использующих домашнюю электропроводку.

Проводной вариант построения сети «Умного дома» отличается прежде всего надежностью и безопасностью соединения. Обычно реализуется с помощью витой пары. Идеальными условиями для создания такой проводной сети являются капитальный ремонт и проектирование зданий «с чистого листа».

Однако у проводных решений есть один общий недостаток – все они требуют прокладки проводов и кабелей, реализация которой, особенно в старом жилом фонде, вызывает большие трудности. Более того, существует ряд случаев, при которых прокладка новых кабелей невозможна или крайне нежелательна.

Поэтому особый интерес всегда вызывали те технологии, которые позволяли обойтись без прокладки новых кабелей. На данный момент существует два успешных подхода к этой проблеме – это беспроводные сети и технологии PLC (Power Line Communications – коммуникации по силовым линиям).

Беспроводные технологии «Умного дома» работают обычно на частотах 868 и 433 МГц. Датчики могут быть как без обратной связи, так и с обратной связью. В последнем случае сенсор повторяет сигнал, пока не получит подтверждение от исполнительного устройства, что команда выполнена.

С одной стороны, беспроводные технологии характеризуются:

– мобильностью;

– простотой и меньшим временем развертывания;

– гибкостью, т.е. быстрой реструктуризацией и изменением размеров конфигурации сети;

– возможностью развертывания в тех местах, где нельзя воспользоваться кабельными сетями;

– низким энергопотреблением;

– огромной номенклатурой беспроводных датчиков.

С другой стороны, эти технологии имеют:

– более высокую стоимость, чем проводные системы;

– сравнительно низкую надежность связи, связанную с возможным наличие на пути радиоволн препятствий;

– теоретическую возможность блокирования связи злоумышленниками;

– зависимость от энергопитающих элементов (уже сейчас появляются необслуживаемые выключатели и датчики, получающие энергию для своей работы из окружающей среды).

Технологии PLC позволяют построить сеть на основе существующих линий электропередач. В настоящее время технология PLC за счет применения OFDM-модуляции (Orthogonal Frequency Division Multiplex), основанной на ортогональном частотном

уплотнении с одновременной передачей сигналов на нескольких несущих и быстрых сигнальных процессоров, позволяет добиться большой скорости передачи и хорошей устойчивости сигнала к помехам.

Данной технологии присущи следующие преимущества:

– нет необходимости в прокладке кабеля;

– быстрая скорость настройки сети;

– стабильность связи;

– большая безопасность информации по сравнению с беспроводными;

– на качество связи не влияет материал и толщина стен в доме;

– можно использовать для передачи Multicast-трафика, например IPTV.

К недостаткам можно отнести следующее:

— влияние на стабильность и скорость работы качества выполнения электропроводки, наличия стыков из разных материалов (например, медного и алюминиевого проводника);

— не обеспечивается работа устройств, подключенных через сетевые фильтры и к источникам бесперебойного питания, не оборудованные специальными розетками;

— влияние на качество связи наличия дешевых энергосберегающих ламп, тиристорных диммеров, импульсных блоков питания и зарядных устройств.

Таким образом, можно сделать вывод, что на этапе строительства или капитального ремонта здания наиболее рациональным решением для реализации системы «Умный дом» являются проводные технологии, доказавшие свою надежность. Беспроводные и PLC-технологии целесообразно устанавливать в уже готовый дом, в котором нежелательна прокладка кабелей.

Каждый дом или квартира имеет свои особенности планировки, и поэтому оптимальным вариантом все же будут комбинированные системы. Например, сенсоры – беспроводные, а исполнительные устройства – проводные. Зачастую на практике именно так и поступают, поскольку объекты управления привязаны к определенным местам, поэтому к ним заранее можно подвести провода. Управление же может выполняться из любой точки дома, что удобно осуществлять по ИК или радиоканалу.

1. Фальков А. И., Сузан Д. В. Что такое LON. Краткий обзор технологии LonWorks. – М.: Учебный центр АРМО, 2006. – 59 с.

2. Автоматизированное управление пространством [Электронный ресурс]. – URL: http://intelkey.ru.

УДК 004.9

В.В. Гефнер, В.Ю. Демьяненко

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СЕТЕВЫХ СИМУЛЯТОРОВ В УЧЕБНОМ ПРОЦЕССЕ

Рассмотрены проблемы приобретения студентами практических навыков работы с сетевым оборудованием. Приводятся результаты анализа сетевых симуляторов, позволяющих получить навыки управления различными элементами сети.

В настоящее время широкое использование современных информационных технологий требует от будущего специалиста в области телекоммуникаций уверенного владения как теоритическими знаниями, так и навыками их использования на практике. Теоретические знания студент получает на лекционных занятиях, а практические – в процессе выполнения лабораторных работ. Однако в такой технически насыщенной предметной области, как телекоммуникации, существует проблема приобретения практических навыков работы с сетевым оборудованием, связанная с большим количеством производителей и номенклатуры сетевых устройств, а также их стоимостью. Далеко не каждое учебное заведение может позволить себе приобретение коммутаторов, маршрутизаторов и другого сетевого оборудования для проведения лабораторных и практических занятий. Наличие большого количества производителей ещё более усложняет эту задачу.

Одним из путей приобретения студентами устойчивых практических навыков работы с сетевым оборудованием является использование специальных программных продуктов, симулирующих работу телекоммуникационных систем. Применение подобного программного обеспечения позволяет проводить необходимые исследования и эксперименты гораздо экономнее и получать практически те же результаты, что и на реальном оборудовании.

Учитывая, что около 64% мирового рынка сетевого оборудования производит CiscoSystems [1], целесообразно для обучения использовать оборудование этой компании.

В [2] проводился анализ наиболее известных сетевых симуляторов оборудования компании CiscoSystems. Однако при анализе симуляторов не рассматривались:

1. Стоимость программного продукта.

Этот фактор, безусловно является одним из основных. Программный продукт, распространяющийся бесплатно, позволит использовать его непосредственно в вузе и предоставляет возможность студентам выполнять задания дома, что повышает эффективность самостоятельного обучения.

2. Функционал оборудования.

Наиболее полно функционал может быть охарактеризован:

а) количеством симулируемого оборудования.

Для проведения лабораторных работ и обучения необходимо, чтобы в программном продукте реализовывались несколько видов маршрутизаторов из различных серий (например, 2600, 2900, 3600, 7200); Ethernet-коммутаторы и концентраторы; устройства безопасности: сетевые экраныPIX, ASA и системы обнаружения/предотвращения атакIDS/IPS;

б) полнотой реализации технологий Ethernet, FrameRelay, ATM;

в) используемой операционной системой IOS.

Cisco IOS (от англ. InternetworkOperatingSystem — Межсетевая Операционная Система) — программное обеспечение, используемое в маршрутизаторах и коммутаторах Cisco [3]. Программный продукт, реализующий неполный функционал IOS, препятствует эффективному изучению оборудования и создаёт ложное представление о возможностях современных сетевых устройств.

3. Возможность подключения виртуальной сети к реальной.

Это позволяет повысить наглядность созданной топологии и обеспечивает возможность работы с реальным периферийным оборудованием (например, при изучении ip-телефонии).

4. Кроссплатформенность.

Кроссплатформенность снимает ограничение на использование программного продукта в различных операционных системах.

В таблице представлены результаты анализа сетевых симуляторов с указанием авторской оценки значимости потребительских характеристики симуляторов.

Результаты анализа сетевых симуляторов

Симулятор	Стоимость (макс. 3 б.)	Реализуемый функционал оборудования (макс. 3 б.)	Подключение к реальной сети (макс. 1 б.)	Кросс-платформенность (макс. 1 б.)	Интерфейс (макс. 2 б.)	Формирование и автом. проверка тестовых заданий (макс. 1 б.)	Суммарный балл
PacketTracer	Доступен только участникам сетевой академии Cisco (1 б.)	Есть необходимое оборудование, кроме PIX, ASA, IDS/IPS; функционал IOS ограничен (2 б.)	Нет возможности (0 б.)	Да (1 б.)	Интуитивно понятен, русифицирован (2 б.)	Возможно (1 б.)	7
Dynamips	Бесплатен (3 б.)	Нет устройств безопасности PIX, ASA, IDS/IPS; функционал IOS полный (1 б.)	Возможно (1 б.)	Да (1 б.)	Нет графического моделирования, не русифицирован (0 б.)	Нет возможности (0 б.)	6
GNS3	Бесплатен (3 б.)	Есть всё необходимое оборудование; функционал IOS полный (3 б.)	Возможно (1 б.)	Да (1 б.)	Интуитивно понятен, русифицирован (2 б.)	Нет возможности (0 б.)	10
Boson NetSim	99-349$ (2 б.)	Есть необходимое оборудование, кроме PIX, ASA, IDS/IPS; функционал IOS полный (2 б.)	Нет возможности (0 б.)	Нет (0 б.)	Сложен для начинающего пользователя, не русифицирован (0 б.)	Нет возможности (0 б.)	4

Примечание. В скобках указано количество баллов, которое характеризует степень соответствия критериям.

Из таблицы следует, что для проведения лабораторных работ по сетевым технологиям без использования реального оборудования целесообразно использовать симулятор GNS3, поскольку этот продукт наиболее полно отвечает заданным требованиям.

Дополнительными возможностями данного симулятора являются:

– использование виртуальных машин (Qemi, VirtualBox, WMware) в созданной сети;

– симуляция маршрутизаторов других производителей: Juniper и MikroTik;

– анализ трафика в любой точке виртуальной сети с помощью Wireshark;

– использование сервера для переноса нагрузки моделируемой топологии без применения специализированного программного обеспечения [4].

Следует отметить, что наряду с формированием у студентов устойчивых навыков работы с реальным сетевым оборудованием, GNS3 может эффективно использоваться и преподавателем для демонстрации лекционного материала. Студенты выпускных курсов могут использовать GNS3 как платформу, на которой будут реализовываться сетевые топологии из их дипломных проектов.

Список литературы

1. Сетевое оборудование [Электронный ресурс]. – URL: http://www.info.uz/press/?p=353.

2. Ромазов В.В., Матюнина Е.С. Анализ существующих способов и средств обучения специалистов по сетевой тематике/ ред. кол.: А.М. Потапенко (отв. ред.) [и др.] // XII Международная научно-методическая конференция вузов и факультетов инфокоммуникаций; Юго-Зап. гос. ун-т. – Курск, 2012. – С. 190-192.

3. Уэнделл Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNAICND2. – 3-е изд. – М.: Вильямс, 2010. – 752 стр.

4. GNS3: Graphical Network Simulator [Электронный ресурс]. – URL: http://www.gns3.net.

УДК 004.77

Ю.А. Василенко, А.А. Гуламов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ИНФОРМАЦИОННАЯ СИСТЕМА ДОШКОЛЬНОГО ДЕТСКОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Рассматривается информационная модель детского образовательного учреждения при разработке инфокоммуникационной системы.

Деятельность дошкольного детского образовательного учреждения (ДОУ), как и любой организации, сопровождается обработкой и перемещением большого количества информации. Подразделения ДОУ пронизаны вертикальными и горизонтальными связями, они обмениваются информацией между собой, выполняя часть одной большой работы.

Такой взгляд на ДОУ позволяет сформулировать некоторые общие принципы при разработке для него инфокоммуникационной системы. От скорости обработки и передачи данных в инфокоммуникационной системе будет зависеть успех всей деятельности ДОУ. Без оптимизации применения технических средств и грамотно разработанной информационной системы затраты на внедрение не дадут желаемого результата.

Оборудование и программные средства для информационной системы – это набор инструментов. Только полное представление о том, как и какие задачи будут решаться с использованием этих инструментов, дает результат при внедрении информационной системы [1, 2].

Информационная модель ДОУ представлена на рисунке.

Типовая информационная модель ДОУ имеет 5 основных контуров:

1) административный контур;

2) контур безопасности;

3) контур мониторинга медицинского и санитарного состояния;

4) хозяйственный контур;

5) образовательно-развлекательный контур.

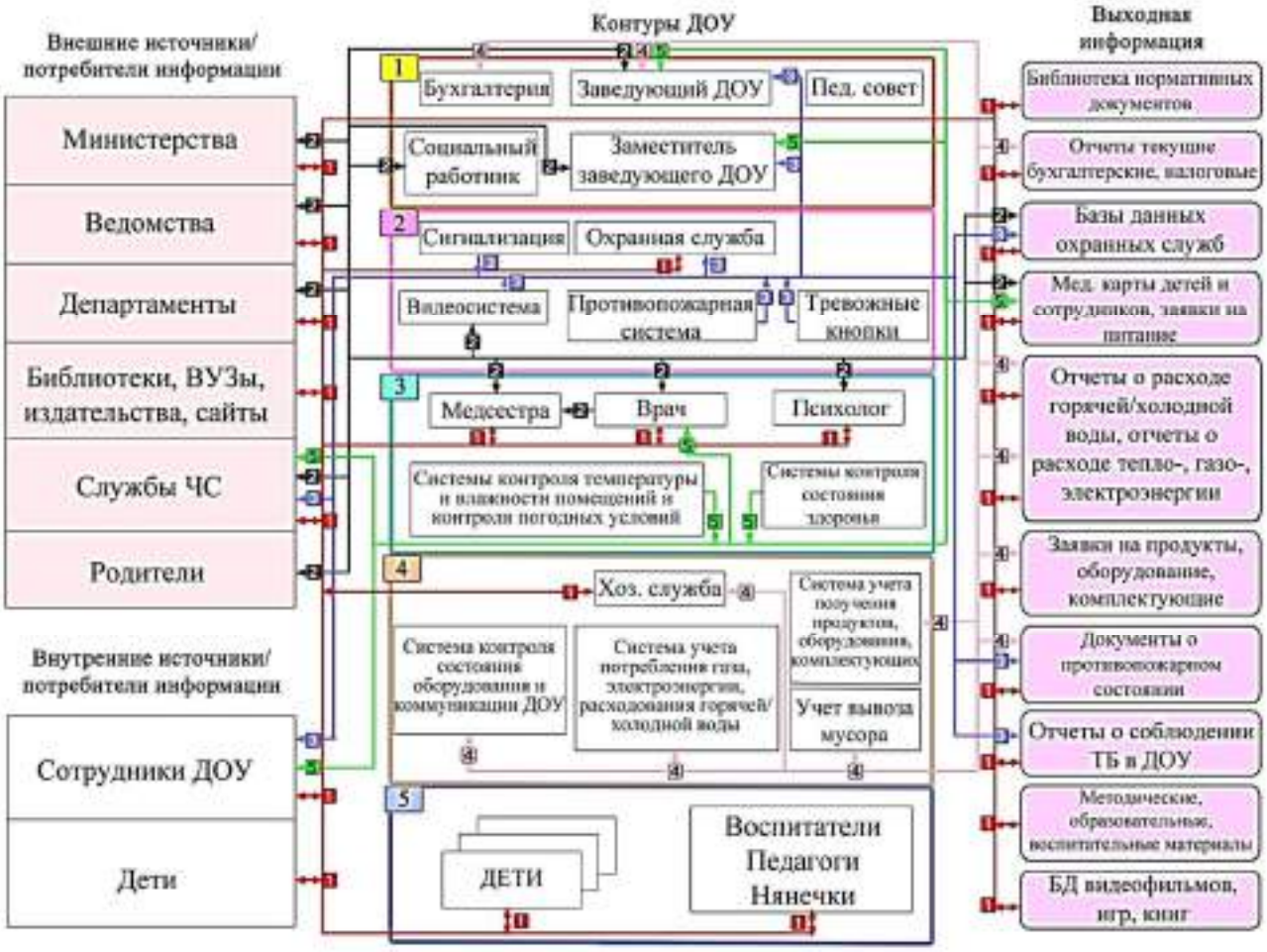


Рис. Информационная модель ДОУ

Контуры на рисунке обозначены цифрами от 1 до 5 соответственно.

В ДОУ циркулирует 5 основных видов информации, на рисунке каждый поток обозначен цифрой от 1 до 5 соответственно: текст; видео; сигналы с датчиков пожарной безопасности, сигналы сигнализации, тревожная кнопка; сигналы сенсорных систем показаний состояния оборудования ДОУ; сигналы с сенсорных систем биомедицинской информации.

В левой части рисунка представлены внешние и внутренние источники и получатели информации. Внешними являются федеральные, региональные, местные законодательные и исполнительные органы власти, ведомства, организации, родители и др. Внутренними – сотрудники ДОУ и дети.

Административный контур содержит в себе информацию текстового характера (нормативные документы, распоряжения и т. д.).

Данный вид информации необходим для организации повседневной деятельности ДОУ в рамках законодательства РФ. В административный контур поступает информация от федеральных, региональных служб, министерств и ведомств РФ. Данная информация направлена на регулирование деятельности ДОУ в законодательной, налоговой сферах деятельности, а также деятельности в сфере воспитания и здравоохранения.

Данная информация поступает в первую очередь к заведующей ДОУ, а затем распространяется по всему административному контуру, после чего уже поступает в виде внутренних распоряжений во все остальные контуры информационной системы ДОУ. В свою очередь внутренние потребители информации предоставляют текущую отчетную информацию и другую информацию в административный контур, таким образом, поток информации является двунаправленным.

Контур безопасности охватывает широкий спектр задач. Информация данного контура представляет собой видеоматериалы с камер видеонаблюдения, сигналы с датчиков регистрации пожарной безопасности, сигналы с датчиков, регистрирующих проникновение в помещения ДОУ, установленных на окнах и дверях, а также сигналы тревожной кнопки. Данный контур должен обеспечивать организацию непрерывного видеонаблюдения за внешней и внутренней территорией ДОУ, а также по ее периметру. Данная информация должна быть доступна таким внутренним потребителям, как дежурный охранник, заведующий ДОУ, медицинским работникам. Система также может обеспечивать возможность просмотра поведения детей внешними потребителями – родителями. Она должна обеспечивать длительное хранение видеоматериалов в базе данных. Потребителями информации систем пожарной безопасности, сигнализации на проникновение, а также тревожной кнопки являются служба охраны и заведующий ДОУ, которые принимают решение о передаче информации в службу 112 в случае ЧС.

Вопрос о возможности просмотра видеоинформации родителями принимается заведующим ДОУ на основе решения общего собрания родителей, медицинских работников и педагогического коллектива ДОУ в соответствии с законодательством РФ.

Контур мониторинга медицинского и санитарного состояния получает распоряжения от административного контура в виде распоряжений и приказов. Данный контур содержит в себе информацию с камер видеонаблюдения, которая необходима психологу для оценки поведения детей и психологической обстановки в группах. Данная информация должна поступать психологу непрерывно, т. к. в случае регистрации каких-либо отклонений в поведении ребенка психолог должен незамедлительно отреагировать на сложившуюся ситуацию. Информация с сенсорных систем мониторинга биомедицинского состояния детей, а также сотрудников ДОУ поступает к врачу. Данная информация необходима для непрерывного контроля состояния детей в стенах учреждения, быстрого реагирования медицинского работника в случае ухудшения показателей, изоляции больного ребенка от остальной группы детей и принятия необходимых мер для проведения его лечения, а также с целью выявления больных детей и сотрудников ДОУ по результату измерения их температуры экспресс-методом на входе в помещение ДОУ для принятия решения о пребывании ребенка в группе или в изоляторе и допуске сотрудника к месту работы.

В медицинском контуре содержится информация с сенсорных систем измерения показателей температуры, влажности внутри помещения и на внешней территории ДОУ. Данная информация необходима медицинскому работнику ДОУ для принятия решения о коррекции данных показателей внутри помещения с целью приведения данных показателей к нормам, установленным санитарными требованиями [3], а также для принятия решения о проведении прогулки детских групп в зависимости от погодных условий.

В случае жалоб детей сотрудникам в устной форме на ухудшение их физического или психологического состояния эта информация должна передаваться медицинскому персоналу, который оповещает заведующего ДОУ для принятия совместного решения. Данные о состоянии здоровья детей и сотрудников ДОУ заносятся в медицинские карты с последующим сохранением их в базе данных. Текущие данные о санитарном состоянии помещений и прилегающей территории ДОУ фиксируются и сохраняются в базе данных.

Таким образом, в данном контуре видеоинформация пересекается с информацией, содержащейся в контуре безопасности. Потребителями данной информации являются медицинские работники и заведующий ДОУ. Отчеты, сформированные врачом ДОУ, поступают к заведующему ДОУ, т. е. информация данного контура также является двунаправленной.

Информация хозяйственного контура – это информация с различных сенсорных систем, регистрирующих потребление тепловой энергии, горячей и холодной воды, газа и электроэнергии, а также предназначенных вести контроль за состоянием оборудования и различных систем ДОУ. В данном контуре формируется следующая выходная информация: заявки на закупку продуктов, оборудования и комплектующих; документы, фиксирующие расход тепловой энергии, газа, расход холодной и горячей воды; документы, фиксирующие состояние противопожарных систем ДОУ, а также соблюдение техники безопасности на территории ДОУ. Данный вид информации необходим для таких потребителей информации, как заведующий ДОУ, бухгалтерия, службы ЧС.

Образовательно-развлекательный контур получает информацию от внешних источников, таких как библиотеки, ВУЗы, издательства, сайты для формирования детской библиотеки в ДОУ, проведения занятий в детских группах и просмотра обучающих и развлекательных видеофильмов. Методическая информация поступает к педагогам и воспитателям ДОУ, данная информация необходима для проведения повседневной педагогической деятельности. Воспитатели ДОУ формируют отчеты о проведенной ежемесячной работе с группой.

Основные виды формирующейся информации в ДОУ представлены в правой части рисунка.

Разработанная информационной модель ДОУ служит основой в процессе разработки варианта типовой инфокоммуникационной системы ДОУ. Анализ всех информационных потоков позволяет предложить оптимальный вариант архитектуры и топологии инфокоммуникационной системы.

Список литературы

1. Информационная система предприятия [Электронный ресурс]. – URL: http://www.itn.ru/ solutions/system/.

2. Корпоративные информационные системы: технологии и решения [Электронный ресурс]. – URL: http://xsieit.ru/download/design_of_ information_systems/lectures/ 876.html.

3. Постановление Главного государственного санитарного врача Российской Федерации от 22 июля 2010 г. N 91 // Российская газета. – 2010. – 8 сент. – Вып. №5280.

УДК 621.372

А.Е. Севрюков, М.Г. Жидких

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПЕРСПЕКТИВЫ МОДЕРНИЗАЦИИ СЕТЕЙ СВЯЗИ ОТ 2G/3G К LTE

Рассмотрена стратегия, подразумевающая создание объединенной сети с учетом условий, необходимых для поддержания взаимодействия сети 4G с существующими сетями 2G/3G.

Основной целью создания стандарта четвертого поколения LTE можно назвать наращивание возможностей высокоскоростных систем мобильной связи, уменьшение стоимости передачи данных, возможность предоставления широкого спектра всевозможных услуг. LTE-сеть кардинально отличается от сетей 2G/3G, во-первых, принципиально иным методом формирования группового радиосигнала, во-вторых, значительно расширенным логическим уровнем и отличным программным обеспечением, в-третьих, повышенной абонентской емкостью, намного большими скоростями передачи в восходящем и нисходящем каналах, более разумным использованием частотного ресурса. В настоящей работе ставится перспективная задача модернизации существующих сетей 2G и 3G путем их преобразования и интеграции, что позволит перейти к сетям 4G.

Известно, что 2G – цифровая мобильная связь с коммутацией каналов (стандарты GSM 900/1800 и cdmaOne). 3G – стандарты UMTS и CDMA2000, которые предусматривают наряду с коммутацией каналов и пакетную передачу данных. Основой для создания семейства стандартов 3G стала технология радиодоступа WCDMA.

Сети, разработанные на основе WCDMA, имеют все функции и возможности GSM и радиоинтерфейс WCDMA, который обеспечивает передачу данных с теоретической скоростью до 7 Мбит/с. В радиоканале используется частотный диапазон 5 ГГц.

Стандарт четвертого поколения LTE характеризует беспроводную мобильную сеть, которая позволяет достигнуть скорости передачи данных до 300 Мбит/с. При этом стандартом предусмотрена возможность работы сети в нескольких радиочастотных диапазонах, начиная от 700 МГц, заканчивая 4 ГГц, с вариативным дуплексом FDD (частотный дуплекс) или TDD (временной дуплекс).

В интегрированных сетях необходимо использовать уже развернутые в сетях 2G/3G элементы основной сети, такие как SGSN и GGSN.

Так, SGSN (англ. Serving GPRS SupportNode) – это узел обслуживания абонентов GPRS, основной компонент GPRS-системы по реализации всех функций обработки пакетной информации. Он является точкой соединения между системой базовых станций (BSS) сети радиодоступа (RAN) и базовой сетью (CN), взаимодействующей с HLR (англ. HomeLocationRegister), централизованной базой данных, которая содержит информацию о каждом абоненте данной сети. SGSN можно назвать аналогом коммутатора MSC сети GSM.

SGSN выполняет следующие функции:

− контроль доставки пакетов данных пользователям;

− взаимодействие с реестром собственных абонентов сети HLR или аутентификация;

− мониторинг пользователей, находящихся в режиме online;

− преобразование кадров GSM в форматы, используемые протоколами TCP/IP глобальной компьютерной сети Internet;

− регистрация абонентов, вновь «появившихся» в зоне действия сети;

− шифрование данных в соответствии с алгоритмом шифрования в технологии GPRS;

− сбор поступающей биллинговой информации, т.е. информации об использовании телекоммуникационных услуг, их тарификации, выставлении счетов абонентам и т.д.

В свою очередь, GGSN (англ. GPRS GatewayServiceNode) – это узел, входящий в состав GPRS CoreNetwork и обеспечивающий маршрутизацию данных между GPRS Corenetwork (GTP) и внешними IP-сетями. Помимо маршрутизации, GGSN обеспечивает запросы на аутентификацию к RADIUS-серверу, а также взаимодействие с DNS-серверами для определения IP-адреса, запрошенного пользователем. Основной функцией GGSN является роуминг (маршрутизация) данных, идущих к абоненту и от него через SGSN.

Функциями GGSN являются:

- адресация данных;
- динамическая выдача IP-адресов;
- отслеживание информации о внешних сетях и собственных абонентах;
- хранение маршрутизирующей базы данных, базы данных с адресами и фильтрующей базы данных основной сети после введения LTE-сети, что необходимо для поддержки функций, выполняемых MME (англ. MobilityManagementEntity – узел управления мобильностью) и SAE-GW (SGW) (англ. ServingGateway – обслуживающий шлюз) [2].

Одним из вариантов сетевого решения рассматриваемой интеграции является сохранение в так называемых независимых сетях 2G/3G доступа существующих элементов основной сети – SGSN и GGSN, а также включение новых устройств, таких как MME, SAE-GW (SGW), которые с учетом передачи межсистемных функций поддерживают LTE-доступ (рис. 1).

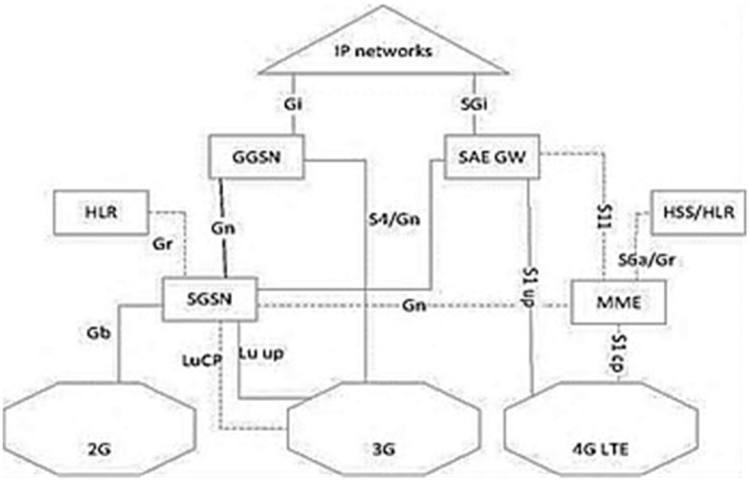


Рис. 1. Независимые сети

MME (англ. MobilityManagementEntity – узел управления мобильностью) – это ключевой контролирующий модуль для сети доступа LTE. Он отвечает за процедуры обеспечения мобильности, хэндовера, слежения и пейджинга UE (англ. UserEquipment – пользовательское устройство), а также участвует в процессах активации/дезактивации сетевых ресурсов.

SAE-GW (SGW) (англ. ServingGateway – обслуживающий шлюз) предназначен для обработки и маршрутизации пакетных данных, поступающих из/в подсистему базовых станций. SGW маршрутизирует и направляет пакеты с пользовательскими данными, в то же время выполняя роль узла управления мобильностью (англ. mobilityanchor) для пользовательских данных между базовыми станциями, также являясь узлом управления мобильностью между сетью LTE и сетями с другими технологиями (см. рис. 1).

Регистр местоположения абонента HLR/HSS (англ. HomeLocationRegister/HomeSubscriberServer), который является расширением HLR, включает в себя всю административную информацию по каждому абоненту, зарегистрированному в этой сети, информацию о разрешенных услугах и информацию о текущем местоположении мобильной станции в форме адреса сигнализации текущего гостевого регистра местоположения VLR (англ. VisitorLocationRegister).

Преимущества внедрения независимых (интегрированных) сетей:

− LTE-сеть является сетью вторичного развертывания и планирования, что служит фактором, исключающим негативное влияние существующей сети (2G/3G);

− внедрение LTE-сети не снижает качества услуги 2G/3G.

Недостатком внедрения независимых (интегрированных) сетей является:

− низкая эффективность передачи между 2G/3G и LTE;

− увеличение оборудования ядра сети;

− увеличение эксплуатационных расходов.

Вторым вариантом сетевого решения является создание так называемых независимых 2G-сетей в результате отделения старых узлов SGSN и GGSN для поддержания 2G-сети и подключения MME и SAE-GW/PGW для 3G/LTE (рис. 2).

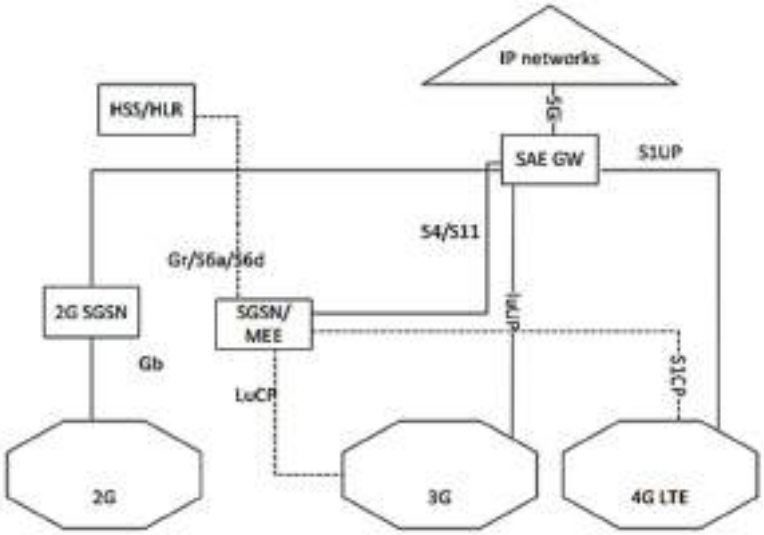


Рис. 2. Независимые 2G-сети

Преимуществом внедрения независимых 2G-сетей является постепенное снижение сетевого тарифа 2G.

Недостатками их внедрения являются:

− необходимость дополнительных подключений для дальнейшего отделения 2G от существующих смешанных 2G/3G-сетей;

− увеличение затрат на техническое обслуживание.

Итак, первоочередной задачей при создании сетей LTE в городах и густонаселенных районах является наличие условий, необходимых для поддержания взаимодействия сетей LTE с существующими сетями 2G/3G. На конечном этапе построения сетей LTE, при увеличении числа пользователей сетями LTE, происходит полное обновление всех сетей при поддержке MME функции MME/SGSN. Постепенная интеграция сетей 3G и LTE устранит 2G-сеть, поэтому для конечного этапа построения сетей LTE можно использовать второй вариант сетевых решений.

Список литературы

1. Lecuyer P., Thierry L. Evolved Packet System (EPS): the LTE and SAE Evolution of 3G UMTS, IohnWiley&Sons, 2008.

2. LTE-технология, сети LTE [Электронный ресурс]. – URL: http://www.yota-system.ru/info/333/ (дата обращения: 10.10.2012).

3. 3GGP TS 32.299 V8.7.0 2009-06 3rd Generation Partnership Project: Technical Specification: Telecommunication management: Charging management: Diameter charging applications [Electronic resourse] // 3GPP TS 21.101 V8.1.0 (2009-06) (Release 8). – URL: www.quintillion.co.jp/3GPP/.../21101-810.

УДК 621.372

А.Е. Севрюков, М.Г. Жидких

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ РАДИОРЕЛЕЙНЫХ ЛИНИЙ В НОВЫХ ЧАСТОТНЫХ ДИАПАЗОНАХ 60-80 ГГЦ

Проведено изучение состояния оборудования РРЛ в новых диапазонах и показано, что эта аппаратура позволяет решать в городах проблему подачи интернет-трафика с гигабитными скоростями на базовые станции.

Интенсивное развитие новых технологий в сетях широкополосного беспроводного доступа (ШБД), в частности в сетях LTE, требует подачи на базовые станции потоков со скоростями до 500 Мбит/с. Существующие РРЛ диапазонов 6-38 ГГц ограничены полосой ствола 28 или 56 МГц и не позволяют достичь требуемых скоростей даже с модуляцией QAM высокой кратности. Эти факторы требуют перехода на более высокие свободные частотные диапазоны 60-80 ГГц. В данных диапазонах регламентирующие органы выделили более широкие радиоканалы (с полосой частот до 1000 МГц), что позволяет значительно увеличить скорость передачи информации.

Первым фактором, вызвавшим стремительный интерес к новым частотам, является перегрузка традиционных диапазонов. Как показывает практика, полосу частот шириной 56 МГц в диапазонах 18, 23, 38 ГГц (именно для этих диапазонов выпускают оборудование передовые производители) в городах получить затруднительно. Лучшие компании предлагают для РРЛ в данных диапазонах уровень модуляции не выше 256 QAM [2], что определяет коэффициент эффективности использования частотного спектра в канале передачи $\gamma = 6,4$. $\gamma = C / B$ – это отношение скорости передачи канала С (бит/с) к полосе радиочастот В (Гц). Следовательно, через полосу 56 МГц можно в РРЛ максимально пропустить около 360 Мбит/с. Современный уровень аппаратуры [3] позволяет передать с помощью одной базовой станции LTE, при выделенной полосе канала 20 МГц, следующие скорости передачи информации с учетом параметров оборудования, приведенных в таблице 1.

Таблица 1

Скорости передачи информации в стандарте LTE с учетом параметров оборудования

Тип модуляции	QPSK	16QAM	64QAM	64QAM	64QAM
Вид MIMO	нет	нет	нет	2x2	4x4
Скорость	20.8	57,6	86,4	172,8	345,6

Это означает, что всего лишь для одной базовой станции, излучающей по трем секторам, необходим тракт подачи информации со скоростью около 1 Гбит/с (345,6x3 Мбит/с), что почти в три раза больше, чем может передать традиционная РРЛ. Следовательно, поиск новых решений для РРЛ является требованием времени.

Вторым фактором ускорения работ в новых диапазонах является уменьшение дальности пролетов радиорелейных линий. Третьим фактором, вызвавшим ускорение перехода в новые диапазоны, являются законодательные решения последних лет, на основе которых выделяются более широкие радиоканалы (до 1000 МГц), что позволяет значительно увеличить скорость передачи информации в РРЛ (до 4 Гбит/с). Таким конкретным документом является решение Государственной комиссии по радиочастотам (ГКРЧ) об упрощении процедуры выделения полос радиочастот 71-76 ГГц и 81- 86 ГГц для использования радиорелейными станциями прямой видимости [4]. Практически упрощается выделение частот также в диапазоне 60-66 ГГц.

Затухание сигнала зависит от геоклиматических параметров региона и, самое главное, от диапазона частот, в котором работает станция. Один из таких графиков зависимости затухания радиорелейного сигнала в воздухе от частоты, построенный на основе данных [5], приведен на рисунке 1.

Из графика следует, что с ростом частоты увеличивается затухание радиосигнала в воздухе, особенно в каплях воды или снега. Максимум затухания достигается в диапазоне 60 ГГц и составляет 16 дБ/км. Это связано с физическими явлениями — поглощением сигнала в молекулах кислорода. Далее затухание уменьшается до значений 0,5 дБ/км на частотах 70-80 ГГц.

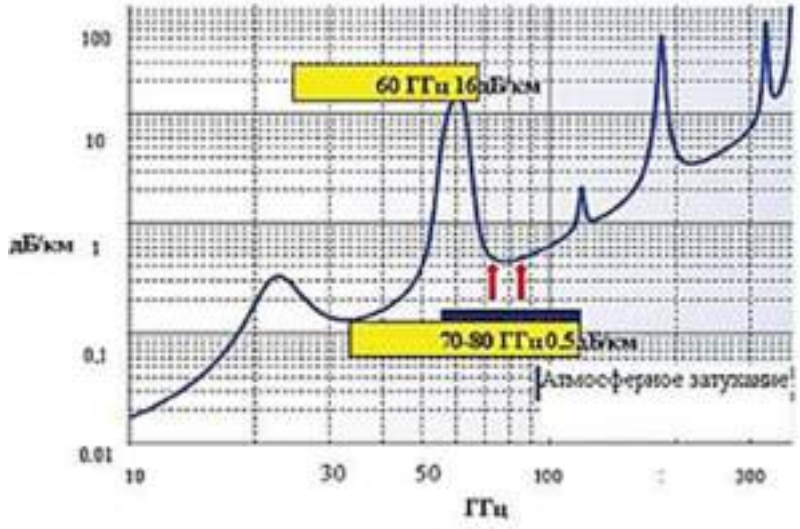


Рис. 1. График зависимости километрического затухания от частоты

Радиорелейные линии в диапазоне 80 ГГц (71-76 ГГц – нижний диапазон и 81-86 ГГц – верхний диапазон) за счет меньшего затухания в молекулах кислорода и воды позволяют передавать большие скорости на большие расстояния. Используя радиоканал шириной 1000 МГц и изменяемую в зависимости от погодных условий модуляцию BPSK-QPSK-16QAM, можно достичь скорости до 2,4 Гбит/с на приемопередатчик на расстоянии до 3-5 км. В пакетных РРЛ учитывается нагрузка и с применением адаптивной модуляции можно передавать более значительные скорости.

При проектировании линий необходимо пользоваться графиками, которые показывают, как выполняются международные нормы по готовности (availability) для данной конкретной аппаратуры. Такой график показан на рисунке 2 для диапазона 80 ГГц, антенн диаметром 60 см, с условием необходимости передачи информации со скоростью 1250 Мбит/с.

По этим данным можно определить, что для курского погодного региона (это регион Е) безотказная работа для данной РРЛ будет обеспечена с вероятностью 99,995% на длинах пролета до 4,5 км.

Крупными российскими операторами в России и, в частности, в Курске были проведены полевые испытания оборудования 80ГГц. Был построен радиорелейный пролет длиной 2150 м диапазона 80 ГГц с антеннами диаметром 0,6 м. Измеренные значения надежности приведены в таблице 2.

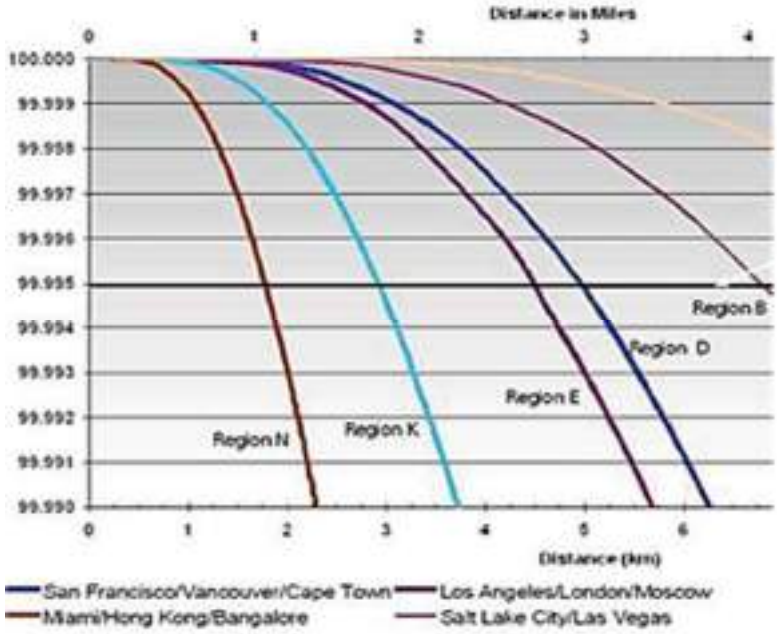


Рис. 2. Показатель готовности для РРЛ в диапазоне 80 ГГц

Таблица 2

Измеренные значения надежности

Интенсивность осадков, мм/ч	Рекомендация	Поляризация	Длина линка, км	Мощность Tx, дБм	Уровень Rx, дБм	Пороговый уровень Rx, дБм	Запас мощности, дБ	Надежность, %
22	ITU-R P.837-1	V	2.14	20	- 16.84	-62.4	45.56	99.99933
26.8	ITUR P.837-5	V	2.14	20	- 16.84	-62.4	45.56	99.99887

В соответствии с данным документом максимальная мощность передатчика не должна превышать 0,15 Вт (+ 21,7 дБМ), чувствительность приемника быть не хуже - 57 дБм, а ширина диаграммы направленности в вертикальной и горизонтальной областях не более 1 град. Следовательно, экспериментальная линия удовлетворяет требованиям ГКРЧ при диаметре антенн 0,6м.

Еще одним типом оборудования являются приемопередатчики в диапазоне 60 ГГц (57-64 ГГц). Данные РРЛ работают на очень коротких дистанциях (до 500-700 м), так как эти линии очень сильно подвержены затуханию в условиях дождя, снега или тумана. Однако, с другой стороны, при расчете таких сетей можно прене-

брегать интерференцией сигналов и организовывать множество высокоскоростных (до 1 Гбит/с) каналов в одном географическом месте. Для Курска, попадающего в зону Е по количеству осадков в год, длина радиорелейного пролета с требуемой гарантированной надежностью 99,995% составляет до 750 м. Обычно в этом диапазоне применяется модуляция QPSK и при специальном кодаке FEC достигается скорость до 1000 Мбит/с на приемопередатчик.

Если взять, например, диапазон 71-76 ГГц, то надо учесть, что здесь можно разместить лишь четыре полноценных радиоканала с полосой 1 ГГц каждый. Следовательно, в одном месте без интерференции могут одновременно работать не более 4-х радиорелейных линий этого диапазона.

Рассмотренные высокочастотные решения в диапазонах 60-80 ГГц обладают своими преимуществами и недостатками. Выбор того или иного диапазона должен быть обусловлен, в первую очередь, возможностями применения оборудования и его экономическими характеристиками. В свою очередь, рекомендуется использовать диапазон 60 ГГц в условиях плотной городской застройки и требования к сохранению архитектурного облика в центральных частях города на арендованных площадях. Диапазон 80 ГГц позволяет достичь больших скоростей передачи данных на большие расстояния, но имеет ряд ограничений по планированию и запуску сети в эксплуатацию.

Список литературы

1. Кирик Ю.М. Тенденции в развитии городской радиорелейной связи // Электросвязь. – 2009. – № 3. – С. 11-13.

2. Журавель С., Шашков А. РРЛ NEC: традиции, качество, надежность // Технологии и средства связи. – 2008. – № 5. – С. 44-45.

3. TD LTE and FD LTE. A basic comparison [Электронный ресурс]. – URL: http://www.ascom.com/ en/tems-fdd-lte-vs-td (дата обращения: 10.11.2012).

4. ФГУП ГРЧЦ (Государственный радиочастотный центр). Решение от 15.07.2010 [Электронный ресурс]. – URL: http://www.grfc.ru/ (дата обращения: 04.04.2014).

УДК 004.75

А.Л. Марухленко, К.В. Кустова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РАЗРАБОТКА РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ ДЛЯ УДАЛЕННОГО КОНТРОЛЯ ДОСТУПА В ЗДАНИИ

Рассмотрен вариант организации распределенной системы видеонаблюдения на удаленном расстоянии на базе здания кафедры защиты информации и системы связи, позволяющей обеспечить удаленный онлайн-просмотр изображений с камер видеонаблюдения и предотвратить несанкционированный доступ в здание.

На сегодняшний день задача контроля доступа к объектам частных фирм, государственных организаций и мест потенциального скопления людей требует повышенного внимания. Это обусловлено необходимостью защиты авторских прав, сохранения материальных ценностей и безопасности жизнедеятельности. Для решения этих задач применяются системы видеонаблюдения. Современные системы видеонаблюдения подразделяются на аналогово-цифровые и сетевые (IP).

Аналогово-цифровые системы видеонаблюдения используются в основном на небольших объектах, где нет необходимости в построении территориально распределенных систем видеонаблюдения. В такой системе видеонаблюдения изображение с аналоговой видеокамеры передается на цифровое устройство, представляющее собой расширительные платы видеозахвата (производители Pinnacle, Orient) или автономные видеорегистраторы (BestDVR, Polivision), в которых происходит оцифровка полученного изображения и при необходимости сохранение его в виде файла. Такая схема организации видеонаблюдения получила широкое распространение благодаря ряду преимуществ: приемлемая стоимость оборудования и монтажа, простота в использовании, возможность интеграции с охранными системами, одновременная запись изображения с нескольких камер на один видеорегистратор, длительная автономная работа, оперативный доступ к любому записанному видеофрагменту. К недостаткам можно отнести: ограничение по удаленности видеокамеры от видеорегистратора, среднее разрешение видеозаписи (обычно не превышающее 720x576 точек).

Сетевые или IP-системы видеонаблюдения используются на больших, территориально-распределенных объектах с применением IP-видеокамер (рис. 1). Использование сетевого видеонаблюдения делает возможным использование практически неограниченного количества видеокамер и позволяет организовывать в единую систему группу территориально распределенных объектов, что невозможно при использовании аналогово-цифровой системы видеонаблюдения.

Рис. 1. Структурная схема IP-видеонаблюдения

Функции, комплектация и стоимость систем видеонаблюдения зависят от предъявляемых требований к системе. Самые простые системы включают в себя несколько аналоговых видеокамер для фиксирования видеоизображения, видеорегистратор для записи на встроенный жесткий диск и монитор для отображения видеоинформации в режиме реального времени. В настоящее время все чаще применяются достижения в технологии IP-видеонаблюдения. Существуют интеллектуальные системы видеонаблюдения, которые могут самостоятельно анализировать видеоданные (распознавать автомобильные номера и лица людей, детектировать пересечение заданной границы, появление постороннего объекта или оставление предмета в области наблюдения) и оповещать пользователя о произошедших событиях по каналам GSM и сети Интернет. Также IP-видеонаблюдение позволяет удаленно вести наблюдение в режиме реального времени и управлять видеокамерами.

В рамках бакалаврской работы на основе здания учебного корпуса ЮЗГУ спроектирован вариант системы видеонаблюдения,

который способен зафиксировать факт несанкционированного доступа в здание и совершение других противоправных действий.

Техническая реализация системы представляет использование 10 видеокамер (4 уличных IP-камеры и 6 внутренних аналоговых купольных камер), гибридного видеорегистратора, двух мониторов (рис. 2). Для аварийного питания системы видеонаблюдения предусмотрен блок источника резервного питания (БИРП).

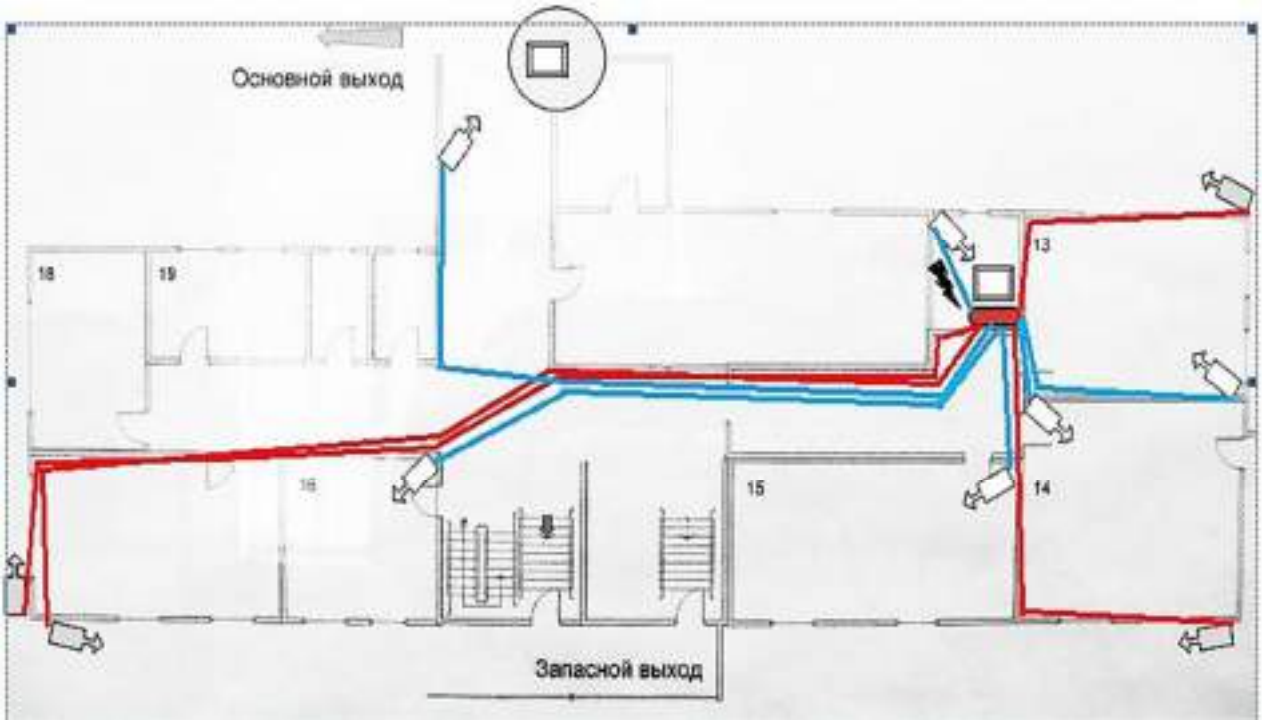


Рис. 2. Структурная схема разрабатываемой системы видеонаблюдения:

– уличная видеокамера; – видеомонитор; – внутренняя видеокамера; – пост охраны; – видеорегистратор; – БИРП; – маршрутизатор; – коаксиальный кабель; – витая пара

В качестве уличной видеокамеры была выбрана IP-камера Polyvision PN2-M2-V12IR-IP в связи с лучшими техническими характеристиками по сравнению с аналоговыми. Данная камера выполнена в профессиональном гермокожухе с удобным кронштейном и мощной ИК-подсветкой.

Технические параметры:

- высокочувствительная матрица 1/2.8" Sony Exmor CMOS;
- вариофокальный мегапиксельный объектив 2.8-12 мм;

− автоматическая функция День/Ночь – механический ИК-фильтр;

− дальность ИК-подсветки до 40 метров;

− разрешение 1080p, 720p, D1 со скоростью 25 к/с;

− поддержка протокола RTSP (возможность транслировать видеопоток на сайте);

− удалённый доступ через web-интерфейс и CMS;

− антивандальное исполнение;

– широкий диапазон температур эксплуатации -40...+55°С (цена данной видеокамеры около 10 000 рублей).

В здании кафедры будут установлены купольные видеокамеры Novicam серии 87, которые обладают матрицей 1/3" SONY с разрешением 700ТВ линий и чувствительностью 0,01 люкс. Камеру в корпусе возможно вращать для лёгкой установки на вертикальную, горизонтальную или наклонную поверхность, что даёт возможность изменять направление обзора камеры после монтажа. На выбор могут использоваться объективы 2.8 мм или 3.6 мм в зависимости от необходимого угла обзора (цена камеры примерно 3500 рублей).

Для видеозаписи будет использоваться гибридный 16-канальный видеорегистратор Polyvision PVDR-16WDS2, который позволяет работать в гибридном режиме, т.е. поддерживает подключение как аналоговых, так и IP-камер. Обычные видеорегистраторы не позволяют записывать видеосигнал с разрешением выше 540 ТВЛ. В отличие от них выбранный видеорегистратор поддерживает запись с разрешением 960x576 пикселей. Для интеграции с охранной сигнализацией регистратор имеет 4 тревожных входа, а удаленный доступ возможен через Web-интерфейс или с мобильных устройств Android и iOS. Поддерживаются два жестких диска по 2 Тб. Возможна архивация на USB-носителе и по сети (цена видеорегистратора около 12000 рублей).

Видеорегистратор и БИРП будут установлены в отдельном техническом помещении с ограниченным доступом.

Установленные видеокамеры будут подключены к видеорегистратору: уличные – по витой паре; внутренние – по коаксиальному кабелю. Для видеонаблюдения и оперативного реагирования на

посту охраны будет установлен монитор, отображающий видео со всех видеокамер. Видеозапись будет производиться «по расписанию» в вечернее и ночное время, а также «по детекции движения» или в случае срабатывания охранной сигнализации.

Общая стоимость спроектированной системы видеонаблюдения (включая стоимость БИРП, аккумуляторов и кабелей) составляет около 90000 рублей без самого монтажа.

Представленный вариант системы видеонаблюдения не является бюджетным. При необходимости сокращения затрат возможно использовать только аналоговые видеокамеры и цифровой видеорегистратор с более низкими техническими параметрами.

---

1. Кругль Герман. Профессиональное видеонаблюдение // Практика и технологии аналогового и цифрового CCTV. Германия, 2010.

2. Рембовский А.М., Ашихмин А.В. Радиомониторинг: задачи, методы, средства. – Изд. 2-е. – М.: Горячая линия-Телеком, 2010. – 624 с.

УДК 004.77

А.В. Ляпунов, А.А. Гуламов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СИСТЕМА ДИСТАНЦИОННОГО МОНИТОРИНГА СОСТОЯНИЯ ЗДОРОВЬЯ ПАЦИЕНТОВ И ПЕРСПЕКТИВЫ ЕЁ РАЗВИТИЯ

Рассмотрена система дистанционного мониторинга состояния здоровья больного в свете процесса персонализации медицины.

В настоящее время в медицине нарастают тенденции к персонализации. Эти тенденции являются следствием развития науки и роста уровня жизни. Первым их отражением является появление компактных приборов медицинской диагностики, расширение их возможностей и повышение точности. Вторым отражением становится комплексных подход к медицинской диагностике заболеваний и их лечению, который позволяет рассматривать организм как совокупность систем и применять более эффективные методы лечения, сводя их негативные эффекты к минимуму.

Персонализация медицины позволяет пациентам после первичного стационарного обследования и установления важных осо-

бенностей и основных предрасположенностей организма в большинстве случаев проводить дальнейшее обследование и текущий контроль необходимых показателей здоровья вне стационарных условий. Оперативный контроль, анализ этих данных и принятие своевременных решений специалистами требуют создания системы дистанционного мониторинга состояния здоровья пациентов. Кроме того, система должна обеспечивать доведение информации до пациента о коррекции лечения, посещении врача, проведении дополнительных исследований и неотложных мероприятий в стационарных условиях, избавляя пациента от неудобств стояния в очередях. Функционально систему дистанционного мониторинга состояния здоровья можно разделить на три основных компонента.

Первый компонент – это пациент с персональными устройствами медицинской диагностики и средствами связи. Он должен регулярно снимать все необходимые для проведения мониторинга состояния его здоровья показания диагностических устройств и пересылать их в диагностический центр.

Второй компонент – это медицинский диагностический центр. Здесь хранятся электронные медицинские карты пациентов и производится сбор, обработка и хранение в общей базе данных информации о пациентах и текущих результатах диагностики.

Третий компонент – это обследующие и/или лечащие врачи, оснащенные устройствами связи и соответствующим ПО для связи с пациентами и диагностическим центром, а также работы по результатам медицинской диагностики пациентов.

Связь между компонентами может осуществляться по двум основным путям в зависимости от наличия соответствующего телекоммуникационного оборудования и возможностей у пациента.

Первый предусматривает использование Интернета и предоставляет практически неограниченные возможности для передачи результатов диагностики от пациента в диагностический центр и обратной связи с пациентом. В этом случае пациент может быть оснащён любыми устройствами медицинской диагностики.

Использование первого пути требует наличия устройств с полноценными ОС и возможностью подключения к Интернету, а также наличия самого подключения к сети.

Второй путь основан на передаче результатов медицинской диагностики при помощи SMS-сообщений. В этом случае от пациента требуется лишь наличие мобильного телефона и нахождение в зоне действия сети сотовой связи. От диагностического центра при этом требуется наличие SMS-шлюза и ПО для работы с ним.

Необходимость использования второго пути наравне с первым обусловлена широким покрытием территории страны сетями сотовой связи и наличием у абсолютного большинства людей соответствующих устройств для связи посредством этих сетей, а также отсутствием доступа в Интернет у многих людей, что особенно актуально для пожилых людей и для жителей удалённых сельских районов. Использование сотовых сетей также предоставляет пользователям большую мобильность. Но при наличии возможностей должен использоваться первый путь, т.к. посредством SMS может быть передан только ограниченный объем данных в текстовом формате, что делает невозможным полное раскрытие функциональных возможностей многих устройств медицинской диагностики и использование других возможностей для связи между врачом и пациентом, которые предоставляет Интернет.

Основой данной системы является база данных, представляющая собой набор универсальных медицинских карт с информацией о каждом проходящем обследование пациенте.

При поступлении пациента в медицинский диагностический центр производится необходимое его обследование, результаты которого вносятся в базу данных диагностического центра вместе с результатами предыдущих медосмотров, а также результатами применения медицинских препаратов и иных методов лечения болезней и купирования их обострений. На основании этих обширных данных врач, проводящий медицинскую диагностику пациента, формирует первичный состав индивидуального диагностического оборудования, который может в дальнейшем изменяться по его усмотрению.

Важным свойством системы медицинской диагностики состояния здоровья является её расширяемость. Это означает, что состав диагностического оборудования может меняться по необходимости

и вследствие появления новых диагностических устройств при дальнейшем развитии телемедицины.

Одной из важных частей системы является опросная форма, содержащая в себе вопросы, касающиеся самочувствия пациента. Короткий её вариант может реализовываться также посредством отправки SMS-сообщений, полноценный же будет доступен для заполнения на веб-сайте.

Текущие результаты медицинской диагностики вносятся в базу данных в числовом и графическом формате. Туда же вносятся жалобы пациента, полученные через опросник и при общении с врачом, промежуточные заключения врача и его комментарии.

Большую часть времени система работает в автоматическом режиме, а специалисты диагностического центра и врачи вмешиваются в её работу по необходимости.

Специалисты диагностического центра постоянно следят за текущими результатами медицинской диагностики и общим состоянием здоровья пациента. При возникновении опасности они могут связаться с врачом или вызвать бригаду скорой помощи.

Врачи посредством сотовой связи или Интернета могут проводить консультации, а также онлайн-приёмы (при наличии вебкамеры). Выводы, полученные в результате таких консультаций и приёмов, а также в результате наблюдений и оценки текущих показателей состояния здоровья пациента, отмечаются в электронной карте больного. На основании этих выводов врач может изменить состав диагностического оборудования с соответствующими отметками в медицинской карте пациента.

Обобщённая архитектура сети описанной системы изображена на рисунке.

Комплексный подход требует наличия самых обширных данных о пациенте и внесения их в единую медицинскую карту больного. Важную роль в таком подходе может играть так называемая предсказательная медицина (predictivemedicine). Этот раздел медицины призван заранее определять риски развития тех или иных заболеваний. Центральное место в предсказательной медицине принадлежит исследованию генома человека.

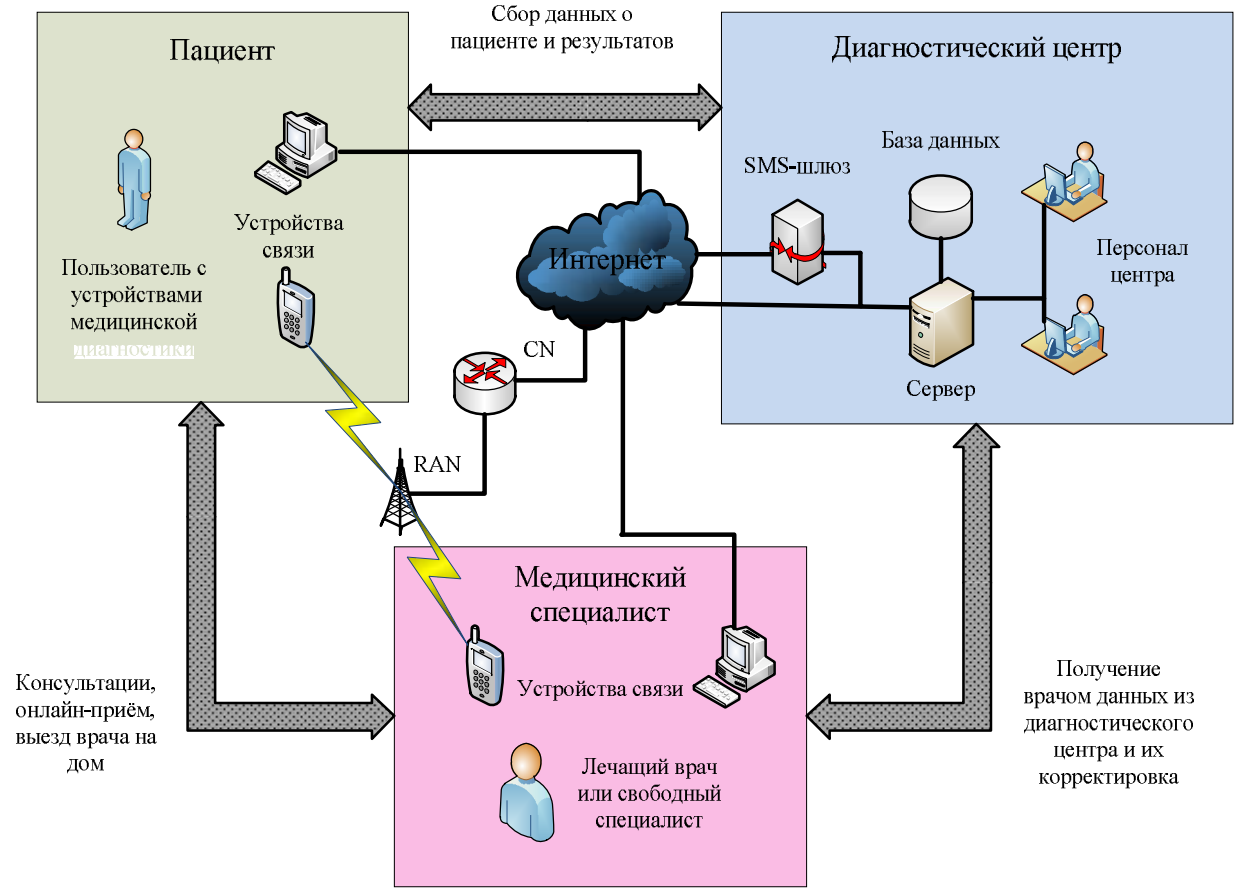


Рис. Обобщённая архитектура сети

Исследования в области генетики позволили установить генетически обусловленные предрасположенности к широкому ряду болезней, а при дальнейших исследованиях будут выявляться всё новые предрасположенности к различным заболеваниям. Это предоставляет новые возможности для профилактики болезней и их обострений. В частности, стало возможным создание генетического паспорта пациента, который представляет собой базу ДНК-данных этого пациента, где отражаются все его индивидуальные особенности, связанные с генетикой – данные о наследственных и мультифакторных заболеваниях и иных особенностях организма [1].

Такой паспорт позволит заранее определить основные предрасположенности организма и связанные с ними риски, что поможет определить показатели здоровья, за которыми необходимо следить, и сформировать первичный состав диагностического оборудования для их мониторинга.

Применение генетического паспорта поможет оптимизировать систему дистанционного мониторинга состояния больного

уже на начальном этапе организации диагностики состояния здоровья пациента, а также сэкономит время и ресурсы и ощутимо повысит эффективность как самого мониторинга, так и оказания необходимой медицинской помощи пациенту.

В случае полной реализации системы дистанционного мониторинга состояния здоровья пациента, она сможет на ранних стадиях эффективно диагностировать множество болезней, к которым у пациентов есть предрасположенности, и проводить мониторинг состояния здоровья при их лечении, что, в свою очередь, поможет максимально точно оценивать эффективность применения тех или иных методик лечения. Также данная система поможет оперативно выявлять наступление кризисных ситуаций и применять меры для стабилизации состояния здоровья пациента, что может спасти жизни немалому количеству людей.

Помимо всего этого, система даст возможность врачам лучше распределять своё рабочее время, а также предоставит им возможность выполнять значительную часть своих обязанностей, не выходя из дома.

Всё это поможет людям дольше жить полноценной жизнью, сводя накладываемые болезнями ограничения к минимуму, и значительно повысит свободу перемещений как самих больных, так и врачей.

---

1. Персонализированная медицина: перспективы использования нанобиотехнологий [Электронный ресурс]. – URL: http://www.umj.com.ua/article/10408/personalizirovannaya-medicina-perspektivy-ispolzovaniya-nanobiotexnologij.

УДК 004.7

Е.С. Маклаков, А.А. Гуламов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ FTTH В СОВРЕМЕННЫХ ГОРОДСКИХ СЕТЯХ ДОСТУПА

Рассмотрен принцип применения технологии FTTH в частном секторе городских сетей доступа. Анализируются стандарты, которые предоставляют организацию сети по технологии FTTH.

В последние годы сети доступа являются наиболее динамичным сегментом телекоммуникационной отрасли. Они непосредственно связаны с предоставлением операторских услуг абонентам, поэтому сети доступа хорошо окупаются даже в условиях неблагоприятной экономической ситуации. Ежегодно растет интерес к развертыванию сетей доступа с возможностью предоставления абоненту широкополосного канала связи. Причиной данного интереса служит быстрый рост требований к полосе пропускания сетей связи, обусловленный появлением новых широкополосных услуг. Используемые в настоящее время технологии не могут в достаточной мере удовлетворить потребности населения частного сектора города, в связи с этим все более актуальным и экономически целесообразным является применение новых технологий широкополосного доступа, одной из которых является технология FTTx на базе технологии PON.

Архитектура построения сетей оптического доступа характеризуется степенью приближения оптического сетевого терминала к пользователю. Сектор стандартизации ITU-T выделяет несколько характерных вариантов.

Как видно из рисунка 1, все архитектуры FTTx предполагают наличие участка с распределительными медными кабелями, но чем он короче, тем больше пропускная способность сети. Максимальное использование оптических технологий предполагает структура FTTH, при которой оптический сетевой терминал находится в квартире пользователя и соединяется короткими соединительными кабелями с оконечными устройствами.

Выбор архитектуры зависит от множества условий и, в первую очередь, от плотности размещения абонентов. Но ориентировочно можно высказаться за применение системы FTTB для многоэтажных жилых зданий. Для частной застройки или офисов более целесообразным будет применение FTTH.

Существует два типа организации FTTH сетей: на базе Ethernet и на базе PON.

В решении Ethernet FTTH для коммутации линий подразумевается использование коммутаторов с оптическими портами или оптическими трансиверами. Коммутаторы объединяются либо в «кольцо» Ethernet (GE или 10GE), либо по топологии «звезда» и

располагаются на цокольном или чердачном этаже. К портам коммутатора подключаются устройства конечных пользователей. Такой подход обеспечивает высокий уровень надежности за счет возможности резервирования оптических каналов и обеспечивает преемственность с существующей «медной» инфраструктурой. К недостаткам Ethernet FTTH можно отнести узкую полосу пропускания и недостаточные возможности масштабирования [1].

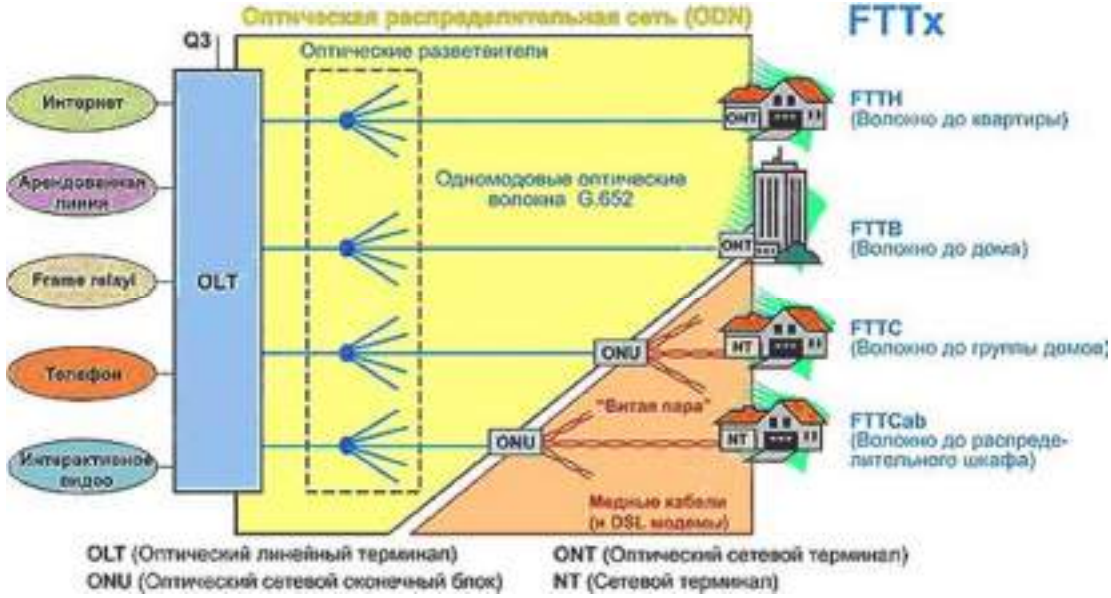


Рис. 1. Архитектуры построения оптических сетей доступа

При использовании решения на базе PON – пассивной оптической сети – для развертывания сети FTTH оптоволоконная линия распределяется по абонентам с помощью пассивных оптических разветвителей (сплиттеров) с коэффициентом деления от 1:2 до 1:128.

ONT представляет из себя более сложное устройство, чем CPE, используемое в Ethernet-решении.

Архитектура FTTH на базе PON поддерживает различные протоколы передачи данных, одним из которых является Ethernet. В некоторых случаях используется дополнительная длина волны нисходящего потока, что позволяет предоставлять традиционные аналоговые и цифровые телевизионные услуги пользователям без применения телевизионных приставок с поддержкой IP.

На рисунке 2 изображена типичная пассивная оптическая сеть PON, в которой используются различные терминаторы оптической

сети (opticalnetworktermination, ONT) или устройства оптической сети (opticalnetworkunit, ONU). ONT предназначены для использования отдельным конечным пользователем. Устройства ONU обычно располагаются на цокольных этажах или в подвальных помещениях и совместно используются группой пользователей. Голосовые сервисы, а также услуги передачи данных и видео доводятся от ONU или ONT до абонента по кабелям, проложенным в помещении абонента.

Для больших операторов, строящих большие разветвленные сети с системами резервирования, наиболее удачной считается технология GPON, которая наследует линейку APON – BPON, но с более высокой скоростью передачи – 1244 Мбит/с и 2488 Мбит/с (в асимметричном режиме) и 1244 Мбит/с (в симметричном режиме).

Оптические сети доступа на основе технологии G-PON могут иметь различные способы резервирования:

– резервирование волокон, по которым осуществляется передача оптического сигнала;

– использование второго блока OLT в качестве резервного плюс использование резервного волокна в направлении от OLT к разветвителю;

– полное дублирование блоков OLT и ONU на передающей и принимающей сторонах.

Наличие в PON-сетях достаточно хорошей системы резервирования говорит о том, что они не уступают сетям Ethernet, которые очень активно применяются в настоящее время.

Передача данных осуществляется по протоколу SDH со всеми вытекающими преимуществами и недостатками. Предполагается подключение до 32-х абонентов на расстоянии до 20 км (с возможностью расширения до 60 км). GPON поддерживает как трафик ATM, так и IP, речь и видео, а также SDH. Сеть работает в синхронном режиме с постоянной длительностью кадра. Линейный код NRZ со скремблированием обеспечивают высокую эффективность полосы пропускания. Единственным серьезным недостатком GPON является относительно высокая стоимость оборудования [2].

Сравнительная таблица по характеристикам различных видов PON представлена в стандарте ITU-T G.983.

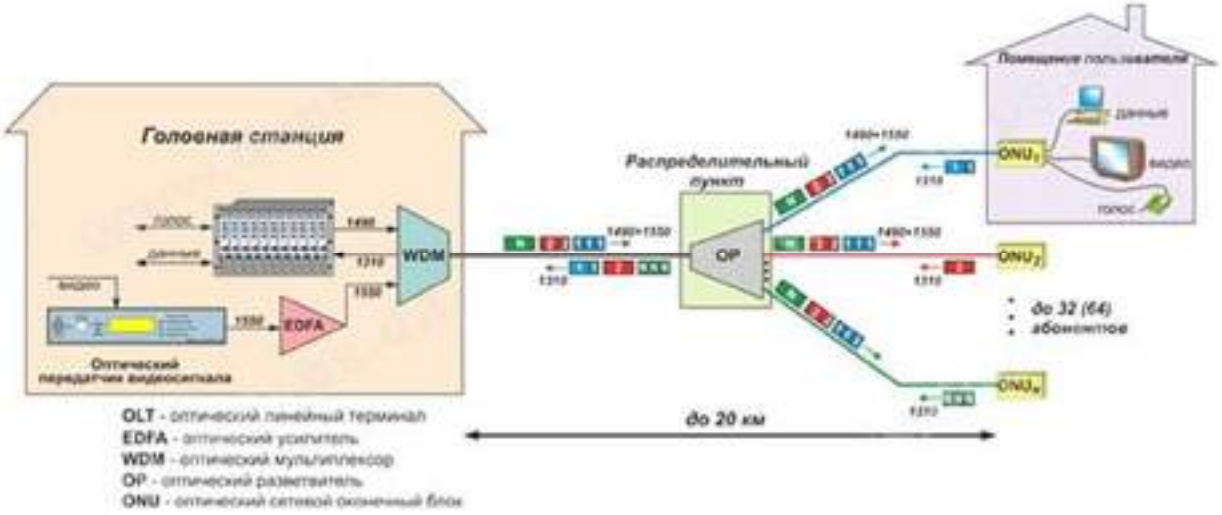


Рис. 2. Архитектура PON

Сети FTTH с использованием технологии PON – наиболее перспективный вариант систем абонентского доступа, поскольку представляет собой эффективный способ обеспечения передачи информации. Архитектура PON обладает необходимой гибкостью наращивания узлов сети FTTH и пропускной способностью. Современные требования по скорости доступа FTTH – минимум 100 Мбит/с на абонента сети PON. Если закладываемые сегодня технические решения не способны обеспечить такие показатели, то моральное устаревание оборудования произойдет до окончания инвестиционного цикла.

---

1. Яременко Ю.И. Теоретические основы построения и применения средств связи оптического диапазона. – СПб.: ВАС, 1992. – 300 с.

2. Битнер В.И., Михайлова Ц.Ц. Сети нового поколения NGN. – М., 2011. – 121 с.

УДК 004.75

А.Л. Марухленко, А.С. Сидельникова, Е.И. Шевцов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВАРИАНТ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ МОНИТОРИНГА ЖИЗНЕННОГО ЦИКЛА ОБЪЕКТОВ СЕЛЬСКОХОЗЯЙСТВЕННОЙ ПРОМЫШЛЕННОСТИ

Рассмотрен вариант организации распределенной системы фитомониторинга.

На сегодняшний день успешное развитие регионов Российской Федерации определяется качеством и количеством произведенной продукции. Это напрямую связано с наличием природных ресурсов, квалифицированного персонала и уровнем материальной базы. Анализ состояния объектов сельскохозяйственной промышленности показал неэффективное использование результатов научно-технических средств, обеспечивающих автоматизированный режим контроля и поддержания жизненного цикла растений. Применение подобных систем позволит повысить урожайность и создаст условия для выведения новых видов и сортов сельскохозяйственных культур в масштабах тепличного комплекса.

Современное тепличный комплекс – это сложный технологический объект, состоящий из блоков, включающих в себя совокупность территориально распределенных теплиц. Основная задача заключается в оптимальном поддержании микроклимата (температура, влажность, концентрация углекислого газа, свет и.т.д.) в автоматизированном режиме. Для решения этой цели современные тепличные комплексы оборудуются необходимой аппаратурой:

– системой мониторинга параметров полива (план полива, концентрация и кислотность раствора);

– системой мониторинга микроклимата;

– системой мониторинга физиологических процессов растения (сокодвижения, температуры листьев, динамики набора массы растения, роста плода);

– системой управления.

Типовой вариант построения автоматизированной системы фитомониторинга показан на рис.1. Здесь в состав автоматизированного комплекса входят:

– датчик влажности воздуха и температуры;

– датчик освещенности, который отслеживает уровень освещения в тепличном помещение и автоматически включает или выключает свет при достижении определенной степени освещенности;

– датчик влажности почвы, который располагается в грунте и предназначен для измерения реального уровня содержания влаги. Используется в системе автоматического полива;

– датчик уровня углекислого газа, который контролирует уровень его концентрации в теплице (недостаток углекислого газа негативно влияет на рост растения);

– управляющий микроконтроллер, который получает информацию от системы датчиков, обрабатывает ее, а также управляет оборудованием АСУ. Для передачи управляющих сигналов на исполнительные механизмы используется отдельный блок релейной коммутации. В качестве управляющего устройства может быть выбран микроконтроллерный блок Arduino. Одним из его преимуществ является простота языка программирования. Пример текста программы для подключения датчика температуры и влажности представлен на рис.2;

– диспетчерский компьютер теплицы. Программное обеспечение диспетчерского компьютера позволяет архивировать и графически отображать в реальном времени все заданные и измеренные параметры микроклимата, а также рассчитанные в соответствии с заданным алгоритмом управляющие воздействия.

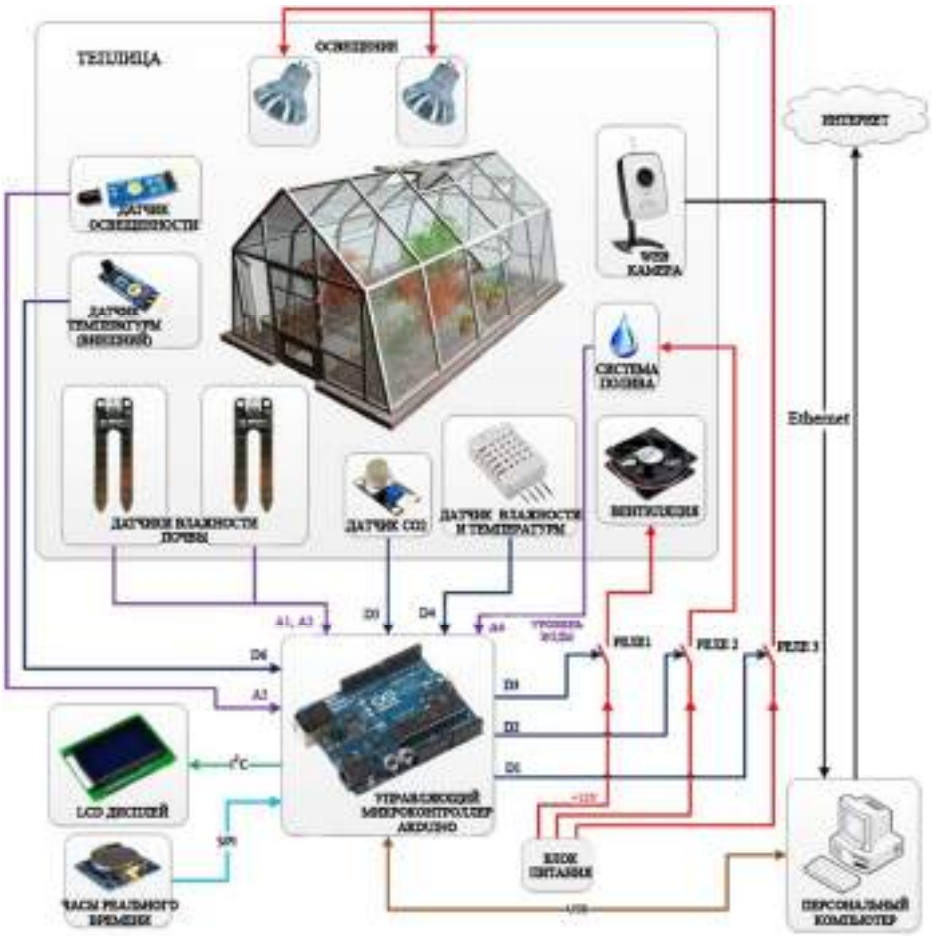


Рис. 1. Командная архитектура автоматизированного комплекса по выращиванию культур

```
#include "DHT.h"
#define DHTPIN 2
#define DHTTYPE DHT11
DHT dht(DHTPIN, DHTTYPE);
void setup() {
  Serial.begin(9600);
  Serial.println("arduino.ru.com");
  dht.begin();
}
void loop() {
  float h = dht.readHumidity();
  float t = dht.readTemperature();
  if (isnan(t) || isnan(h)) {
    Serial.println("Failed to read from DHT");
  } else {
    Serial.print(h);
    Serial.print(" %\t");
    Serial.print(t);
    Serial.println(" *C");
  }
}
```

Рис. 2. Фрагмент исходного кода для отображения статистики

Основным недостатком подобных систем при выведении новых сортов продукции является отсутствие датчиков роста, диаметра плода и низкий уровень интеграции. Таким образом, целесообразно расширить типовой вариант АСУ. Модифицированная система будет дополнительно содержать:

– датчик роста плода. Кривая роста плода определяется двумя процессами: собственно ростом и водным режимом. В то же время при стрессе возможно замедление роста или даже уменьшение плода. Это может быть результатом дефицита влаги, света или влияния другого лимитирующего фактора. Таким образом, датчики этого типа позволяют оценивать эффекты полива и других воздействий, влияющих на водный баланс и рост плодов;

– датчик диаметра ствола, динамика показаний определяется двумя процессами: ростом и водным балансом. Скорость роста зависит от вида и возраста объекта и экологических условий, а суточная кривая отражает колебания влагосодержания тканей стебля. Для оценки состояния растения используют два параметра кривой: амплитуду полуденного сжатия и суточный прирост.

Для решения проблемы низкой интеграции и неэффективного использования масштабного тепличного комплекса в масштабах корпорации (предприятия) необходима интеграция АСУ в виде локальной вычислительной сети. Для решения задачи установления

доверительного соединения с удаленным пользователем необходимо использование VPN-сервера, который одновременно будет являться интернет-шлюзом (рис.3).

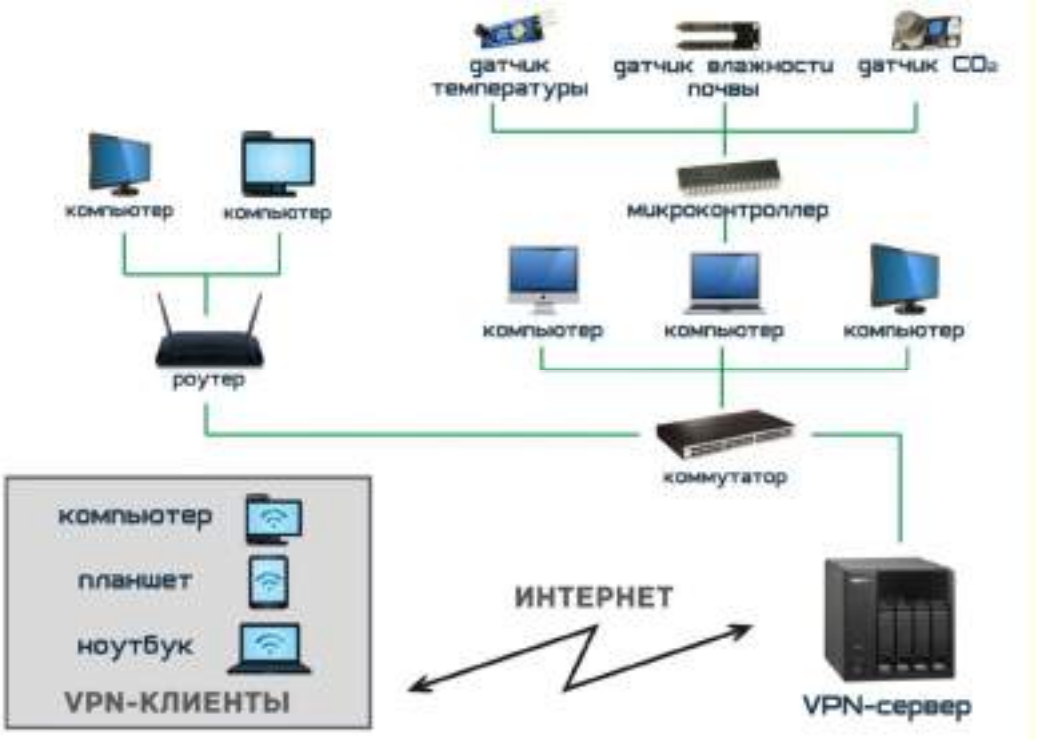


Рис. 3. Вариант построения сети

Здесь АСУ тепличного комплекса являются элементами распределенной сети, взаимодействующими по выделенным каналам связи или через точку доступа. Для получения доступа к системе фитомониторинга удаленный пользователь, имеющий выход в Интернет, устанавливает соединение с VPN-сервером, через который предоставляется возможность оперативного управления АСУ и работой со статистическими данными.

Особенностью предложенного варианта организации автоматизированной системы мониторинга жизненного цикла объектов сельскохозяйственной промышленности является возможность обработки статистики в корпоративных масштабах, а интеграция дополнительного оборудования позволит обеспечить условия для выведения новых сортов продукции.

Список литературы

1. Фрайден Дж. Современные датчики: справочник / под ред. Е.Л. Свинцова. – М.: Техносфера, 2005. – 592 с.

2. Иванов А.И., Куликов А.А., Третьяков Б.С. Контрольно-измерительные приборы в сельском хозяйстве: справочник. – М.: Колос, 1984. – 352с.

3. Максимов Н.В., Попов И.И. Компьютерные сети: учеб. пособие для студентов учреждений среднего профессионального образования. – 3-е изд., испр. и доп. – М.: ФОРУМ, 2008. – 448с.

4. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей: учеб. пособие для вузов. – М.: Горячая линия – Телком, 2003. – 249с.

УДК004.75

Р.В. Трофимова, В.В. Чуйкова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВАРИАНТ ИНФОКОММУНИКАЦИОННОЙ СЕТИ ПРОЕКТНОЙ ОРГАНИЗАЦИИ

Показан вариант локальной сети для ООО «Дельрус-Курск».

Локальная сеть в настоящий момент является неотъемлемой частью любого современного офиса, где нужна оперативность, быстрый и централизованный доступ к различной информации, а также где ценят время и деньги. В то же время локальные сети – сложные структурированные кабельные системы, в составе которых функционирует множество компонентов. Именно поэтому крайне важен квалифицированный подход к проектированию и монтажу локальных сетей.

Основная цель построения сети для ООО «Дельрус-Курск» – обеспечить возможность быстрого обмена информацией между работниками организации, а также высокоскоростной доступ во всемирную сеть Internet через один максимально быстродействующий канал. Результатом использования ЛВС является повышение эффективности работы организации или предприятия. Сети снижают потребность предприятий в других формах передачи информации, таких как телефон или обычная почта.

Первоочередной задачей при построении ЛВС является выбор топологии сети, среды и протокола передачи данных, операционной системы сервера. С помощью этих данных можно значительно повысить скорости и функциональность системы и сократить расходы на её создание и обслуживание. Одной из наиболее ответ-

ственных задач при проектировании сети является выбор сетевого оборудования, так как при этом необходимо обеспечить необходимые характеристики сети и избежать лишних материальных затрат. Типовой проект по построению локальной сети начинается с обследования объекта, которое включает в себя поэтажный план здания, описание кабельных систем, подбор сетевого оборудования.

В таблице перечислены собранная конфигурация сервера, а также сетевое оборудование, необходимое для построения ЛВС ООО «Дельрус-Курск».

Сервер и составляющие ЛВС

Сервер:	
Платформа	SuperMicro 1U 6017R-WRF
Процессор	CPU Intel Xeon E5-2620 V2 2.1 GHz/6core/1.5+15 Mb/80W/7.2 GT/s LGA2011
Оперативная память	2x: DDR3 8 Gb
Жесткие диски	2x: HDD 2 Tb SATA 6Gb / s Western Digital Se <WD2000F9YZ> 3.5" 7200rpm 64Mb
Сетевое оборудование:	
Рабочие станции	40 компьютеров (исходные данные)
Коммутатор	2x: D-Link DGS-1210-28/c1a
Витая пара	UTP категории 5e

Серверная платформа построена на базе материнской платы SuperMicro Super X9DRW-iF, основанной на чипсете Intel C602, поддерживающей установку 1 или 2 процессоров Intel Xeon LGA2011 серии E5-26xx, E5-26xx v2, содержит 16 слотов DIMM для установки модулей памяти 1600/1333/1066/800MHz ECC DDR3 объемом до 512 Гб (для RDIMM), 4 отсека 3,5 дюйма для дисков SATA с возможностью горячей замены. Система оснащена блоком питания 750 Вт. В платформе находится встроенная плата аппаратного управления/мониторинга Renesas SH7757 BMC с поддержкой IPMI (Intelligent Platform Management Interface) v.2.0 и KVM-over-LAN. Встроены два 2-канальных сетевых контроллера Intel i350 10/100/1000 Мбит/с. Имеется выделенный порт управления.

Серверный процессор CPU Intel Xeon E5-2620 V2, частота работы процессора 2.1 ГГц или до 2.6 ГГц в режиме Turbo Boost. Имеет 6 ядер Ivy Bridge-EP. Гнездо процессора Socket LGA2011 Square ILM, Socket LGA2011 Narrow ILM. Частота шины CPU

7200 МГц, рассеиваемая мощность 80 Вт. Официально поддерживаемые стандарты памяти PC3-12800 (DDR3 1600 МГц), PC3-10600 (DDR3 1333 МГц), PC3-8500 (DDR3 1066 МГц), PC3-6400 (DDR3 800 МГц). Максимальный объём оперативной памяти 1536 Гб. Напряжение питания от 0,65 до 1,30 В.

Коммутатор D-Link DGS-1210-28/c1a имеет графический пользовательский интерфейс GUI, протоколом мониторинга компьютерных сетей является RMON, расширение SNMP, разработанное IETF. Протокол сетевого управление – SNMP. Криптографический протокол – SSL. Режим коммутации пакетов с промежуточным хранением (Storeand Forward). Соответствует стандартам 802.1d (Spanning Tree Protocol), 802.1p (CoS), 802.1Q (VLAN), 802.1w (RSTP), 802.1x (User Authentication), 802.3 (Ethernet), 802.3ab (1000Base-T), 802.3ad (LACP), 802.3az (Energy Efficient Ethernet), 802.3u (Fast Ethernet), 802.3x (Flow Control), ANSI/IEEE 802.3 автосогласование. Пропускная способность – 56 Гбит/с.

Выбранная операционная система Windows Server 2008 является надёжной, устойчивой и защищённой средой для обеспечения доступа к файлам, службам печати и сетевым приложениям со стороны клиентских компьютеров.

Методом доступа выбрана технология Gigabit Ethernet со скоростью передачи данных 1000 Мбит/с, описываемая стандартом IEEE 802.3ab (1000Base-T), который является дополнительной главой 802.3. Он основан на том же методе доступа CSMA/CD с сохранением форматов кадров. При этом все соотношения, измеренные в битовых интервалах, сохраняются. 1000Base-T, IEEE 802.3ab использует витую пару категорий 5e. В передаче данных участвуют все 4 пары со скоростью 250 Мбит/с по одной паре. Используется метод кодирования PAM5, частота основной гармоники 62,5 МГц.

На рисунках 1 и 2 показаны схемы оборудования.

В результате работы можно сделать вывод, что при проектировании ЛВС для ООО «Дельрус-Курск» был выбран оптимальный состав оборудования с учетом последующего расширения сети. Основной акцент при выборе кабельной системы сделан на витую пару как наиболее экономичный вид кабеля. Пропускная способность сети 1000 Мбит/с.

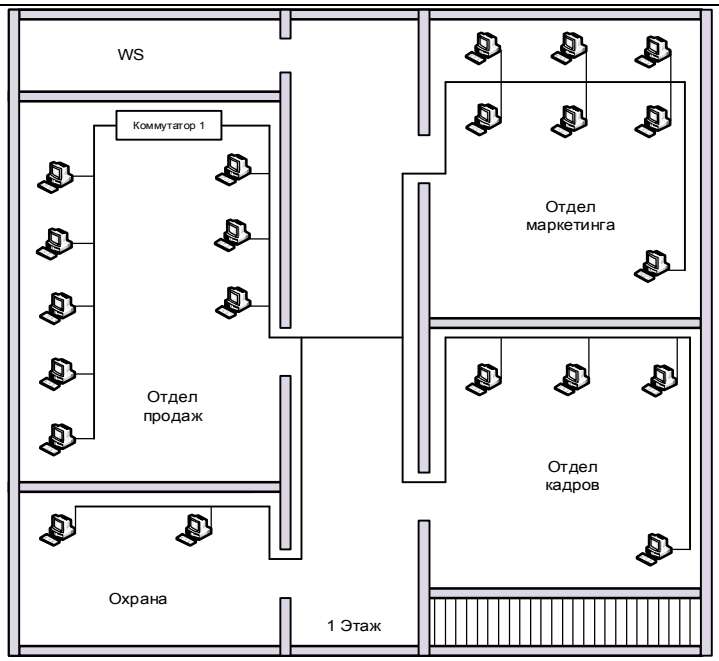


Рис. 1. Схема расположения оборудования на первом этаже

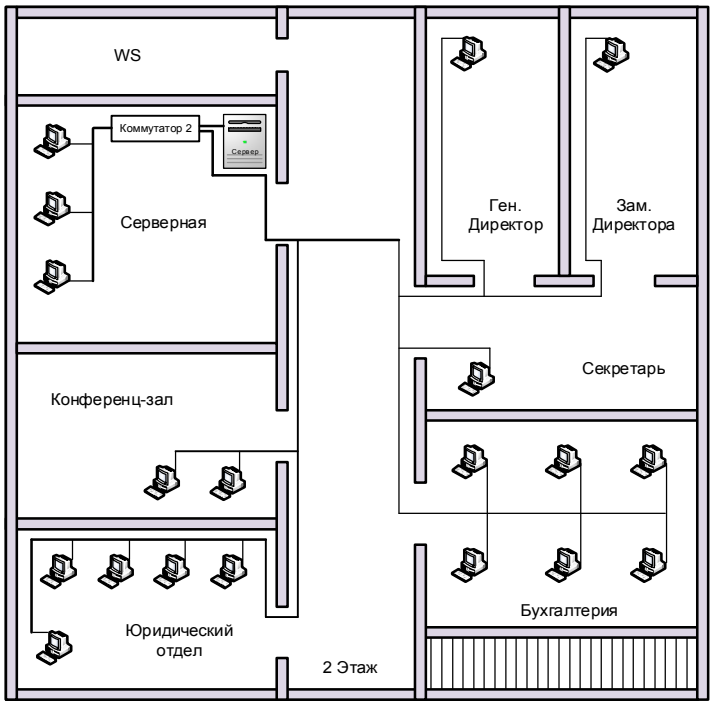


Рис. 2. Схема расположения оборудования на втором этаже

Разработанная локальная сеть выполняет следующие функции:

– создание единого информационного пространства;

– обеспечение достоверности информации и надежности ее хранения путем зеркального копирования (RAID-1);

– обеспечение доступа пользователей к сети Internet.

Использование сети приводит к совершенствованию коммуникаций, то есть к улучшению процесса обмена информацией и взаимодействия между сотрудниками предприятия, а также его клиентами и поставщиками.

---

1. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: учебник для вузов. 2-е изд. – СПб.: Питер, 2004. – 703 с.

2. Сергеев А.П. Офисные локальные сети: самоучитель. – М.: Вильямс, 2006. – 320 с.

УДК 004.733

В.В. Чуйкова, Я.А. Хасан, Аб.А. Нассер

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ METROETHERNET В ПОСТРОЕНИИ СОВРЕМЕННОЙ СЕТИ ГОРОДА ТАИЗ

Предложен вариант по созданию современной сети г. Таиза на базе MetroEthernet, рассмотрены перспективы развития данной технологии.

MetroEthernet является широкополосной сетью масштаба мегаполиса, современной и многофункциональной, с огромными возможностями для использования сетевых ресурсов и мультимедийных услуг, таких как цифровое телевидение, интерактивные телевизионные услуги [1].

MetroEthernet в мире и в Йемене (г. Таиз).

Во всем мире широко используются сети MetroEthernet, но в Йемене пока речь можно вести лишь о сетях с элементами MetroEthernet, и поэтому предлагается разработать вариант системных решений по созданию сети MetroEthernet после проведения анализа уровня развития телекоммуникационной системы в г. Таиз и платежеспособного спроса на новые виды услуг.

Город Таиз – культурная столица республики Йемен и один из активно развивающихся субъектов страны, занимает 10,321 кв. км. Численность населения составляет 2,727,186 человек. Город разбит на 10 районов [2], каждый из которых обслуживается одним OLT. Районы подключаются к центральной станции по топологии «кольцо». Данный способ увеличивает надёжность сети. Район делится на участки. Каждый участок обслуживается одним портом

GPON, т.е. на район отводится оптический сплиттер, от которого до каждого дома прокладывается оптический кабель.

Для увеличения надёжности районная сеть построена по топологии «точка-точка» с резервированием. Для этого используются оптические сплиттеры 2xN. На рисунке приведена структурная схема оптоволоконных линий связи сети города Таиз.

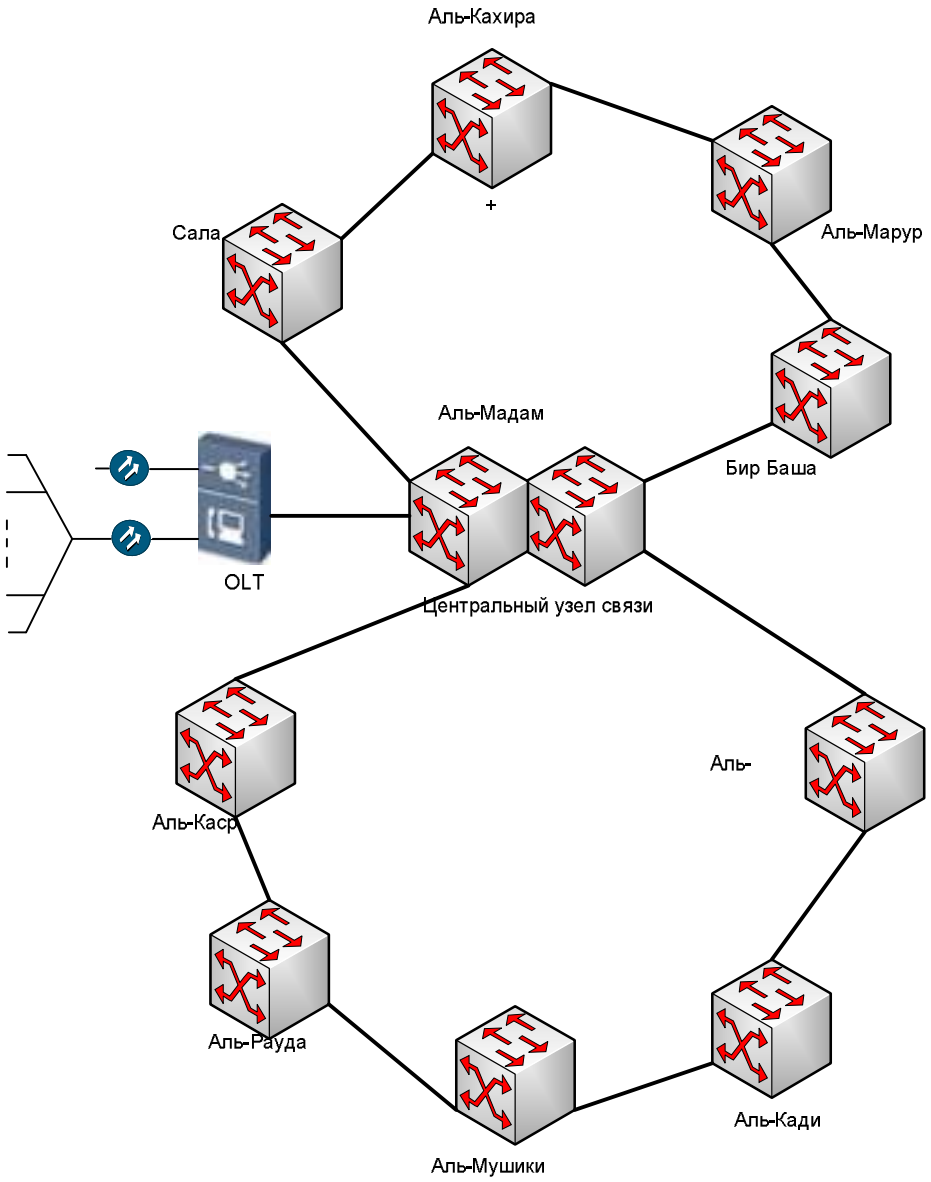


Рис. Структурная схема оптоволоконных линий связи сети города Таиз

На рисунке видно, что на один участок отводится два порта GPON (при этом один порт GPON – резервный, при пропадании оптического сигнала на одном входе сплиттера, система автоматически переключает порт с основного на резервный). Связь между

OLT и центральным коммутатором осуществляется по технологии 10GEthernet.

В будущем при увеличении трафика районы города Тайз разбиваются на микрорайоны. При этом возможно применить такие современные технологии, как CWDM, CWDM и другие. Также предусмотрена возможность подключения абонентов непосредственно волоконно-оптическим кабелем. Центр обработки данных (ЦОД) находится на центральной станции.

Центральный узел связи Аль-Мадам (см. рис.) состоит из магистрального коммутатора, OLT, оборудования цифрового телевидения, SoftSwitch, маршрутизатора, обеспечивающего доступ к сети Internet, и систем, обеспечивающих управление и контроль доступа. Все компоненты подключаются к магистральному коммутатору по интерфейсу MetroEthernet.

---

1. Епанешников А.М., Епанешников В.А. Локальные вычислительные сети. – М.: Диалог-МИФИ, 2005. – 224 с.

2. Государственный информационный центр [Электронный ресурс]. – URL:http://www.yemen-nic.info.

СЕКЦИЯ 3
СИСТЕМЫ КОДИРОВАНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

Н.А. Белова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРИМЕНЕНИЕ ВЕЙВЛЕТ-ПАКЕТНОГО РАЗЛОЖЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СТЕГОВЛОЖЕНИЙ В ФАЙЛАХ ИЗОБРАЖЕНИЙ

Рассмотрен предмет стеганографии, её происхождение и применение на современной стадии развития информационных систем. Приведен краткий обзор проблем стегоанализа. Рассмотрена применимость вейвлет-пакетного разложения для исследования файлов формата jpeg.

Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. Одними из наиболее востребованных в этой области являются технологии, базирующиеся на использовании методов компьютерной стеганографии, позволяющие скрытно встраивать данные в любой формат данных в целях обеспечения эффективной защиты от подделки, копирования и несанкционированного использования. Сегодня указанные технологии широко используются при решении задач создания защищенной связи и передачи данных, аутентификации пользователей, создания цифровых водяных знаков и др.

Стеганография – это наука о передаче секретной информации, причем сам факт передачи остается неизвестен внешнему наблюдателю.

В процессе исследования стеганографии в рамках компьютерной безопасности становится очевидным, что она по существу не является чем-то новым, так как возникла еще во времена Древнего Рима. Первая запись об использовании стеганографии встречается в трактате Геродота «История», относящегося к 440 году до н. э. В трактате описаны два метода скрытия информации. Демарат отправил предупреждение о предстоящем нападении на Грецию, записав его на деревянную подложку восковой таблички до нане-

сения воска. Второй способ заключался в следующем: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Таким образом скрывалось не только значение сообщения, но и вообще его существование.

В настоящее время под стеганографией чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения. Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации – компьютерная стеганография.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, дополняя её. Криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Все алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп:

1. Работающие с самим цифровым сигналом. Например, метод LSB (Least Significant Bit, наименьший значащий бит) – суть метода заключается в замене последних значащих битов в контейнере (изображения, аудио- или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для восприятия человеком.

2. «Впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания ЦВЗ. Цифровые водяные знаки (ЦВЗ) используются для защиты от копирования, сохранения авторских прав. Невидимые водяные знаки считываются специальным устройством, которое может подтвердить либо опровергнуть корректность.

3. Использование особенностей форматов файлов. Сюда можно отнести запись информации в метаданные или в различные другие не используемые зарезервированные поля файла.

4. Другие методы скрытия информации в графических файлах ориентированы на форматы файлов с потерей, к примеру JPEG. В отличие от LSB, они более устойчивы к геометрическим преобразованиям за счёт варьирования в широком диапазоне качества изображения, что приводит к невозможности определения источника изображения.

Существует масса инструментов, пригодных для стеганографии. Важное различие, которое должно быть сегодня проведено среди доступных инструментов стеганографии, – это те, которые стеганографируют, и те, что стегаанализируют.

Стегоанализ – процедура обнаружения факта стеганографического скрытия информации и, если возможно, определения стеганоключа и/или выделения скрытой информации. Если факт скрытого внедрения информации выявлен и удалось выделить скрываемые данные, то становится возможным не только узнать конфиденциальные сведения, но и уничтожить или модифицировать встроенную информацию, или заменить ее на ложную информацию.

Актуальность решения задач стегоанализа обусловливается необходимостью жесткого контроля потоков информации во избежание утечек или нежелательной скрытой коммуникации.

Сегодня в Internet доступны более сотни бесплатных и условно-бесплатных программ для скрытия информации. Вместе с тем число известных программ для стегоанализа ничтожно мало. Данный факт можно объяснить тем, что сама процедура анализа цифровых данных на предмет наличия в них скрытной встроенной информации является значительно более сложной по сравнению с процедурой скрытия. Кроме того, наиболее популярный в настоящее время формат изображений jpeg позволяет осуществлять в него стеговложения, которые не могут быть обнаружены традиционными методами стегоанализа. Для разбора файлов таких форматов нужны более сложные и дорогие методы, результаты применения которых к тому же будут обладать меньшей достоверностью.

Более подробно рассмотрим метод стегоанализа, основанный на оптимальном вейвлет-пакетном разложении.

Можно выделить следующие этапы стегоанализа:

1. Выполнение полного вейвлет-пакетного разложения обучающей выборки, состоящей из пустых файлов-контейнеров и файлов с вложенным стегосообщением, по результатам разложения получается набор коэффициентов разложения, разбитых по диапазонам частот.

2. Вычисляются характеристические признаки изображений, которыми являются абсолютные значения моментов характеристических функций гистограммных коэффициентов субполос, полученных с помощью вейвлет-разложения изображения.

3. Для обучения на вход нейрона, играющего роль классификатора, подаётся полученный (обучающий) набор признаков.

4. Производятся аналогичные действия для тестового набора изображений в целях получения характеристических признаков.

5. Характеристические признаки тестового набора подаются на вход классификатора, в результате будет получена вероятностная оценка вложенности стего в изображении.

Для примера классификации изображений возьмем трёхслойный персептрон с 1-м нейроном на выходе, 5-ю нейронами в скрытом слое и 252-я нейронами на входе.

Выходные значения функции лежат в диапазоне [-1,1], если значение близко к 1, то классификатор указывает на то, что в изображении содержится скрытое сообщение, в случае если выходное значение приближается к -1, это означает, что в изображении нет стеговложений. Максимальное количество возможных итераций установлено в количестве 300000, желаемая выходная ошибка 0,01.

При обучении можно ввести параметры скорости обучения, желаемой ошибки и количество максимальных итераций.

При проверке изображения на вложения есть возможность посмотреть его вейвлет-пакетное разложение, благодаря чему появляется шанс произвести визуальную атаку на некоторые алгоритмы скрытия (рис.).

Определение факта вложения в изображение будет производиться с некоторой погрешностью. Для получения более точных результатов необходимо расширять обучающую выборку и использовать различные размеры внедряемой информации по отношению к файлу-контейнеру.

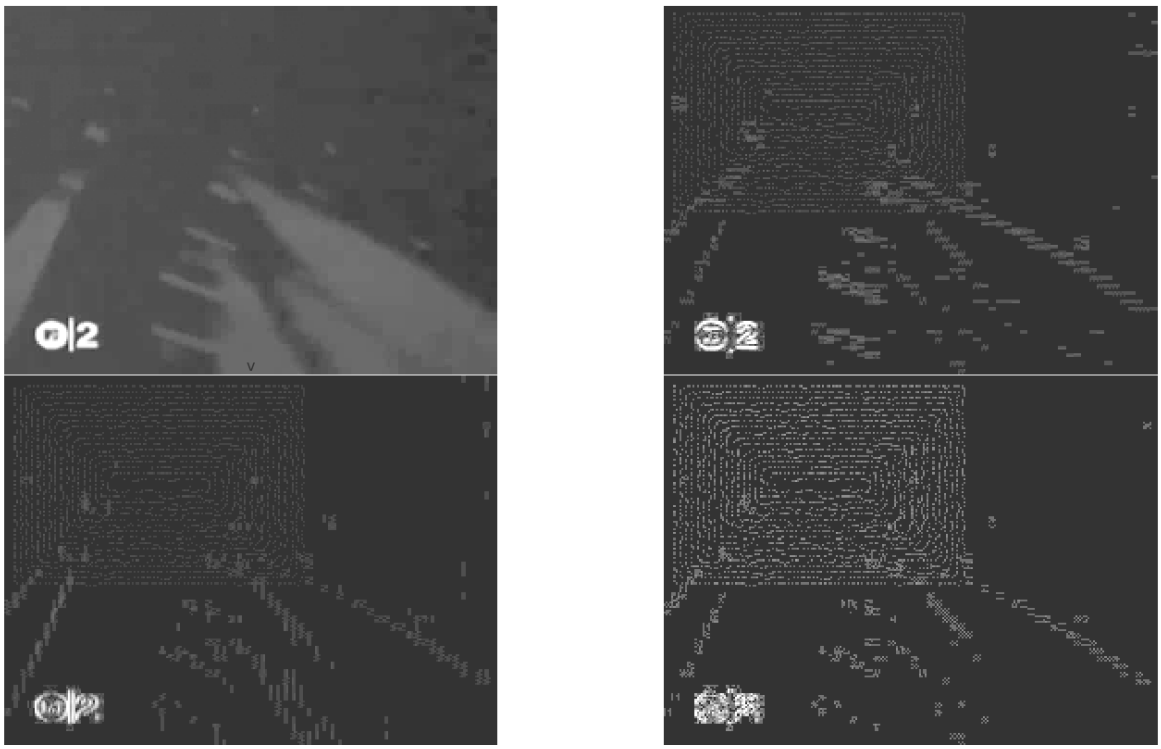


Рис. Результат вейвлет-пакетного разложения

Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к развитию методов компьютерной стеганографии будет усиливаться всё больше и больше. Актуальность проблемы информационной безопасности постоянно растет и требует разработки как новых методов стеганографии, так и методов стегоанализа.

Несмотря на то, что математический аппарат вейвлет-анализа хорошо разработан, вейвлеты оставляют обширное поле для исследований. Кроме того, огромное значение имеет задача разработки приложений, использующих вейвлет-анализ – как в перечисленных областях, так и во многих других, перечислить которые просто не представляется возможным.

---

1. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. – Киев: МК-Пресс, 2006. – 288 с.

2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. – 2-е изд. – М.: Горячая линия – Телеком, 2013. – 232 с.

УДК 004.056

Н.А. Белова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ИССЛЕДОВАНИЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ КАК ОДНОГО ИЗ МЕТОДОВ СТЕГОАНАЛИЗА

Указывается актуальность стегоанализа. Приведены основные элементы стегосистемы. Рассмотрена эффективность применения вейвлет-преобразования в стеганографии.

Стегоанализ – процедура обнаружения факта стеганографического скрытия информации и, если возможно, определения стеганоключа и/или выделения скрытой информации.

В настоящее время стегоанализ является актуальной задачей, особенно в системах, где необходим жесткий контроль потоков информации во избежание утечек или нежелательной скрытой коммуникации. Если факт скрытого внедрения информации выявлен и удалось выделить скрываемые данные, то становится возможным не только узнать конфиденциальные сведения, но и уничтожить или модифицировать встроенную информацию, или заменить ее на ложную информацию.

Для осуществления той или иной угрозы нарушитель применяет атаки. Наиболее простая атака – субъективная. Злоумышленник внимательно рассматривает изображение (слушает аудиозапись), пытаясь определить «на глаз», имеется ли в нем скрытое сообщение. Ясно, что подобная атака может быть проведена лишь против совершенно незащищенных стегосистем.

Первичный анализ также может включать в себя следующие мероприятия:

1. Первичная сортировка стего по внешним признакам.
2. Выделение стего с известным алгоритмом встраивания.
3. Определение использованных стегоалгоритмов.
4. Проверка достаточности объема материала для стегоанализа.
5. Проверка возможности проведения анализа по частным случаям.
6. Аналитическая разработка стегоматериалов. Разработка методов вскрытия стегосистемы.

7. Выделение стего с известными алгоритмами встраивания, но неизвестными ключами и т.д.

Задачу встраивания и выделения сообщений из другой информации выполняет стегосистема. Она состоит из следующих основных элементов:

– прекодер – устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигнал. Например, если в качестве контейнера выступает изображение, то и последовательность встраиваемой информации необходимо представить как двумерный массив бит;

– стегокодер – устройство, предназначенное для осуществления вложения скрытого сообщения в другую информацию;

– стегодетектор – устройство, предназначенное для определения наличия и/или выделения сообщения;

– декодер – устройство, восстанавливающее скрытое сообщение (может отсутствовать).

Известно, что изображения обладают большой психовизуальной избыточностью. Глаз человека подобен низкочастотному фильтру, пропускающему мелкие детали. Это связано с особенностями системы восприятия человека. Особенно незаметны искажения в высокочастотной области изображений. Эти особенности человеческого зрения используют при разработке алгоритмов сжатия изображений.

В большинстве методов скрытия данных в изображениях используется та или иная декомпозиция изображения-контейнера (изображение, в которое производится встраивание). Среди всех линейных ортогональных преобразований наибольшую популярность в стеганографии получили вейвлет-преобразование и дискретное косинусное преобразование (ДКП), что отчасти объясняется их успешным применением при сжатии изображений. Кроме того, желательно применять для скрытия данных то же преобразование изображения, как и то, которому оно подвергнется при возможном дальнейшем сжатии. Так, например, в стандарте JPEG используется ДКП, а в JPEG2000 – вейвлет-преобразование. Стегоалгоритм может быть весьма робастным к дальнейшей компрессии изображения, если он будет учитывать особенности алгоритма сжатия.

Эффективность применения вейвлет-преобразования и ДКП для сжатия изображений объясняется тем, что они хорошо моделируют процесс обработки изображения в системе зрения человека, отделяют «значимые» детали от «незначимых». Значит, их более целесообразно применять в случае активного нарушителя. В самом деле модификация значимых коэффициентов может привести к неприемлемому искажению изображения. При применении преобразования с низкими значениями выигрыша от кодирования существует опасность нарушения вложения, так как коэффициенты преобразования менее чувствительны к модификациям.

Реальные изображения вовсе не являются случайным процессом с равномерно распределенными значениями величин. Известно, что большая часть энергии изображений сосредоточена в низкочастотной части спектра. Отсюда и потребность в осуществлении декомпозиции изображения на субполосы. Низкочастотные субполосы содержат подавляющую часть энергии изображения и, следовательно, носят шумовой характер. Высокочастотные субполосы наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие или НЧ-фильтрация. Таким образом, для вложения сообщения наиболее подходящими кандидатами являются среднечастотные субполосы спектра изображения.

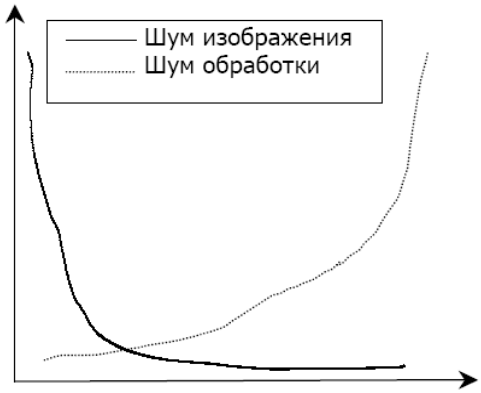


Рис. 1

При сжатии изображения с допустимыми потерями коэффициент сжатия может достигать сотен раз. Популярность вейвлет-преобразования (ВП) во многом объясняется тем, что оно успешно может использоваться для сжатия изображения как без потерь, так и с потерями.

Вейвлет-кодер изображения устроен так же, как и любой другой кодер с преобразованием. Он состоит из трех основных частей: декоррелирующее преобразование, процедура квантования и энтропийное кодирование.

При исследовании сигналов их представляют в виде совокупности последовательных приближений грубой (аппроксимирующей) $A_n(t)$ и уточненной (детализирующей) $D_n(t)$ составляющих

$$S(t) = A_n(t) + \sum_{j=1}^{n} D_j(t)$$

с последующим их уточнением итерационным методом. Каждый шаг уточнения соответствует определённому масштабу a_n, т.е. уровню *n* анализа (разложения) и синтеза сигнала. Такое представление каждой составляющей сигнала вейвлетами можно рассматривать как во временной, так и в частотной областях. В этом суть кратномасштабного анализа – метода анализа данных, основанного на представлении данных с различной степенью детализации. Это позволяет изучать глобальные особенности данных на крупномасштабном представлении и детализировать локальные особенности на мелких масштабах.

Свёртка сигнала с вейвлетами позволяет выделить характерные особенности сигнала в области локализации этих вейвлетов, причём, чем больший масштаб имеет вейвлет, тем более широкая область сигнала будет оказывать влияние на результат свёртки.

В связи с проблемой вычисления большого количества интегралов в вейвлет-преобразовании предлагается использовать быстрое вейвлет-преобразование. При его рассмотрении на каждом шаге происходит расщепление сигнала на ВЧ- и НЧ-составляющие.

В результате получается «полное» дерево (рис. 2).

На вершине полного дерева разложения – исходный сигнал, а ниже – его пакетные вейвлет-коэффициенты. Ветви влево указывают на аппроксимирующие коэффициенты, а правые ветви идут к детализирующим коэффициентам предыдущего узла. Из числа всех представлений мы должны выбрать то, которое представляет сигнал наиболее эффективно.

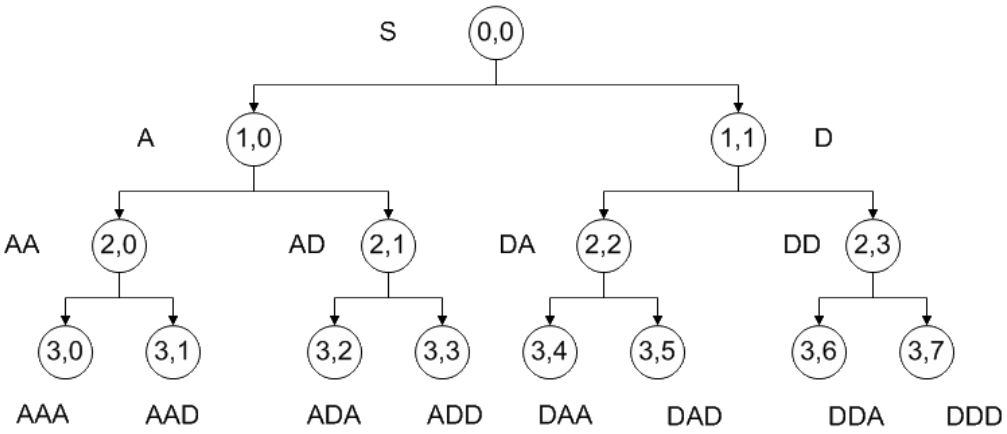


Рис. 2. «Полное» дерево разложения

Обычно в качестве критерия для выбора самого эффективного или лучшего базиса для данного сигнала используется критерий минимальности энтропии. Энтропия характеризует усреднённость, «размазанность» сигнала. Если при разложении коэффициентов некоторого узла сумма энтропий, полученных при разложении компонент, меньше, чем энтропия коэффициентов в исходном узле, то разложение применяется, в противном случае коэффициенты вместе с базисными функциями остаются без изменения.

В настоящее время в мире предложено огромное количество алгоритмов незаметного встраивания информации с использованием вейвлет-преобразования. Первое дискретное вейвлет-преобразование было придумано венгерским математиком Альфредом Хааром. Самый распространенный набор дискретных вейвлет-преобразований был сформулирован бельгийским математиком Ингрид Добеши в 1988 году.

Другие формы дискретного вейвлет-преобразования включают непрореженное вейвлет-преобразование, преобразование Ньюлэнда, пакетное вейвлет-преобразование, комплексное вейвлет-преобразование.

У дискретного вейвлет-преобразования много приложений в естественных науках, инженерном деле, математике. Наиболее широко оно используется в кодировании сигналов, где свойства преобразования используются для уменьшения избыточности в представлении дискретных сигналов, часто – как первый этап в компрессии данных.

Несмотря на то, что математический аппарат вейвлет-анализа хорошо разработан, вейвлеты оставляют обширное поле для исследований. Кроме того, огромное значение имеет задача разработки приложений, использующих вейвлет-анализ как в перечисленных областях, так и во многих других, перечислить которые просто не представляется возможным.

---

1. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в Matlab. – М.: ДМК Пресс, 2005. – 304 с.

2. XiangYang Luo, FenLin Liu, ChunFang Yang and DaoShun Wang. Image universal steganalysis based on best wavelet packet decomposition // SCIENCE CHINA Information Sciences. – 2010. – Vol. 53. – № 3. – P. 634-647.

УДК 621.377.037.3

И.Н. Белугин, Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПОВЫШЕНИЕ СТРУКТУРНОЙ УСТОЙЧИВОСТИ РЕЧЕВОГО ОРТОГОНАЛЬНОГО КОДЕРА

Произведен анализ работы кодера mp3, рассмотрена его структура. Предложены методы повышения помехоустойчивости потока, выходящего из кодера, в случае передачи его по каналу связи.

Использование аудиокодера MPEG уровня 3 для кодирования речи имеет на данный момент весьма большие перспективы. Этот кодер позволяет уменьшить поток передаваемых данных до 25 процентов от начального. Основной преградой для его использования в этих целях является то, что структура файла не способна сохранять свою целостность при воздействии помех в реальном канале связи, что приводит к невозможности воспроизведения речи на приемном конце.

Цель данного исследования – добиться повышения структурной устойчивости потока данных, выходящих из кодера, для обеспечения правильного приема и воспроизведения сообщения после его прохождения по каналу связи (рис. 1).

Рис. 1. Структура кодера mp3

Поскольку кодер изначально разрабатывался для сжатия высококачественной музыки, его необходимо модифицировать для применения в качестве кодера речи:

– во-первых, уменьшить число полосовых фильтров с 20 до 5 для обработки лишь канала тональной частоты;

– во-вторых, использовать только частоту дискретизации, равную 8000, являющуюся стандартной для mp3;

– в-третьих, необходимо полностью отказаться от блока кодирования информации о параметрах канала;

– в-четвертых, упростить блок формирования выходного битового потока для расстановки стартовых и стоповых битов в каждом фрейме.

При передаче потока с выхода кодера по каналу связи, для которого он не предназначен, появляется проблема, связанная с тем, что в кодере не предпринято мер для противодействия помехам при передаче файлов.

Кодер формирует из сигнала фреймы равной длины. Они содержат в себе данные о состоянии фильтров, закодированные при помощи кода Хаффмана.

В начале каждого фрейма передается дерево Хаффмана для него. В случае если при передаче фрейма в канале произойдет ошибка в этом месте, весь фрейм будет неправильно декодирован и воспроизведен.

Для повышения структурной устойчивости кодера к помехам в канале связи целесообразно ввести блок дополнительного кодирования, способного корректировать ошибки при передаче.

Длина каждого фрейма при использовании статических параметров кодера постоянна и рассчитывается по формуле

$$L = 144 \cdot \frac{BR}{SR} + P, \quad (1)$$

где BR (BitRate) – битрейд;
SR (SampleRate) – частота дискретизации;
P (Pad) – заполненность фрейма, равен 0 или1.

Для канала тональной частоты длина фрейма

$$L = 144 \cdot \frac{16000}{8000} + 0 = 288 \text{ бит.} \quad (2)$$

Из них 32 бита – информация о параметрах канала, которая в нашем случае является лишней. Также необходимо избавиться от контрольной суммы по умолчанию. Конечная длина фрейма будет равна 256 бит.

Структура фрейма до модернизации показана на рисунке 2.

Структура фрейма после модернизации показана на рисунке 3.

Заголовок	Контрольная сумма	Вспомогательная информация	Основные данные	Дополнительные данные

Рис. 2. Структура фрейма до модернизации

Вспомогательная информация	Основные данные	Дополнительные данные

Рис. 3. Структура фрейма после модернизации

Для применения кода Хемминга фрейм необходимо разделить на несколько частей равной длины.

При разделении фрейма на блоки длиной 26 бит получим 10 блоков, в которые необходимо добавить в сумме 50 проверочных бит. Длина посылки составит 310 бит, так как последний блок нужно заполнить до получения целого блока.

При использовании канала связи с заранее неизвестной вероятностью ошибки необходимо применять коды с большей корректирующей способностью. Для этой цели применяется сверточный код. Его избыточность равна ½, но при этом он позволяет исправлять практически все ошибки. При применении сверточного кода

длина фрейма увеличится до 512 бит, при этом исправляется до 256 ошибок.

Также для примера можно рассмотреть использование распространенного кода Рида-Соломона RS(255,223) с 8 разрядными символами. Каждое ключевое слово содержит 255 бит кодового слова, из которых 223 – данные, а 32 – паритетные биты.

Декодер исправит любые 16 ошибок символа в кодовом слове, т.е. ошибки вплоть до 16 бит где-нибудь в ключевом слове автоматически исправляются.

При применении этого кода длина посылки составит 510 бит. Это позволит исправить до 32 ошибок в ней.

На рисунке 4 отображена зависимость исправляемых ошибок от количества избыточных бит.

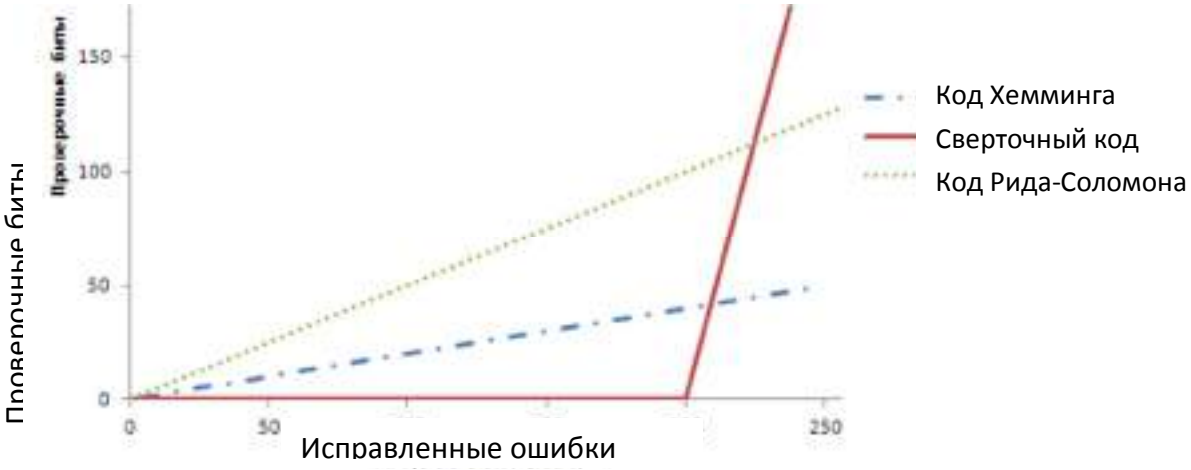


Рис. 4. Зависимость исправляемых ошибок от количества избыточных бит

Методы, показанные в работе, позволяют существенно повысить структурную устойчивость потока данных из речевого кодера.

Выбор оптимального кода зависит от конкретной ситуации, в частности от вероятности ошибки в канале и его пропускной способности. При небольшой вероятности ошибки достаточно применения кода Хемминга. Он прост в реализации и способен исправлять достаточно большое количество единичных ошибок. Если вероятность ошибки в канале очень высока, то необходимо применение сверточных кодов. Они не сложны в реализации, но при этом исправляют большее количество ошибок. Однако главным недостатком применения сверточных кодов является увеличение потока данных в два раза.

1. Сергиенко А.Е. Цифровая обработка сигналов: учебник для вузов. – СПб.: Питер, 2002. – 603 с.

2. Скляр Б. Цифровая связь: [пер. с англ.] / под ред. А.В. Назаренко. – М.: Вильямс, 2003. – 1091 с.

УДК 004.056.55

С.С. Волокитин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДЫ НЕЙРОСЕТЕВОГО БЛОЧНОГО ШИФРОВАНИЯ

В данной работе приводится описание различных методов блочного шифрования на основе нейронных сетей, позволяющих избежать статистических атак с применением только шифротекста.

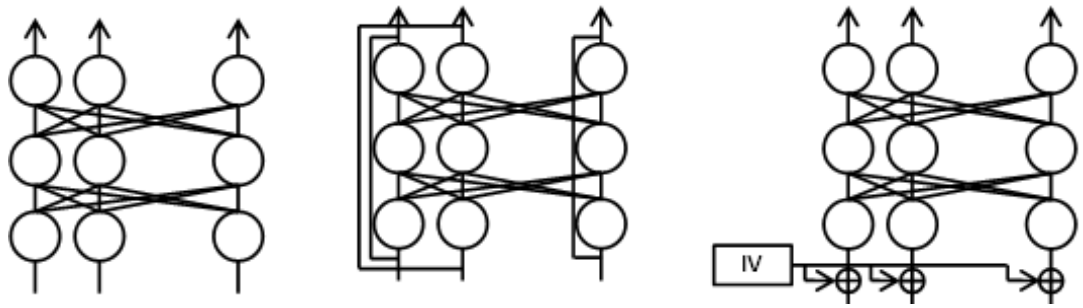
В основе алгоритмов блочного шифрования лежит принцип, согласно которому исходное сообщение разбивается на блоки фиксированной длины и затем выполняется их шифрование. Если применять один и тот же алгоритм с неизменным ключом к одинаковым блокам открытого текста, то в результате шифрования будут получены одинаковые шифротексты, что дает возможности для проведения криптоанализа на основе только шифротекста [1].

В зависимости от алгоритма выделяют следующие виды блочного шифрования:

- шифрование независимыми блоками;
- шифрование сцепленными блоками;
- шифрование с применением вектора инициализации.

Описанные выше методы блочного шифрования находят применения также и в алгоритмах шифрования, основанных на нейронных сетях. На рисунке представлены три структуры нейронных сетей, которые позволяют выполнять блочное шифрование в различных режимах. Топология на рисунке (*а*) – это искусственная нейронная сеть прямого распространения, которая может использоваться для реализации блочного шифра в режиме независимых блоков [2, 3]. Существенным недостатком данного метода, как упоминалось выше, является то, что он подвержен статистическим атакам на шифротекст. К его преимуществам относится более простая структура и меньшее количество связей между нейронами.

На рисунке (*б*) приводится структура рекуррентной искусственной нейронной сети [4], блочные шифры построенные на данном типе нейронных сетей выполняют шифрование в режиме сцепленных блоков, при котором полученный шифротекст зависит не только от входного открытого текста, но и от предшествующего блока, в результате чего одинаковые блоки открытого текста имеют отличные шифротексты.



а) *б*) *в*)

Рис. Топологии нейронных сетей, выполняющих различные режимы блочного шифрования

В основе шифрования с применением вектора инициализации (рис. *в*) лежит применение псевдослучайного значения, используемого в начале передачи либо добавляемого к каждому блоку его порядкового номера. Основным преимуществом шифрования в режиме счетчика является возможность параллельной реализации шифрования последовательных блоков.

Методы нейросетевого блочного шифрования не ограничиваются описанными выше В частности, для реализации шифрования в режиме связанных блоков может применяться нейросеть прямого распространения, представленная на рисунке (*а*), а вместо связей, идущих от выходных нейронов к входным, применяется обучение нейросети после шифрования каждого блока данных. В качестве обучающей пары данных используется открытый текст и полученный на предыдущем этапе шифротекст. После выполнения одной или нескольких эпох обучения нейросети при поступлении одинаковых блоков входных данных получаемые шифротексты на выходе нейросети не будут эквивалентны.

Разнообразие методов блочного шифрования, основанного на применении искусственных нейронных сетей, показывает, что искусственные нейронные сети могут успешно применяться в крип-

тосистемах, позволяя получить необходимые свойства криптографических систем, необходимых для конкретной задачи.

Список литературы

1. Morris Dworkin. Recommendation for Block Cipher Modes of Operation – Methods and Techniques. Special Publication 800-38A (National Institute of Standards and Technology (NIST)) [Электронный ресурс]. – URL: http://csrc.nist.gov/publications/nistpubs/ 800-38a/sp800-38a.pdf (дата обращения: 17.02.2014).

2. Kotlars P., Kotulski Z. On application of neural networks for S-box design, in: P.S. Szczepaniak, J. Kacprzyk, A. Niewiadomski, ed.Advances in Web Intelligence. AWIC 2005, LNCS 3528. – Berlin, 2005. – P. 243-248.

3. Канунников Д.С., Добрица В.П. Нейросетевой подход к шифрованию информации. Проблемы информационной безопасности // Компьютерные системы. – 2010. – № 4. – С. 36-38.

4. Shiguo Lian. A block cipher based on chaotic neural networks // Neurocomputing. – 2009. – Vol. 72. Issues 4–6. – P. 1296–1301.

УДК №004.056

А.В. Губарев

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК СИСТЕМЫ КОНТРОЛЯ ПОДЛИННОСТИ КОМАНДНЫХ СЛОВ

Предметом данного доклада является краткое описание алгоритма определения подлинности и целостности передаваемых командных слов, а также описание результатов моделирования.

Описание алгоритма

В настоящем докладе описываются зависимости между характеристиками передаваемых командных слов (КС) и коллизиями, возникающими в результате приема-передачи указанных слов в процессе определения подлинности и целостности принятых командных слов. Сам алгоритм определения подлинности и целостности принятых КС подробно описан в работе [1]. Здесь мы приведём лишь его основные этапы.

Приемник формирует пул легальных командных слов S_i, состоящих из информативной части, имитоприставки и порядкового номера КС с начала текущего пула i. В процессе формирования

пула к каждому командному слову применяется функция формирования имитоприставки заданной длины $F_{хеш}$. Кроме того, с целью исключения передачи командного слова в открытом виде для каждого командного слова приемник выполняет следующую последовательность действий:

1) формирует слово $i' = F_A\ (S^{sec}, i)$;

2) формирует слово $S_i' = F_B\ (S_i\ , i')$;

3) формирует слово $i'' = F_C\ (S_i'\ , i)$;

4) отправляет в приёмник слово $\{S_i'|i''\}$.

Приёмник в свою очередь выполняет следующие операции:

1) определяет номер $i'_{\text{пр}} = F_{\text{C}}^{-1}(S_i'\ , i'')$;

2) определяет слово $i'_{\text{пр}} = F_A\ \left(S^{sec}, i_{\text{пр}}\right)$;

3) определяет содержимое полученного

$$\text{КС}\ S_i = F_{\text{B}}^{-1}\left(S_i'\ , i'_{\text{пр}}\right),$$

где S^{sec} – секретное слово, известное и источнику, и приемнику;

$F_A\ (B, \text{A})$ – необратимое преобразование;

$F_B\ (A, B)$ и $F_C\ (B, \text{A})$ – обратимые преобразования слова A в соответствии с ключом B, в результате которых длина получаемое слова равна длине слова A;

$F_B^{-1}(A, B)$ и $F_C^{-1}(B, A)$ – преобразования, обратные $F_B\ (A, B)$ и $F_C\ (B, A)$ соответственно.

Полученные командные слова буферизируются, а их имитоприставки проверяются по заданному алгоритму, в результате чего приемник выделяет цепочку командных слов, выданных легальным отправителем.

Результаты моделирования

Задачей имитационного моделирования, использованного для проверки характеристик вышеописанного алгоритма, является определение соотношений между параметрами системы передачи сообщений: размером пула легальных командных слов, размером информативного поля, размером имитоприставки, количеством посторонних слов и вероятностями возникновения коллизий при передаче данных. Под коллизией мы будем понимать ситуацию, при которой приёмник сообщений, выполнив все необходимые опера-

ции, не в состоянии выделить из потока информации командные слова, выданные легальным источником. То есть часть посторонних слов опознаётся приёмником как легальные. Очевидно, что при возрастании количества посторонних слов количество цепочек командных слов, которые приемник может принять за легальные, возрастет. Коллизий такого рода можно избежать, увеличив размер имитоприставки, однако при формировании командного слова необходимо учитывать величину информационной избыточности данного командного слова в целях возможности передачи как можно больше информации за меньшее количество циклов передачи.

При помощи разработанной имитационной модели был смоделирован процесс приема-передачи сообщений длины 16 бит [1] при различных параметрах имитационной модели. Всего проводилось 1000 экспериментов для каждого из набора входных параметров, в каждом из которых цикл передачи сообщений повторялся 100 раз.

Для каждого эксперимента подсчитывалось число циклов передачи, в которых произошла коллизия, и приемник не смог выделить легальные сообщения из всего множества буферизированных. Из полученных 1000 чисел находилось среднее, мода, доверительный интервал.

Графики зависимостей наиболее вероятного числа коллизий от числа посторонних командных слов и размера пула легальных сообщений представлены на рис. 1.

Как видно, для каждого размера пула легальных командных слов при неизменных характеристиках самих командных слов наступает момент «насыщения», когда количество посторонних слов слабо влияет на количество появляющихся коллизий. Именно для этой области мы и находим доверительные интервалы для числа возникающих коллизий. Для пула из 5 легальных командных слов максимальное число коллизий при сколь угодно большом количестве посторонних командных слов лежит в интервале (13, 21). Для пула из 10 легальных командных слов число коллизий в 90% экспериментов попадает в интервал (25, 37) с модой 34. Для пула из 15 командных слов аналогично: интервал (35, 46), мода 42. Для пула из 25 командных слов – в интервале (53, 64), мода 60, а для пула из 31 командного слова – в интервале (60, 71), мода 67.

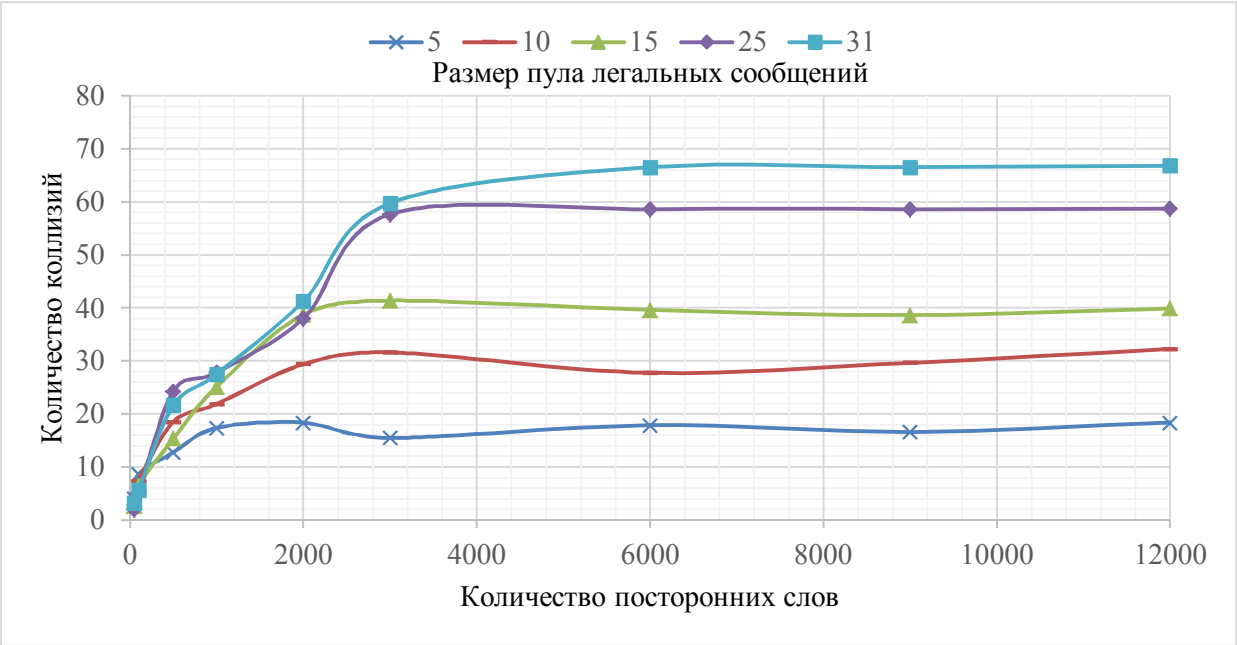


Рис. 1. Графики зависимостей наиболее вероятного числа коллизий от числа посторонних командных слов и размера пула легальных командных слов при постоянном размере имитоприставки

На втором этапе моделирования мы оставляли размер буфера неизменным и варьировали размер имитоприставки. На рис. 2 представлен график зависимости наиболее вероятного числа возникших коллизий от размера имитоприставки и количества командных слов, генерируемых посторонним источником.

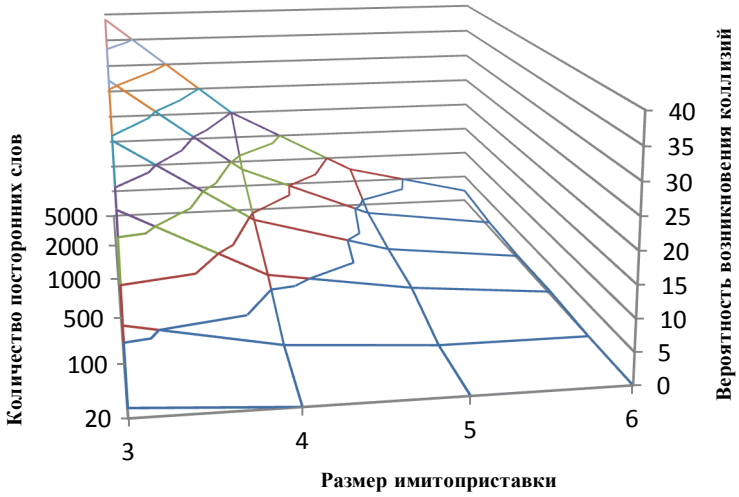


Рис. 2. График зависимости наиболее вероятного числа коллизий от числа посторонних слов и размера имитоприставки

В процессе моделирования приема, передачи и определения подлинности командных слов было установлено следующее:

– вероятность возникновения коллизий при сколь угодно большом количестве посторонних командных слов зависит только от размера пула легальных командных слов и размера имитоприставки;

– оптимальным с точки зрения информационной избыточности размером имитоприставки является 3 бита;

– увеличение имитоприставки на единицу приводит к снижению частоты коллизий в среднем в 2 ÷ 3 раза.

---

1. Таныгин М. О. Верификация данных, передаваемых между устройством и программным обеспечением // Электронные средства и системы управления: материалы докладов Международной научно-практической конференции (13–16 октября 2010 г.). – Томск: В-Спектр, 2011. – Ч. 2. – С. 49–52.

УДК 004.056.55

А.А. Евсеева

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РЕЖИМЫ ШИФРОВАНИЯ БЛОЧНЫХ ШИФРОВ

Рассмотрены основные режимы шифрования, применяемые в блочных шифрах, их преимущества и недостатки.

Режим шифрования блочных шифров – это такой метод шифрования, который позволяет преобразовать последовательность блоков открытого текста в последовательность блоков шифротекста. Блочный шифр работает с отдельными блоками данных, тогда как алгоритм режима шифрования – со всем сообщением, которое уже и разбивается на блоки. Режимы шифрования используются для изменения процесса шифрования таким образом, чтобы результат шифрования каждого блока не зависел от находящихся в нем данных. Блочные шифры шифруют данные блоками определенного размера, поэтому существует вероятность, что злоумышленник может сделать выводы о структуре данных в повторяющихся частях блока. Режимы шифрования созданы, чтобы этому воспрепятствовать.

Существуют следующие основные режимы шифрования:

- Электронная кодовая книга.
- Сцепление блоков по шифротексту.
- Обратная загрузка шифротекста.
- Обратная загрузка выходных данных.
- Шифрование со счётчиком.

Режим «электронной кодовой книги» или «простой замены», в котором исходный текст разбивается на блоки, а каждый блок шифруется отдельно от другого, является самым простым режимом. Так как один и тот же блок исходного текста заменяется одним и тем же блоком шифротекста, то теоретически существует возможность создать электронную книгу, в которой будут сопоставлены блоки исходного текста с соответствующими им шифротекстами. Достоинство данного режима заключается в том, что нет необходимости в последовательном шифровании, так как блоки шифруются независимо друг от друга. Если размер исходного текста не кратный размеру блока, то текст дополняется с конца, чтобы сделать последний блок таким же, как другие. Недостатком данного режима является то, что из одинаковых блоков исходного текста получаются одинаковые блоки шифротекста. Злоумышленник сможет начать составлять электронную книгу, не зная ключ, сделает выводы о свойствах исходного текста благодаря повторяющимся блокам.

В режиме «сцепление блоков» результат шифрования текущего блока зависит не только от исходного текста, но еще и от результата шифрования предыдущих блоков. Перед шифрованием над каждым блоком исходного текста проводится операция «исключающее или» с предыдущим блоком шифротекста. Когда блок зашифрован, его отправляют в выходные данные и сохраняют в памяти, чтобы использовать для шифрования следующего блока исходного текста. Дешифрация происходит аналогичным образом.

Преимуществом данного режима является то, что при его использовании практически невозможно выявить шаблонные блоки исходного текста, за исключением первого блока, над которым операция «исключающее или» проводилась с фальшивым блоком, называемым «вектор инициализации». Но данный режим имеет и

свои недостатки. Каждый блок шифртекста зависит от предыдущего блока, поэтому не удастся выполнять параллельное шифрование блоков, что существенно увеличит временные затраты. Одинаковые блоки, принадлежащие одному и тому же сообщению, зашифровываются в отличные друг от друга блоки шифртекста. Если одинаковые блоки стоят в начале двух сообщений, шифрующихся с помощью одного и того же вектора инициализации, то шифртекст данных блоков тоже будет совпадать. В добавок ко всему злоумышленник может добавить некоторые блоки или биты в конец потока зашифрованного текста, тем самым сделав невозможным для получателя процесс расшифрования текста.

В режиме «обратной загрузки шифротекста» результатом каждой стадии является проведение операции «исключающее или» над результатом предыдущей стадии и текущим блоком исходного текста. Данный режим схож с режимом сцепления блоков. Вектор инициализации можно делать открытым, как и в режиме сцепления блоков, но он должен быть уникальным для каждого сообщения. Недостаток данного режима заключается в том, что ошибка, возникающая в шифротексте при передаче, сделает невозможной расшифровку как блока, в котором произошла эта ошибка, так и следующего за ним. Однако на последующие блоки эта ошибка не распространяется.

Режим «обратной загрузки выходных данных» или «внешней обратной связи» очень похож на режим «обратной загрузки шифротекста», но с той разницей, что каждый бит в зашифрованном тексте независим от предыдущих битов. Данная особенность режима позволяет избежать распространения ошибок. Это означает, что если при передаче возникает ошибка, она затрагивает лишь бит, в котором эта ошибка произошла.

В режиме «шифрования со счетчиком» псевдослучайный ключевой поток достигается с помощью счетчика. Счетчик приобретает заранее определенное значение (вектор инициализации), а затем увеличивается по заранее определенному правилу, которое может зависеть от номера обрабатываемого блока данных. Так как отсутствует обратная связь, то алгоритмы шифрования и расшифровки могут выполняться параллельно, что существенно уменьшает время работы алгоритмов.

Рассмотренные режимы шифрования различны по структуре и характеристикам. Выбор конкретного режима зависит от цели, поставленной обладателем информации. Режим электронной кодовой книги подходит для шифрования ключей, так как данные, используемые в качестве ключа, обычно малого размера и случайны. Для шифрования текста подходят режимы обратной связи и режим со счетчиком, а для шифрования файлов – режим сцепления блоков. Выбор режима шифрования – поиск компромисса между производительностью и эффективностью.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: [пер. с англ.]. – М.: Изд-во ТРИУМФ, 2002. – 816 с.

2. Скляров Д.В. Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2006. – 271с.

3. Берхоуз А. Математика криптографии и теория шифрования [Электронный ресурс]. – URL: http://www.intuit.ru/studies/courses/552/408/info.

4. Введение в криптографию / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко [и др.]; под ред. В.В. Ященко. – 4-е изд., доп. – М.: МЦНМО, 2012. – 348 с.

УДК 004.056.55

А.А. Евсеева

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВИДЫ АТАК НА БЛОЧНЫЕ ШИФРЫ

Рассмотрены основные виды атак на блочные алгоритмы шифрования.

Атака на блочный шифр – попытка криптоаналитика дешифровать без знания ключа данные, которые зашифрованы блочным алгоритмом.

Атака на основе шифротекста – один из основных способов атак на блочные шифры. Криптоаналитик обладает некоторым набором шифротекстов, которые получены в результате зашифрования одним и тем же алгоритмом. Цель атаки заключается в том, чтобы получить как можно большее количесво открытых текстов или же (в лучшем случае) ключа, применяемого при шифровании. Данный вид атаки является основным, так как получить шифротек-

сты совсем не сложно, если зашифрованные данные передаются по открытому каналу. Но несмотря на простоту получения исходных данных, атака на основе только шифротекста является очень неудобной, так как криптоаналитик обладает наименьшим объемом информации.

Атака на основе открытых текстов – вид атаки, при котором у атакующего есть открытый текст и соответствующий ему шифротекст, или же в зашифрованном тексте присутствуют отрывки, смысл которых заранее ему известен. Задачей криптоаналитика является нахождение ключа, использованного при шифровании сообщений, для расшифровки других шифротекстов. Получение открытых текстов является самой важной составляющей этой атаки. Например, можно догадаться о содержимом файла по его расширению, а сообщения переписки обычно начинаются и заканчиваются одним и тем же текстом (приветствие, заключительная форма вежливости, подпись). Это позволяет криптоаналитику подобрать часть зашифрованного текста, а затем, используя частотный анализ либо какие-нибудь другие методы, восстановить исходное сообщение. Данный вид атаки сильнее, чем атака на основе только шифротекста.

Атака на основе подобранного открытого текста – вид атаки, при котором у криптоаналитика также имеется набор открытых текстов и соответствующих им шифротекстов, но помимо этого он имеет возможность зашифровать некоторые подобранные им открытые тексты. Задачей криптоаналитика является нахождение ключа. Зашифрование подобранного открытого текста осуществляется следующим образом: атакующий пересылает пользователю подготовленный открытый текст и заставляет его переслать данный текст кому-либо еще. Программа на компьютере пользователя автоматически шифрует данное сообщение перед отправкой. Криптоаналитик перехватывает трафик и получает шифротекст по написанному им самим открытому тексту. Этот вид атаки дает криптоаналитику больший объем информации об использованном ключе.

Атака на основе подобранного шифротекста — атака, при которой криптоаналитик может выбирать шифротекст, который будет расшифрован, а также имеет доступ к открытому тексту, кото-

рый получится из подобранного шифротекста. Криптоаналитик может воспользоваться устройством расшифрования один или несколько раз для получения шифротекста в расшифрованном виде. Используя полученные данные, он может попытаться восстановить ключ для расшифровки. Атака на основе подобранного шифротекста может быть адаптивной и неадаптивной. При неадаптивной атаке шифротексты подбираются заранее, следующая атака не зависит от предыдущей. В противоположном случае криптоаналитик подбирает шифротекст, который зависит от результатов предыдущих расшифровок.

Дифференциальный криптоанализ – атака, в которой анализируется пара шифротекстов, полученных из пары открытых текстов. Криптоаналитику известны различия открытых текстов, и на основе различий полученных шифротекстов он может сделать вывод о ключе. Криптоаналитик берет два открытых текста и следит за изменениями, происходящими при шифровании. Расхождения в результате получаемого шифротекста помогают составить карту вероятностных значений ключа. Криптоаналитик проделывает данную операцию с максимально возможным количеством пар открытых текстов, тем самым постепенно определяет ключ. Данный способ относится к атаке на основе подобранного открытого текста.

Линейный криптоанализ – атака, в которой криптоаналитик выполняет атаку на основе известного открытого текста с максимальным количеством слов. Она анализирует вероятность того, что определенные входные значения дают определенную выходную комбинацию. Это позволяет криптоаналитику анализировать различные вероятностные значения ключа, пока не найдется повторяющийся шаблон. Методы линейного и дифференциального криптоанализа являются в данный момент самыми популярными видами атак на блочные алгоритмы шифрования.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: [пер. с англ.]. – М.: Изд-во ТРИУМФ, 2002. – 816 с.

2. Скляров Д.В. Искусство защиты и взлома информации. – СПб: БХВ-Петербург, 2006. – 271 с.

3. Берхоуз А. Математика криптографии и теория шифрования [Электронный ресурс]. – URL: http://www.intuit.ru/studies/courses/552/408/info.

4. Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров [Электронный ресурс]. – URL: http://www.ssl.stu.neva.ru/psw/crypto/ rostovtsev/cryptoanalysis.html.

УДК 004.056.55

К.Ю. Игуменов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АУТЕНТИФИКАЦИЯ СООБЩЕНИЙ

Рассмотрены реализации процесса аутентификации сообщений в электронном документообороте. Приведенные приемы основаны на использовании криптографических алгоритмов.

Под аутентификацией сообщений подразумевается подтверждение их подлинности, то есть однозначно устанавливается и подтверждается авторство сообщений. Для решения этой проблемы широко используются криптографические методы. Могут применяться как симметричные, так и асимметричные шифры.

Например, симметричный шифр ГОСТ 28147-89 предусматривает режим выработки имитовставки. Она передается по каналу данных после зашифрованных блоков.

Имитовставка – это отрезок информации фиксированной длины, который передается вместе с зашифрованными данными для обеспечения имитозащиты, то есть защиты от навязывания ложных данных.

Аутентификация может быть обеспечена и с помощью асимметричных алгоритмов. Для этой цели используются схемы с электронной подписью. Электронная подпись – аналог собственноручной подписи человека, адаптированная для использования в электронном документообороте. Она сохраняет все свойства традиционной подписи – каждая подпись уникальна, ее можно сгенерировать на любом документе, подлинность подписи всегда можно проверить с помощью сверки с образцом.

Схемы электронной подписи основаны на использовании однонаправленных функций с секретом, которые используются в алгоритмах с открытым ключом шифрования. Секретный ключ ис-

пользуется отправителем, которым он подписывает сообщение перед отправкой получателю. Получателю достаточно знать открытый ключ отправителя, который хранится в общедоступных справочниках.

Рассмотрим пример функционирования системы.

Пусть *S* (подписывающий) – участник криптосистемы, который будет отправлять сообщения. Параметр однонаправленной функции с секретом выбирает *S* и держит его в тайне. Ему известна вся функция с параметром, которую он может вычислить. Функцию без секретного параметра он помещает в общедоступный справочник.

S берет однонаправленную функцию и, зная ее секретный параметр, вычисляет прообраз сообщения *M*. У него получается некоторая величина *Q*, которая объявляется электронной подписью сообщения *M* и отправляется по открытому каналу вместе с сообщением получателю *V*.

V, решив проверить подлинность сообщения ~*M*, обращается в общедоступный справочник и считывает оттуда открытый ключ предполагаемого подписывающего. Далее с помощью этого ключа он вычисляет однонаправленную функцию, беря в качестве параметра подпись ~*Q*. Полученное значение сравнивается с сообщением ~*M*. В случае совпадения результата подпись признается действительной.

Так как схема электронной подписи представляет собой схему шифрования с открытым ключом «наоборот», то для решения задач электронной подписи можно использовать те же алгоритмы, что и в схемах шифрования.

Рассмотрим для примера схему подписи RSA.

В качестве секретного ключа выбирают два больших простых числа *p* и *q*. В качестве открытого ключа будет выступать их произведение и дополнительный параметр *e*. Для подписания сообщения над ним выполняется операция модульного экспоненционирования, используя секретный ключ. Сообщение вместе с подписью отправляется в открытый канал связи.

Получатель для валидации сообщения вычисляет функцию в прямую сторону. Если в результате получается исходное сообщение, то подпись признается действительной.

На примере схемы электронной подписи RSA видна одна существенная проблема: поскольку алгоритм использует модульные операции, длина подписи равна длине исходного сообщения. А что делать, если сообщение достаточно большое? Подпись увеличивает объем передаваемых данных ровно в 2 раза.

Для решения этой проблемы используются хэш-функции, которые одновременно являются средством обеспечения целостности.

Целостность и подлинность – это такие свойства информации, которые чаще всего теряют смысл, если они не выполняются одновременно.

Под обеспечением целостности данных понимают криптографическую функцию, гарантирующую отсутствие неавторизованных изменений данных в процессе их жизненного цикла.

Криптографическая хэш-функция обладает специальными свойствами:

- Функция преобразует вход любой длины в выход фиксированной, который согласован со входом на цифровую подпись.
- Функция является однонаправленной.
- Вычислительно невозможно подобрать такую пару разных чисел, хэш-функции которых будут равны (эта ситуация называется коллизией).

Последнее свойство является наиболее тонким. Поскольку хэш-функция обладает свойством сжатия, ее область значений меньше области определения, поэтому коллизии неизбежны. Следовательно, это свойство стоит понимать не как требование отсутствия коллизий, а как требование трудности их обнаружения.

Хэш-функция применяется с целью сокращения длины подписываемого сообщения и одновременно обеспечения целостности.

Следует отметить криптографические хэш-функции с ключом. Они содержат в себе некий секретный параметр. Такие хэш-функции уже обеспечивают аутентичность сообщений и вычисляются намного быстрее электронных подписей, но, так как они являются симметричным алгоритмом шифрования, требуют для распространения ключей наличие защищенных каналов связи и, кроме того, не обеспечивают свойства неотказуемости от факта создания сообщения.

1. Информационная безопасность открытых систем: в 2 т. – Т. 2. Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – М.: Горячая линия-Телеком, 2000. – 558 с.: ил.

УДК 003.26.09

Р.А. Провоторов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

КРИПТОГРАФИЯ В НАШЕЙ ЖИЗНИ

В статье показана необходимость применения шифрования информации.

В жизни нам часто приходится встречаться с передачей информации в цифровом виде. Отправляем коллегам важные документы, пишем близким людям в социальных сетях и т.д. Всегда найдется тот, кто захочет вторгнуться в личное пространство и заполучить ценные данные. И если при рабочей системе контроля доступа для этого понадобятся определенные знания, то в случае вышеуказанными и неисправными системами для злоумышленников нет препятствий. Абсолютно любой сможет получить доступ к порой очень ценной информации.

Вот тут нам на помощь приходит шифрование, которым занимается криптография. Таким образом, мы имеем помимо систем контроля доступа некую «формулу» или «гарантию безопасности», которая не даст возможности ознакомиться с данными в доступной форме, даже при получении их на руки.

Исторически криптография зародилась как способ скрыть передаваемое сообщение. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов асимметричного или симметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Аутентификация позволяет устанавливать соединение только легальным пользователям и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легальность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Обеспечение целостности, конфиденциальности и подлинности передаваемых и сохраняемых данных осуществляется прежде всего правильным использованием криптографических способов и средств зашиты информации. Большинство криптографических средств защиты информации используют шифрование данных.

Под шифром понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Под зашифровыванием информации понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифротекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют расшифровыванием (дешифрованием).

Выше упоминались понятия: «симметричное» и «асимметричное шифрование». Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифровывания и расшифровывания информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. Соответственно, с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптосистемы называют криптосистемами с секретным ключом – ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Симметричные криптосистемы называют еще одноключевыми криптографическими системами, или криптосистемами с закрытым клю-

чом. Основным их преимуществом является скорость процесса шифрования. Лучше всего симметричные шифры подходят «для себя», чтобы ограничить доступ к информации в отсутствие владельца.

Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:

• открытый ключ *К* используется для шифрования информации, вычисляется из секретного ключа *к*;

• секретный ключ *к* используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа *К*.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ *к* из открытого ключа *К*. Поэтому открытый ключ *К* может свободно передаваться по каналам связи. Асимметричные системы называют также двухключевыми криптографическими системами, или криптосистемами с открытым ключом.

Сегодня существует множество алгоритмов шифрования, которые признаны в разных странах как государственные стандарты шифрования. Для примера приведем несколько наиболее известных: RSA, DES, BlowFish, Rijndael и прочие… Что касается последнего из перечисленных, то у него есть упрощенный вариант с ключами длиной 128, 192 и 256 Бит, который является стандартом в США и называется AES.

Таким образом, если применять шифрование более широко, можно основательно усложнить жизнь мошенникам и облегчить жизнь как рядовому пользователю, так и специалисту по ЗИ.

---

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД «Форум»: Инфра-М, 2008. – 416 с.: ил.

2. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 120 с.

УДК 004.056.5

П.А. Сапельченков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ НЕЙРОСЕТИ

Изложен метод распределения ключей, основанный на возможности обучения нейронных сетей с учителем и методе «синхронизации».

В настоящее время значительное внимание уделяется использованию искусственных нейронных сетей для решения различных задач. Большое распространение ИНС получили и в сфере безопасности.

Много современных методов распределения ключей в шифровании основаны на алгоритме Диффи-Хелмана. Обычно секретный ключ генерирует одна из сторон обмена, затем по каналу связи он передается другой стороне. Дополнительной особенностью нейросетевых систем является то, что секретный ключ не передается между участниками обмена, а генерируется в процессе их общения по системам связи.

Метод «синхронизации» основан на возможности обучения нейронных сетей по образцам (с учителем). Если две нейросети будут обучаться друг по другу, произойдет их синхронизация: благодаря подстройке весовых коэффициентов при использовании одинаковой базы, подаваемой на входы, получим одинаковые ключи на выходе.

Предположим, существуют два абонента, они знают параметры сети, которые не являются секретными, т.е. злоумышленник может свободно завладеть этим знанием. Изначально весовые коэффициенты задаются случайно. Затем абоненты начинают обмениваться обучающими парами «база-ключ», и после нескольких шагов они будут иметь идентичные нейросети, необходимые для генерации одинаковых секретных ключей.

Используя метод синхронизации, абоненты могут получить у себя идентичные нейросети, чтобы после начать процедуру обмена секретными ключами. Основной задачей является сделать недоступной информацию о параметрах ИНС для злоумышленника. Эту проблему можно решить, используя комбинированный метод.

У каждого из двух абонентов имеется программа или аппаратное средство определенной структуры. Две нейронных сети одинакового или различного внутреннего строения, обладающие нужными параметрами входных и выходных сигналов. Первая нейросеть служит для синхронизации с аналогичной у другого абонента. Вторая нейросеть необходима для получения секретного ключа.

Использование шифратора делает возможным сокрытие обучающих вторую – «тайную» нейросеть данных. Для обучения ИНС необходима пара «база-ключ». В ходе работы обучающая пара преобразуется в шифраторе по правилам, известным только абонентам А и В, а не злоумышленнику.

Безопасность процесса, прежде всего, зависит от сохранности в тайне ключа шифратора. Злоумышленник, перехватывая сообщения, содержащие обучающую пару, не сможет получить данные для обучения тайной сети, с помощью которой вычисляется секретный ключ. При этом ключ шифратора может быть достаточно простым, и его передача по секретному каналу намного проще и экономнее, нежели передача параметров или готовых устройств. Чтобы увеличить защищенность, можно проводить переобучение нейросетей через определенные периоды времени. Целью дальнейших исследований является сравнительный анализ алгоритмов распределения ключей.

Нейросетевые технологии все чаще находят применение в различных сферах человеческой деятельности. Основываясь на эффекте синхронизации нейросетей, был разработан комбинированный метод распределения ключей. Его аппаратная реализация может подойти для внедрения в автоматизированные системы аутентификации пользователей на предприятии.

---

1. Добрица В.П., Канонников Д.С. Нейросетевой подход к распределению ключей //Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 3. – С. 52-54.

2. Philip D. Wasserman Neural computing: Theory and Practice. – М., 1992. – 240 с.

УДК 680.5.01

К.Н. Воробьев, И.С. Надеина, С.В. Спевакова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ВЫДЕЛЕНИЕ ДИНАМИЧЕСКИХ ОБЪЕКТОВ ПОДВИЖНОЙ СТЕРЕОСКОПИЧЕСКОЙ СИСТЕМОЙ ТЕХНИЧЕСКОГО ЗРЕНИЯ

Рассмотрена структура подвижной стереоскопической системы технического зрения выделения движущихся объектов с использованием GPS-модуля. Определены основные этапы обработки и анализа изображений исследуемых объектов.

В связи с широким внедрением систем технического зрения (СТЗ) в информационные технологии актуальным направлением является визуальное восприятие движущихся объектов системами видеонаблюдения. Необходимость слежения за динамическими объектами и определения параметров их движения возникает при обеспечении безопасности движения, испытаниях объектов, при реализации взаимодействия объектов между собой. В связи с этим задача выделения движущихся объектов с помощью подвижной стереоскопической системы технического зрения является актуальной.

При неподвижной системе технического зрения объект относительно нее движется и попадает в поле зрения. В результате задача выделения объектов сводится к анализу последовательности изображений и определения параметров его траектории относительно окружающей среды [1,2] .

Решение задачи слежения за объектом, расположенном на сложном фоне, подвижной системой СТЗ сводится к получению пространственных параметров движущегося объекта, размеры и конфигурация которого изменяются в процессе измерения, для чего необходима последовательная обработка, требующая оценки сигнала на каждом такте с учетом информации, поступающей в процессе наблюдения.

При таких условиях движущиеся объекты могут быть выделены путем анализа изменений последовательности изображений, скорректированных на изменение положения системы наблюдения относительно плоскости перемещения исследуемого объекта с помощью GPS-модуля. Так, GPS-модуль, работающий синхронизи-

рованно с системой наблюдения, фиксирует свои координаты. При движении СТЗ осуществляется фиксация координат ее перемещения в периодические интервалы времени, затем производиться корректировка полученных координат с кадрами изображения в те же временные интервалы. Данный метод позволяет выявить, является ли выделенный объект статичным или динамичным, и определить его пространственные координаты.

Система, осуществляющая слежение подобным образом, производит сбор и обработку результатов измерений, поступающих от оптико-электронных и радиолокационных средств наблюдения. Наряду с повышением качества средств наблюдения совершенствование систем слежения достигается путем использования нескольких датчиков изображения, позволяющих повысить точность и быстродействие определения параметров движения.

Разработанная подвижная стереоскопическая оптико-электронная система слежения позволяет вести наблюдение за несколькими динамическими объектами, находящимися в ее поле зрения, определять их геометрические размеры и пространственные координаты.

Структурная схема аппаратной реализации разработанного метода изображена на рисунке.

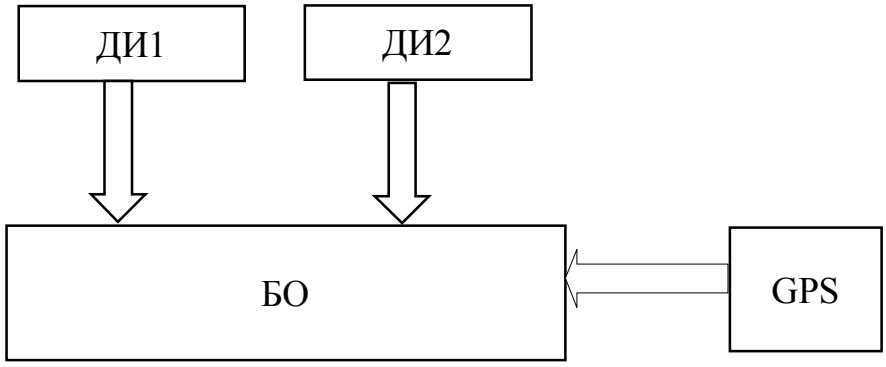


Рис. Структурная схема устройства выделения динамических объектов

Для получения координат точки объекта используются два датчика изображения (ДИ1 и ДИ2), блок обработки данных (БО) и блок GPS. Данные из ДИ1 и ДИ2 параллельно с координатами GPS поступают в блок управления, где осуществляется анализ полученной информации.

Предложенный алгоритм позволяет осуществлять выделение динамических объектов, определение их пространственных координат при использовании как в подвижных, так и неподвижных системах наблюдения.

На основе представленных методов можно создать оптико-электронное устройство автоматического выделения динамических объектов.

Список литературы

1. Independent 3D Motion Detection Through Robust Regression in Depth Layers / A. Argyros, M. Lourakis, P. Trahanias, S. Orphanoudakis // In Proc. BMVC ’96. Edinburgh, UK. – 1996. – S. 9-12.

2. Clarke J. C. and Zisserman A. Detection and Tracking of Independent Motion // Image and Vision Computing. – 1996. –Vol. 14. – P. 565–572.

3. Спеваков А.Г., Ширабакина Т.А. Адаптивная оптико-электронная система обнаружения объектов изображения и выделения их контуров // Известия Тульского государственного университета. – 2002. – Т. 4. – Вып. 1. – С. 91-95.

УДК 004.056

К.А. Тезик, Д.Э. Данилов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

КРИПТОСИСТЕМА НА ОСНОВЕ СИНТЕЗА МЕТОДА ВИЖЕНЕРА И АЛГОРИТМА RSA

В статье предложена криптосистема, основанная на комбинированном использовании шифра Виженера и алгоритма RSA. Рассмотрены принципы работы и возможности компьютерной программы, реализующей криптосистему.

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность. Основные направления использования криптографических методов: передача конфиденциальной информации по каналам связи, установление подлинности передаваемых сообщений, хранение информации на носителях в зашифрованном виде. В качестве информации, подлежащей шифрованию и расшифрованию, рассматриваются тексты, построенные на некотором алфавите. Алфавит – конечное множество используемых для кодирования информации знаков.

Зашифрование – процесс преобразования открытых данных в зашифрованные, расшифрование – обратный процесс преобразования зашифрованных данных в открытые. Криптографическая система представляет собой семейство T обратимых преобразований открытого текста в шифрованный. Члены этого семейства индексируются или обозначаются символом k; параметр k называется ключом. Преобразование T_k определяется соответствующим алгоритмом и значением ключа k.

Ключ – конкретное значение некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из семейства. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованному. Криптосистемы подразделяются на симметричные и асимметричные (или с открытым ключом). В симметричных криптосистемах для зашифрования и расшифрования используется один и тот же ключ. В системах с открытым ключом используются два ключа – открытый (публичный) и закрытый (секретный), которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Асимметричные криптосистемы имеют значительные преимущества по сравнению с симметричными :

– отсутствует необходимость передачи секретного ключа по надежному каналу связи;

– ключи можно не менять более значительное время;

– в больших сетях число ключей в асимметричной криптосистеме связано с количеством абонентов линейной зависимостью, и поэтому оно значительно меньше, чем в симметричной, где данная зависимость квадратичная;

– в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей;

– асимметричные криптосистемы позволяют реализовывать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку закрытый ключ должен быть известен только владельцу.

Однако симметричные криптосистемы тоже имеют некоторые преимущества по сравнению с асимметричными:

– процесс шифрования–расшифрования происходит значительно быстрее;

– при сравнимой криптостойкости длина ключа в симметричной криптосистеме значительно меньше, чем в асимметричной;

– симметричные криптосистемы требуют меньших вычислительных ресурсов.

Актуальной научно-практической задачей является комбинированное использование симметричной и асимметричной систем шифрования в целях повышения криптостойкости шифра.

Предлагаем методику последовательного зашифрования открытого текста в симметричной криптосистеме (шифр Виженера) и асимметричной криптосистеме RSA. Зашифруем сообщение шифром Виженера, а зашифрованный текст еще раз зашифруем с помощью алгоритма RSA. Если криптоаналитик сумеет определить секретный ключ алгоритма RSA, то при расшифровании он получит текст, зашифрованный шифром Вижинера, а не открытое сообщение.

Например, зашифруем слово «ЭВМ» шифром Виженера с ключом 5 – 30 – 31. Это значит, что букву «Э» надо сдвинуть на 5 позиций вправо, букву «В» – на 30 позиций вправо, букву «М» – на 31 позицию вправо. В итоге получаем зашифрованное сообщение «ВАЛ». А затем зашифруем текст «ВАЛ» с помощью алгоритма RSA с параметрами: $p = 7$, $q = 13$, $n = p \cdot q = 91$, $e = 29$ – открытый ключ зашифрования, $d = 5$ – секретный ключ расшифрования. Для этого предварительно закодируем сообщение кодом 02 00 10. При зашифровании необходимо код символа возвести в степень, равную открытому ключу зашифрования $e = 29$, результат разделить на модуль $n = 91$ и остаток от деления будет являться кодом зашифрованного символа. В результате зашифрования по алгоритму RSA код 02 00 10 переходит в код 32 00 82.

При расшифровании необходимо код, соответствующий символу, возвести в степень, равную секретному ключу расшифрования $d = 5$, результат разделить на модуль $n = 91$ и остаток от деления будет являться кодом расшифрованного символа. В результате

получаем код 02 00 10, которому соответствует текст «ВАЛ». Затем необходимо выполнить второй этап расшифрования текста шифром Виженера с ключом 27 – 2 – 1. В результате получаем открытое сообщение, текст «ЭВМ».

Предложенный подход комплексного использования двух шифров позволяет в значительной мере усложнить криптоанализ.

Рассмотренная криптосистема реализована в виде компьютерной программы в среде EmbarcaderoRADStudio 2010 C++ Builder на языке C++.

Программа состоит из следующих модулей: MainFrm, RSA и Visenere.

В модуле MainFrm реализован пользовательский интерфейс: окна многострочного ввода текста, в которых отображается шифрованная и нешифрованная информация; элементы управления шифрованием/дешифрованием и текстовые элементы для отображения характеристик используемых алгоритмов; пункты меню для сохранения/загрузки шифрованного/нешифрованного текста из файла и настроек алгоритмов.

В модулях RSA и Visenere реализованы одноименные классы, инкапсулирующие методы алгоритмов шифрования RSA и Виженера соответственно, а также их ключи.

Шифрованию подвергается информация в кодировке Юникод: на каждый символ текста в этой кодировке отводится 2 байта (16 бит), что позволяет естественно разбивать текст на блоки для шифрования алгоритмом RSA и легко применять к тексту алгоритм Виженера (представив символ как число от 0 до 2^{16}).

В результате шифрования по методу RSA исходное сообщение переходит в числовые коды, которые представляется возможным отображать в графическом виде по кодировке Юникод.

В классе алгоритма Виженера в качестве ключа используется последовательность целых чисел. Для её хранения используется шаблон STLdeque , для которого предоставляются удобные функции доступа к элементам и их изменению. При этом пользователь может вводить ключ алгоритма в естественном виде – списке из чисел, разделенных запятыми.

В классе алгоритма RSA хранятся все основные данные: простые числа p и q, $n = pq$, открытый ключ зашифрования e и секрет-

ный ключ расшифрования *d*, а также дополнительные переменные для автоматической генерации ключей алгоритма. В программе предоставляется возможным устанавливать минимальную и максимальную границы, между которыми выберутся случайные числа для генерации алгоритма. При заданных *p* и *q* предоставляется возможным генерировать открытый ключ зашифрования и рассчитывать секретный ключ расшифрования. Для генерации случайных чисел используются встроенные функции, проверка на взаимно простые числа осуществляется методом перебора.

Для хранения настроек алгоритмов используется формат файла INI. В нем хранятся строковые переменные, полученные с помощью функций для экспорта характеристик алгоритмов. С помощью функций для импорта осуществляется процесс загрузки параметров алгоритмов из файла. Следует заметить, что файлы настроек такого открытого формата не претендуют на хранение ключей секретных данных и предназначены исключительно для личного пользования.

Для примера представим текст модуля Visenere, который реализует шифрование текста методом Виженера:

```
#include "Visenere.h"
#define MAX_WCHAR 65536
Visenere::Visenere(){
	setKeyByString("1,2,3");
}
Visenere::Visenere(String keystr){
	setKeyByString(keystr);
}
void Visenere::setKeyByString(String keystr){
	deque<int> temp;
	int sep;
	while (keystr!=""){
		sep = keystr.Pos(",");
		if (sep) {
			temp.push_back(keystr.SubString(1,sep-
1).ToInt());
			keystr.Delete(1,sep);
```

```
            } else {
                temp.push_back(keystr.ToInt());
                keystr = "";
            }
        }
        if (temp.size())
            key = temp;
}
String Visenere::getKeyOfString(){
        String res = "";
        for (UINT i = 0; i < key.size(); i++)
            res += String(key[i])+",";
        return res.Delete(res.Length(),1);
}
String Visenere::code(String str){
        String res = "";
        wchar_t c;
        for (int i = 1; i <= str.Length(); i++) {
            c = (str[i]+key[(i-1)%key.size()])%MAX_WCHAR;
            res += c;
        }
        return res;
}
String Visenere::decode(String str){
        String res = "";
        wchar_t c;
        for (int i = 1; i <= str.Length(); i++) {
            c = (str[i]-key[(i-1)%key.size()])%MAX_WCHAR;
            res += c;
        }
        return res;
}
String Visenere::getInfo(){
        return getKeyOfString();
}
```

Список литературы

1. Баричев С. Г., Гончаров В. В. , Серов Р. Е. Основы современной криптографии: учебный курс. – 3-е изд., стер. – М.: Горячая линия – Телеком, 2011. – 175 с.: ил.

2. Черчхауз Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет: [пер. с англ.]. – М.: Изд-во «Весь Мир», 2009. – 320 с.

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. – М. : ДМК Пресс, 2010. – 544 с. : ил.

4. Культин Н. Б. C++ Builder. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2008. – 464 с.: ил.

УДК 004.056

К.А. Тезик, Р.А. Приходько, Д.А. Гельплинг

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИЧЕСКИЕ ПОДХОДЫ К РАЗРАБОТКЕ КРИПТОГРАФИЧЕСКИ ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЙ БАЗ ДАННЫХ В СРЕДЕ DELPHI

Рассмотрены методические подходы к разработке приложения в среде Delphi, предназначенного для управления базой данных в СУБД Access по технологии ADO. Реализована криптографическая защита информации, содержащейся в базе данных, методом Виженера.

Анализ литературы [1, 2, 3] показывает, что методы криптографической защиты информации рассматриваются применительно к открытым сообщениям в виде текстов. Однако возникает актуальная научно-практическая задача шифрования не только текстов, но и информации, содержащейся в базах данных. Рассмотрим задачу криптографической защиты информации в базе данных, созданной в СУБД Access. Для примера рассматривается фрагмент базы данных по предметной области «Отдел кадров», который включает информацию о фамилии, имени и отчестве сотрудника.

Разработана программа в среде Delphi, предназначенная для просмотра и редактирования базы данных, поиска информации в базе данных, а также шифрования информации, содержащейся в базе данных методом Виженера.

Управление базой данных из программы в среде Delphi осуществляется по технологии ADO. Технология MicrosoftActiveXDataObjects (ADO) представляет собой универсальный механизм доступа к различным источникам данных из приложений баз

данных. При этом могут быть использованы данные из электронных таблиц, таблиц локальных и серверных баз данных, XML-файлов. В соответствии с терминологией ADO любой источник данных называют хранилищем данных. Приложение взаимодействует с хранилищем данных с помощью провайдера. Провайдер обеспечивает обращение к данным хранилища с запросами и передает результаты выполнения запросов приложению.

Для криптографической защиты информации, содержащейся в базе данных, используем шифр Виженера. В шифре Виженера буквы текста сдвигаются на переменную величину, зависящую от положения буквы в тексте. Данная система сдвигов задается с помощью списка чисел или ключевого слова. Например, зашифруем сообщение *WINDOWS* ключевым словом *TCP*. Это значит, что первую букву сообщения *W* мы сдвигаем на количество позиций, соответствующее коду буквы *T*, то есть на 19 позиций. Вторую букву сообщения *I* мы сдвигаем на количество позиций, соответствующее коду буквы *C*, то есть на 2 позиции. Третий символ сообщения *N* мы сдвигаем на количество позиций, соответствующее коду буквы *P*, то есть на 15 позиций. Следующие 3 символа открытого сообщения мы также сдвигаем на 19, на 2, на 15 позиций и т.д. При шифровании сообщения *WINDOWS* ключом *TCP* получается сообщение *PKCWQLL*.

Чтобы прочесть это сообщение, получатель должен воспользоваться ключом расшифрования, который получается из ключа зашифрования заменой каждого числа, соответствующего коду символа на его дополнение по модулю 26, где 26 – число букв в латинском алфавите. Ключ *TCP* в числовом выражении – 19-2-15. Следовательно, ключ расшифрования 7-24-11 или *HYL*.

Программа для управления базой данных и ее криптографической защиты шифром Виженера состоит из следующих модулей:

1. Модуль обзора, предназначенный для просмотра текущего состояния базы данных.

2. Модуль редактирования, предназначенный для внесения изменений в базу данных.

3. Модуль поиска, предназначенный для нахождения необходимой информации.

4. Модуль шифрования, предназначенный для кодирования информации.

5. Модуль дешифрования, предназначенный для декодирования информации.

Для реализации режима просмотра используются компоненты ADOConnection, ADOTable, DataSource, DBGrid. Компонент ADOConnection устанавливает соединение с хранилищем данных, компонет ADOTable используется для доступа к данным таблицы, компонеты DataSource и DBGrid – для отображения данных по форме. Поиск информации в базе данных по заданному значению поля «Фамилия» реализуется методом Locate. Данный метод осуществляет наиболее быстрый поиск и делает найденную запись текущей.

Для реализации криптографической защиты информация из каждой ячейки базы данных Access копируется в строку ввода компонента Edit, затем происходит шифрование, а получившаяся последовательность символов записывается в ту же ячейку базы данных.

Для обращения к ячейкам базы данных Access мы используем компонент ADOTable и функцию FieldByName, которая служит для обращения к конкретному полю. Таким образом осуществляется чтение открытого текста из базы данных Access и запись зашифрованной информации в поле Access.

Ключ Виженера вводится в строку компонента Edit в виде ключевого слова. При шифровании символа обращение к конкретному символу осуществляется по его номеру в строке.

По процедуре обработчика нажатия кнопки Button шифруется информация текущей строки базы данных Access. В качестве дальнейшего совершенствования программы можно рекомендовать шифрование всего файла базы данных во время выполнения процедуры шифрования.

Для примера приведем листинг модуля, предназначенного для шифрования и дешифрования данных.

Программа шифрования одной строки базы данных Access имеет следующий вид:

```
var alf,e,d,ke:string;  tab:array [1..66,1..66] of char; chr:array [1..255] of char;
 i,j,n,k,p,sr,sl,pr,c: Integer;
begin
edit2.text:=ADOTable1.FieldByName('Nam').AsString;
//Запись информации
                                    //из шифруемого поля в  строку edit
alf:='АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзийклмнопрстуфхцчшщъыьэюя';
k:=0;
fori := 1 to 66 do
begin n:=k+1;
for j := 1 to 66 do
 begin
 if n=67 then n:=1;
 tab[i,j]:=alf[n];  n:=n+1;
 end; k:=k+1;
 end;
e:=edit2.Text;
ke:=edit1.Text;   //Ввод ключа
p:=1;
if length(ke)<length(e) then
for i := 1 to (length(e)-length(ke)) do
begin
 ke:=ke+ke[i];
 end;
pr:=0; c:=1;
while pr=0 do
begin
sr:=pos(ke[c],alf);
sl:=pos(e[c],alf);
chr[c]:=tab[sr,sl];
 if c<length(ke) then c:=c+1
 else pr:=1;
end;
chr[c+1]:=#0;
```

```
d:=chr;
edit5.Text:=d;      //Получение зашифрованной информации
ADOTable1.Edit;
ADOTable1.Fields[2].AsString:=edit5.Text;   // Запись зашифро-
ванного поля в базу данных из строки Edit.
ADOTable1.Post;
```

Программа дешифрования одной строки базы данных Access имеет следующий вид:

```
var alf,e,d,ke:string;  tab:array [1..66,1..66] of char; chr:array
[1..255] of char;
  i,j,n,k,p,sr,sl,pr,c: Integer;
begin
edit2.text:=ADOTable1.FieldByName('Nam').AsString;//Запись
информации
                                        //из шифруемого поля в строку
                                edit
alf:='АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯаб
вгдеёжзийклмнопрстуфхцчшщъыьэюя';
k:=0;
fori := 1 to 66 do
begin n:=k+1;
for j := 1 to 66 do
 begin
 if n=67 then n:=1;
 tab[i,j]:=alf[n];  n:=n+1;
 end; k:=k+1;
 end;
 e:=edit2.Text;
 ke:=edit1.Text;   //Ввод ключа
 p:=1;
if length(ke)<length(e) then
for i := 1 to (length(e)-length(ke)) do
begin
 ke:=ke+ke[i];
end;
```

```
pr:=0; c:=1;
while pr=0 do
begin
sr:=pos(ke[c],alf);
 sl:=pos(e[c],alf);
g:=(sl-sr) mod 66;
chr[c]:=alf[g];
if c<length(ke) then c:=c+1
else pr:=1;
end;
chr[c+1]:=#0;
d:=chr;
edit5.Text:=d;      //Получение расшифрованной информации
ADOTable1.Edit;
ADOTable1.Fields[2].AsString:=edit5.Text;
//Запись расшифрованного поля
                                        // в базу данных из строки Edit
ADOTable1.Post;
```

Таким образом, реализована программа в среде Delphi, которая позволяет шифровать базу данных в СУБД Access методом Виженера. База данных будет храниться на жестком диске ЭВМ в зашифрованном виде. Прочитать информацию может только тот пользователь, который знает секретный ключ шифра Виженера.

Список литературы

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учебной курс. – 3-е изд., стер. – М.: Горячая линия – Телеком, 2011. – 175 с.: ил.

2. Черчхауз Р. Коды и шифры. Юлий Цезарь, «Энигма » и Интернет: [пер. с англ.]. – М.: Изд-во «Весь Мир», 2009. – 320 с.

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. – М. : ДМК Пресс, 2010. – 544 с. : ил.

4. Хомоненко А.Д., Гофман В.Э. Самоучитель Delphi. – 2-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2008. – 576 с.: ил.

УДК 004.056

Е.С. Волокитина

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ИДЕНТИФИКАЦИЯ НА ОСНОВЕ ЦИФРОВОГО МАРКИРОВАНИЯ

В настоящее время всё большую популярность приобретает идентификация человека с применением цифровых татуировок, наносимых на кожу. Приводится анализ существующих способов идентификации с применением цифровых кодов и вариантов их реализации нанесения.

Проблема идентификации человека является одной из ключевых проблем в области информационной и, в частности, компьютерной безопасности. Подтверждение, что человек является тем, за кого он себя выдает в разных ситуациях, таких как, при получении доступа в банке, почте или даже при доступе в помещения, где ограничен доступ, является очень важным.

В настоящее время системы строятся на вводе пароля или предъявлении внешней карточки-идентификатора, которые позволяют получить доступ к какой-либо системе. Однако существует много проблем, связанных с этим: злоумышленник может увидеть пароль при его вводе, а карточка может быть украдена. Именно поэтому возникла необходимость производить идентификацию так, чтобы устранить появившиеся недостатки.

Первые попытки для реализации татуировок как идентификатора при аутентификации человека уже сделаны.

Одним из первых применение чернил предложил Томас В. Хитер [1]. Он рассматривал вариант применения знака, который наносится в виде татуировки на человека. Представленный им метод служил для обеспечения торговых сделок электронными средствами. До того как торговая сделка может быть завершена, татуировка сканируется сканнером. Характеристики сканированной татуировки сравниваются с характеристиками других татуировок, накопленных в компьютерной базе данных, для того, чтобы верифицировать идентичность покупателя. Его изобретение относилось к применению невидимых, нестираемых татуировок на людях для целей идентификации для совершения финансовых операций безопасным способом.

В современное время сделаны опять попытки использовать временные татуировки. Так, например, Motorola решила воспользоваться разработками татуировки, называемой Biostamps, которая была разработана с целью отслеживания здоровья пациента, но Motorola считает, что технология может быть использована для проверки подлинности в качестве альтернативы традиционным паролям [2]. Biostamp можно вставить в тело, используя штамп, и носить в течение двух недель, и Motorola считает, что это делает его идеальным для целей аутентификации.

Однако на данный момент большинство специалистов говорят, что нанесение подобных татуировок на тело человека для аутентификации нас телефонами является неоправданным [3].

Метод идентификации и аутентификации человека с помощью татуировок заключается в нанесении татуировки на кожу человека. Татуировка может располагаться на любом подходящем месте человеческого тела и может быть как временной, так и постоянной, однако использование временной татуировки более предпочтительно, т.к. позволяет сменять её через заданные промежутки времени. Когда человек хочет совершить действие, требующее определения его или подтверждения его личности, татуировка подлежит сканированию сканнером. Далее возможно несколько вариантов: в татуировке может быть зашит ключевой идентификатор и при сканировании он сравнивается с базой идентификаторов системы. Если сканированное значение совпадает с идентификатором из базы данных, то личность считается идентифицированной и человек получает право совершить операцию. Также в татуировке может находиться не только идентификатор, но и ключевая информация, которая может наноситься в свернутом виде, например в виде штрих-кода.

В отличие от кредитной карты или идентификационных документов татуировка не может быть также легко потеряна или украдена.

Существует 2 вида штрих-кодов как способа кодирования информации: линейный и двухмерный.

Линейными называются штрих-коды, читаемые в одном направлении (по горизонтали). Наиболее распространённые линейные символики: EAN, UPC, Code56, Code128, Codabar и другие.

Линейные штрих-коды позволяют кодировать небольшой объём информации – до 20-30 символов, обычно цифр. Их удобнее применять в случае, если нам необходимо закодировать только идентификатор человека без дополнительной информации о нем.

Двухмерные штрих-коды могут применяться для кодирования большого объёма информации. Расшифровка такого кода проводится в двух измерениях (по горизонтали и по вертикали).

Двухмерные коды подразделяются на многоуровневые (stacked), которые представляют собой поставленные друг на друга несколько обычных линейных кодов и матричные (matrix), которые более плотно упаковывают информационные элементы по вертикали.

В качестве чернил может использоваться несколько их видов, в зависимости от того, хотим ли мы, чтобы сам факт наличия татуировки был виден. Если допустимо, чтобы татуировка была нанесена, то могут использоваться чернила для временных татуировок. Срок их использования от 1 до 10 дней. При этом необходимо правильно выбирать место нанесения: кожа должна быть не жирной и необходимо минимизировать трение с одеждой или телом. Иначе срок ношения такой татуировки снизится.

В случае если необходимо скрыть наличие татуировки для восприятия человеческим глазом, то удобно использовать средства невидимой маркировки, разработанные лабораториями прикладной химии для дактилоскопии [4]. После нанесения одного из видов средства невидимой маркировки, выбранного в зависимости от срока и условий использования, татуировка начинает ярко люминесцировать желтым, зеленым, голубым или синим цветом при облучении ультрафиолетовой лампой. Маркировка может быть устойчива к воде и солнечным лучам в течение суток, нескольких месяцев и даже до нескольких лет. Для удаления могут применяться высокие температуры (около 50 градусов) или органические растворители.

Сфера использования временных татуировок с нанесением штрих-кодов на кожу человека широка. Преимущества ее использования также очевидны: невозможность потерять идентификатор, легкая смена идентификатора и сложность его кражи. Такие татуировки могут содержать идентификатор для подтверждения личности человека или ключевую информацию о нем, в зависимости от

цели применения, могут быть видимыми или нет для человеческого глаза. Они могут наноситься на 1 день или на несколько лет.

Список литературы

1. Heeter Thomas W. Method for verifying human identity during electronic sale transactions. United States Patent, Appl. No. 709471, Filed: September 5, 1996.

2. The hi-tech tattoo that could replace ALL your passwords: Motorola reveals plans for ink and even pills to identify us [Electronic resource]. – URL: http://www.dailymail.co.uk/sciencetech/article-2333203/Moto-X-Motorola-reveals-plans-ink-pills-replace-ALL-passwords.html#ixzz2jhKmVWCe.

3. Смогут ли электронные татуировки заменить пароли в Интернете или другие формы идентификации? [Электронный ресурс]. – URL: http://anvictory.org/smogut-li-elektronnye-tatuirovki-zamenit-paroli-v-internete-ili-drugie-formy-identifikacii/ (дата обращения: 30.10.2013).

4. Средства невидимой маркировки [Электронный ресурс]. – URL: http://www.cobra.net.ua/catalog/sredstva-nevidimoj-markirovki.html (дата обращения: 03.11.2013).

УДК 004.3

Е.Ю. Дорошенко

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

УМНОЖИТЕЛЬ ЧИСЕЛ В ТРОИЧНОЙ СИММЕТРИЧНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

В статье предложена структурная схема и алгоритм работы устройства для умножения чисел в троичной симметричной системе счисления.

Известно, что троичная система является более емкой в сравнении с двоичной с точки зрения плотности записи информации. Однако область аппаратного обеспечения для проектирования вычислительных устройств на основе троичной логики не является развитой. В данной статье представлена структурная схема и алгоритм работы умножителя чисел в троичной симметричной системе счисления.

Структурная схема устройства представлена на рис. 1. Основным функциональным блоком является блок управления. Он формирует сигналы переключения мультиплексора, разрешения записи в регистры и их обнуления, обеспечивая работу устройства согласно приведенному ниже алгоритму.

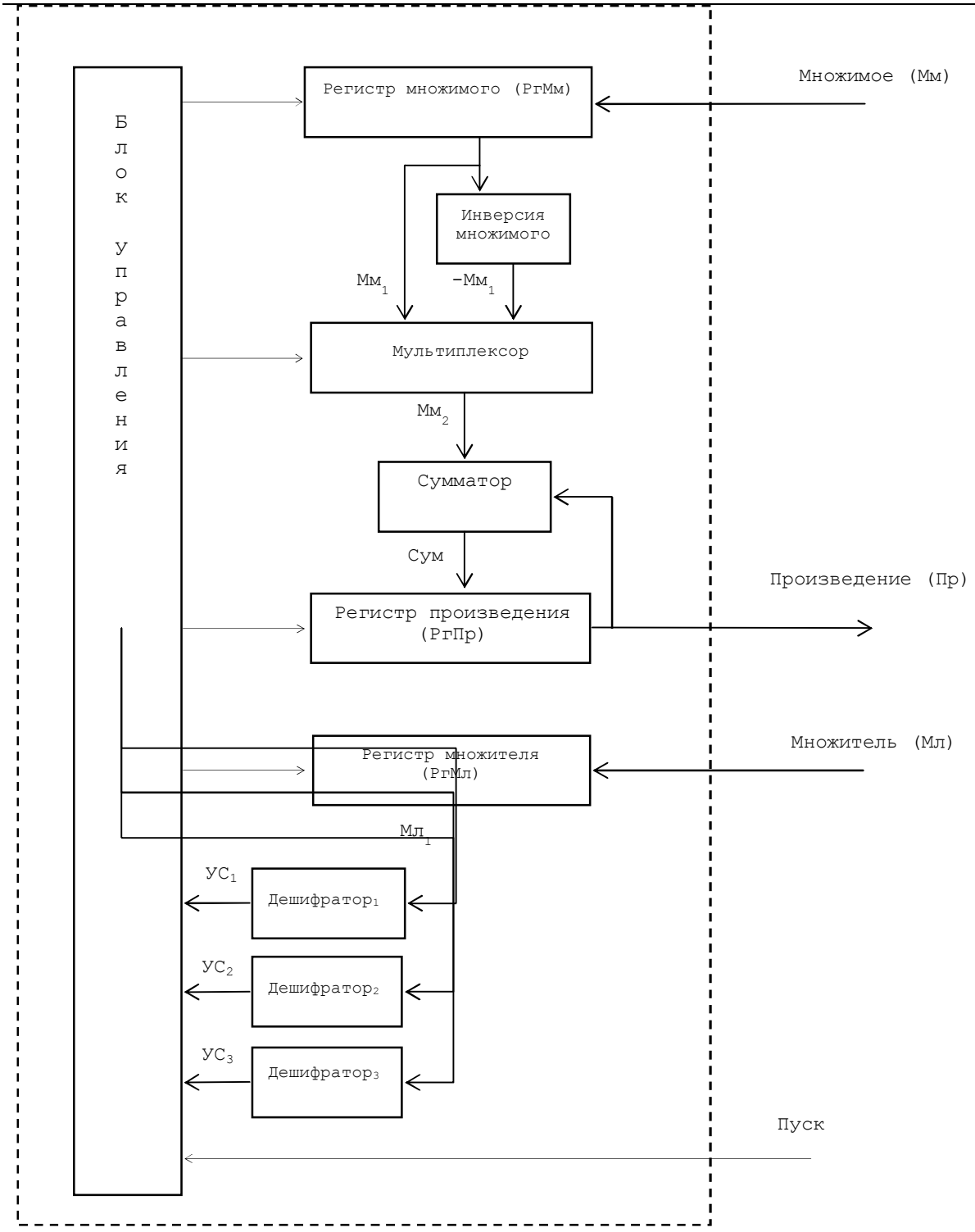


Рис. 1. Структурная схема устройства

Блок-схема алгоритма приведена на рис. 2.
Блок 1 является начальным блоком алгоритма.

В блоке 2 анализируется состояние управляющего сигнала ПУСК. Если сигнал имеет единичное значение, то происходит переход на блок 3 алгоритма, иначе происходит возврат ко 2-му блоку.

В блоке 3 происходит запись нулевого значения в регистр произведения.

В блоке 4 происходит запись значения множимого в регистр множимого.

В блоке 5 происходит запись значения множителя в регистр множителя.

В блоке 6 анализируется управляющий сигнал $УС_1$, принимающий единичное значение в случае, когда число в регистре множителя равно нулю. В этой ситуации происходит переход на блок 15 алгоритма, иначе – на блок 7.

В блоке 7 анализируется управляющий сигнал $УС_2$, принимающий единичное значение в случае, если младший троичный разряд числа в регистре множителя равен плюс единице. В этой ситуации происходит переход на блок 8 алгоритма, иначе – на блок 9.

В блоке 8 алгоритма сигналу $Мм_2$ присваивается значение $Мм_1$. Затем происходит переход на блок 10 алгоритма.

В блоке 9 сигналу $Мм_2$ присваивается значение-$Мм_1$.

В блоке 10 сигналу СУМ присваивается значение суммы троичных чисел, представленных сигналами $Мм_2$ и $Пр_1$.

В блоке 11 анализируется управляющий сигнал $УС_3$, принимающий единичное значение в случае, если младший троичный разряд числа в регистре множителя не равен нулю. В этой ситуации происходит переход на блок 12 алгоритма, иначе – на блок 13.

В блоке 12 в регистр произведения записывается значение сигнала СУМ. Затем происходит переход на блок 13 алгоритма.

В блоке 13 происходит сдвиг числа в регистре множимого на один троичный разряд влево.

В блоке 14 происходит сдвиг числа в регистре множителя на один троичный разряд вправо. Затем происходит переход на блок 6 алгоритма.

Блок 15 является конечным блоком алгоритма.

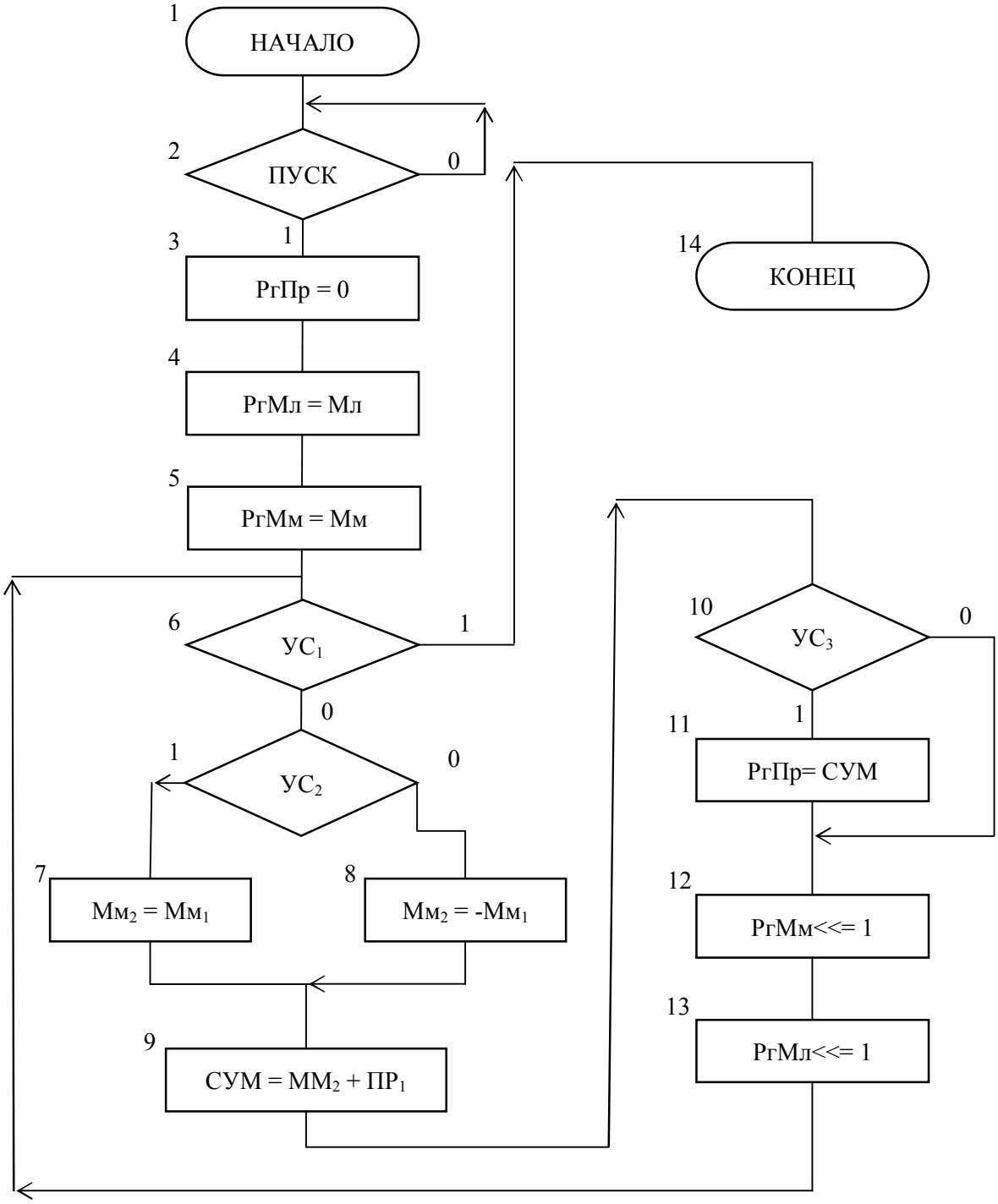


Рис. 2. Блок-схема алгоритма работы устройства

Результатом исследования является разработанная структурная схема устройства. Приведенная выше архитектура может быть использована при построении троичной ЭВМ и при проектировании аналогичных троичных устройств.

1. Савельев А.Я. Прикладная теория цифровых автоматов: учеб. для вузов по специальности ЭВМ. – М.: Высш. шк., 1987. – 272 с.: ил.

2. Стрыгин В.В., Щарев Л.С. Основы вычислительной, микропроцессорной техники и программирования: – М.: Высш. шк., 1989. – 479 с.: ил.

УДК 681.3

С.С. Шевелев

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АЛГОРИТМ РАБОТЫ УСТРОЙСТВА ВЫПОЛНЕНИЯ ЛОГИЧЕСКИХ ОПЕРАЦИЙ

Устройство выполнения логических операций реализует булевы функции: конъюнкцию, дизъюнкцию, инверсию, исключающее ИЛИ. Это устройство может быть выполнено в виде отдельного модуля.

Устройство выполнения логических операций разработано как специализированный модуль, который позволяет выполнить основные логические операции [1]. Задачи этого класса характеризуются большими объемами сложных структур данных и высокой степенью асинхронного распараллеливания. Процесс вычисления логических функций представлен в циклической организации выполнения операций.

Увеличение быстродействия и экономия памяти являются основными критериями оценки качества алгоритма [2]. В цифровом модуле имеется собственное достаточно большое по емкости оперативное запоминающее устройство, предназначенное для хранения результатов вычислений. Независимость ветвей обработки данных позволит увеличить быстродействие вычислительного процесса.

Блок-схема алгоритма работы устройства выполнения логических операций представлена на рисунке.

Блок 1 алгоритма является начальным. В блоке 2 алгоритма происходит установка сигнала – пуск в единичное значение ПУСК:=1. По этой команде все блоки устройства получают команду начало работы. В блоке 3 алгоритма по команде СУПi:=1 происходит подача единичных значений на управляющие входы логических схем И для отпирания соответствующих электронных клю-

чей. Количество управляющих сигналов СУПi зависит от числа введенных переменных в блоке управления. По команде БПРi:=ЗПР каждой булевой переменной присваивается значение, равное нулевому или единичному уровню. В блоке 4 алгоритма анализируется признак работы устройства – сигнал РУС. Если устройство работает – выход ДА блока, то при этом осуществляется переход на блок 5 алгоритма. Если работа устройства завершена – выход НЕТ блока, осуществляется переход на конечный блок 17 алгоритма. Блоки 5, 6 и 7 образуют цикл, в котором определяется количество переменных, а также присваиваются значения булевым переменным. В блоке 5 алгоритма проверяется признак выполнения устройством логической операции конъюнкции КОН. Если устройство выполняет другую логическую функцию – выход НЕТ блока, то осуществляется переход на блок 8 алгоритма. Если выполняется логическая операция конъюнкция – выход ДА, то осуществляется переход на блок 6 алгоритма. В блоке 6 алгоритма по команде КОНi:=(ЗПРi) ИЛИ (РБОi) происходит подача результата логической операции ИЛИ значений переменных ЗПР или результата выполнения другими блоками устройства сигнал РБО. В блоке 7 алгоритма по команде РБО:=БКОН выходная шина устройства РБО принимает значение операции конъюнкции с выхода блока 2 конъюнкторов. В блоке 8 алгоритма проверяется признак выполнения устройством логической операции дизъюнкции (ИЛИ) – ДИЗ. Если устройство выполняет другую функцию – выход НЕТ блока, то осуществляется переход на блок 11 алгоритма. Если устройством выполняется логическая операция дизъюнкция (ИЛИ) – выход ДА, то осуществляется переход на блок 9 алгоритма.

В блоке 9 алгоритма по команде ДИЗi:=(ЗПРi) ИЛИ (РБОi) происходит подача результата логической операции дизъюнкции значений переменных ЗПР или результата выполнения другими блоками устройства сигнал РБО. В блоке 10 алгоритма по команде РБО:=БДИЗ выходной информационный сигнал устройства РБО принимает значение операции дизъюнкции с выхода блока 3 дизъюнкторов. В блоке 11 алгоритма проверяется признак выполнения устройством логической операции исключающее ИЛИ – ИИЛИ. Если устройство выполняет другую функцию – выход НЕТ блока, то осуществляется переход на блок 14 алгоритма.

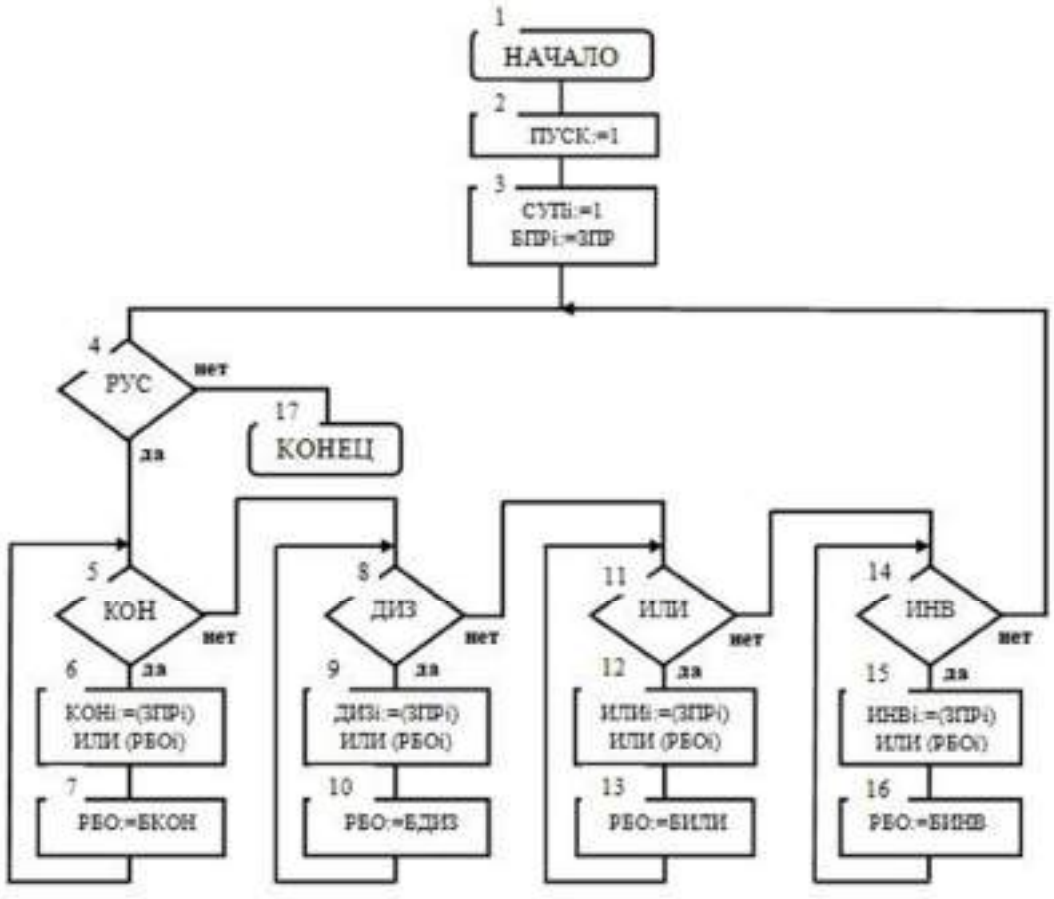


Рис. Блок-схема алгоритма работы устройства выполнения логических операций

Если устройство выполняет логическую функцию исключающее ИЛИ – выход ДА, то осуществляется переход на блок 12 алгоритма. В блоке 12 алгоритма по команде ИЛИi:=(ЗПРi) ИЛИ (РБОi) происходит подача результата логической операции исключающее ИЛИ значений переменных ЗПР или результата выполнения другими блоками устройства. В блоке 13 алгоритма по команде РБО:=БИЛИ выходной информационный сигнал устройства РБО принимает полученный результат операции исключающее ИЛИ с выхода блока 4 операции исключающее ИЛИ. В блоке 14 алгоритма проверяется признак выполнения устройством логической операции инверсии (НЕ) ИНВ. Если устройство выполняет другую функцию – выход НЕТ блока, то осуществляется переход на блок 4 алгоритма. Если выполняется логическая операция инверсия (НЕ) – выход ДА, то осуществляется переход на блок 15 алгоритма. В блоке 15 алгоритма по команде ИНВi:=(ЗПРi) ИЛИ (РБОi) происходит подача результата логической операции ИЛИ

значений переменных ЗПР или результата выполнения другими блоками устройства сигнал РБО. В блоке 16 алгоритма по команде РБО:=БИНВ выходная шина устройства РБО принимает значение операции инверсии с выхода блока 5 инверторов устройства. По выходе этого блока осуществляется переход на блок 14 алгоритма. Блок 17 алгоритма является конечным [3].

Вычислительные специализированные процессоры не менее чем на порядок дешевле равномощного универсального устройства. Представленное устройство может решать только определенный круг задач, выполнять специализированные вычисления, оно имеет собственное запоминающее устройство. Устройство выполнения логических операций можно использовать в вычислительной системе, которое состоит из специализированных модулей, объединенных через единый интерфейс.

Список литературы

1. Самофалов К.Г., Романкевич А.М., Валуйский В.Н. Прикладная теория цифровых автоматов. – Киев: Высш. шк., 1987. – 374 с. : ил.

2. Комарцова Л. Г., Максимов А. В. Нейрокомпьютеры. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – С. 320.

3. Пат. 2288500 Рос. Федерация. Устройство выполнения логических операций / Шевелев С.С., Кобелев Н.С., Лопин В.Н., Кобелев В.Н., Шевелева Е.С., Фетисова Е.В.; заявитель и патентообладатель Юго-Зап. гос. ун-т. – №2005118723/09; заявл. 16.06.2005; опубл. 27.11.2006, Бюл. №33.

УДК 681.3

С.С. Шевелев, Хла Вин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

УСТРОЙСТВО ВЫПОЛНЕНИЯ ЛОГИЧЕСКИХ ОПЕРАЦИЙ

Разработано устройство выполнения логических операций. В блоках устройства выполняются логические операции: конъюнкция (И), дизъюнкция (ИЛИ), отрицание (НЕ), исключающее ИЛИ.

Существуют системы булевых функций, с помощью которых можно аналитически представить любую сколь угодно сложную булеву функцию. Функционально полной системой булевых функций называется совокупность таких булевых функций f1, f2, … , fn, что произвольная булева функция может быть записана в виде

формы через функции этой совокупности. Свойство некоторого набора функций выражать через себя любую функцию называется свойством полноты этого набора. Такой полный набор называют логическим базисом. Функционально полными называют наборы логических элементов, пользуясь которыми можно реализовать любую двоичную функцию. Любая булева функция может быть представлена аналитически одной из нормальных форм: дизъюнктивной и конъюнктивной. Для этих форм такими функциями являются: конъюнкция, дизъюнкция, отрицание (инверсия). К функционально полной системой булевых функций следует отнести системы: конъюнкция (&), дизъюнкция (V), инверсия (НЕ), исключающее ИЛИ [1].

Свойство полноты функции позволяет выпускать ограниченный набор логических элементов, из которых можно строить любые логические схемы [2].

Устройство выполнения логических операций выполняет логические операции конъюнкцию (И), дизъюнкцию (ИЛИ), отрицание (НЕ), исключающее ИЛИ. В устройстве выполнения логических операций последовательность выполнения булевых функций определяется установкой управляющих сигналов на входах электронных ключей в единичное состояние. Тем самым отпираются соответствующие ключи, при этом значения переменных и ранее полученные результаты других блоков поступают на входы очередного блока устройства.

Устройство выполнения логических операций (рис.) содержит: систему электронных ключей СЭКУ, блок конъюнкторов БКОН, блок дизъюнкторов БДИЗ, блок операции исключающее ИЛИ БИЛИ, блок инверторов БИНВ, электронные ключи конъюнкторов ЭККН служат для разрешения передачи переменных в блок конъюнкторов, электронные ключи дизъюнкторов ЭКДЗ предназначены для разрешения передачи переменных в блок дизъюнкторов, электронные ключи операции исключающее ИЛИ ЭКИЛИ выполняют функцию разрешения передачи переменных в блок операции исключающее ИЛИ, электронные ключи инверторов ЭКИН предназначены для разрешения передачи переменных в блок инверторов, блок хранения результатов БХР служит для записи и хранения в нем результатов выполнения логических операций,

блок управления БУ служит для генерации управляющих сигналов устройства.

Работа устройства выполнения логических операций заключается в следующем.

Блок 1 система электронных ключей устройства СЭКУ содержит систему логических элементов И с тремя высоко идемпотентными состояниями. Этот блок служит для разрешения подачи переменных и управляющих сигналов на входы блоков устройства. На вход системы электронных ключей поступают информационные сигналы управления и значения булевых переменные. Булевы переменные поступают на одни из входов пороговых элементов. На вторые входы поступают сигналы управления. При единичных значениях сигналов управления на выходах пороговых элементов будут генерироваться значения булевых переменных. Если сигналы управления равны нулевым значениям, то соответствующие логические схемы И блока будут заперты, что формирует режим отключения этих элементов от других блоков устройства.

Блок 2 конъюнкторов БКОН содержит $\boldsymbol{m}$ пороговых элементов, он служит для выполнения логической операции И. Входным сигналом блока является информационный сигнал КОН, который поступает с выхода блока ЭККН – электронные ключи конъюнкторов. Блок конъюнкторов имеет пирамидальную структуру. Входы $a_1 \ldots a_{3m}$ поступают на входы пороговых элементов. Выходным сигналом блока конъюнкторов является результат конъюнкции.

Блок 3 дизъюнкторов БДИЗ содержит $\boldsymbol{k}$ пороговых элементов. Этот блок служит для выполнения логической операции ИЛИ Входным сигналом блока является информационный сигнал ДИЗ, который поступает с выхода блока ЭКДЗ – электронные ключи дизъюнкторов. Блок дизъюнкторов имеет пирамидальную структуру. Входы $b_1 \ldots b_{3k}$ поступают на входы пороговых элементов. Выходным сигналом блока 3 дизъюнкторов является результат дизъюнкции.

Блок 4 исключающее ИЛИ – БИЛИ содержит $\boldsymbol{f}$ нейронов, он предназначен для выполнения логической операции исключающее ИЛИ. Входным сигналом блока является информационный сигнал ИЛИ, который поступает с выхода блока ЭКИЛИ – электронные ключи операции исключающее ИЛИ. Блок исключающее ИЛИ

имеет пирамидальную структуру. Входы c_1 … c_{w+1} поступают на входы нейронов. Выходы этих нейронов поступают на входы последнего нейрона. Выходным сигналом блока БИЛИ является результат выполнения операции исключающее ИЛИ.

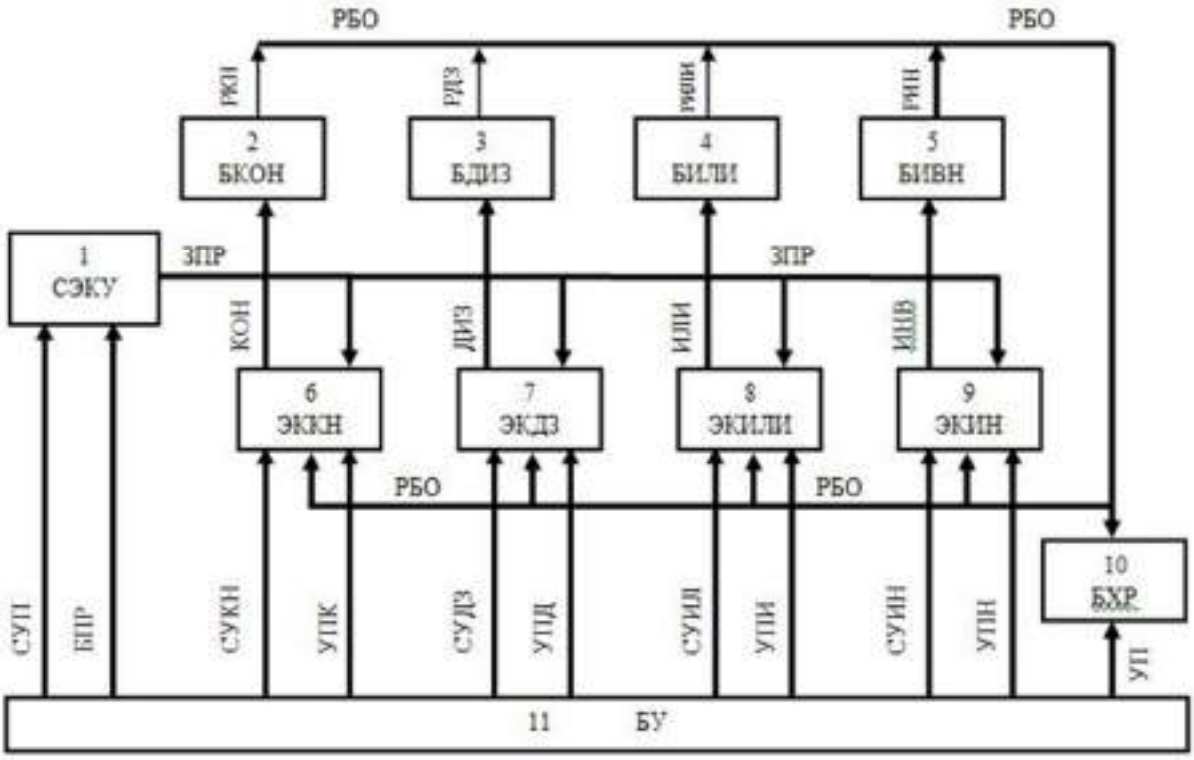


Рис. Структурная схема устройства выполнения логических операции

Блок 5 инверторов БИНВ содержит систему логических элементов НЕ – инверторов, выполненных на пороговых элементах. Этот блок служит для получения инверсных состояний входных переменных. Входным сигналом блока является информационный сигнал ИНВ, поступающий с выхода блока ЭКИН – электронные ключи инверторов. Каждая переменная поступает на вход соответствующего инвертора. Выходным сигналом блока инверторов является информационный сигнал, инверсный по отношению к входному.

Блоки 6,7, 8 и 9 ЭККН, ЭКДЗ, ЭКИЛИ и ЭКИН электронные ключи конъюнкторов, дизъюнкторов, операции исключающее ИЛИ, инверторов соответственно: содержат по две системы логических элементов И и по одной системе логических элементов ИЛИ, построенных на пороговых элементах. На управляющие вхо-

ды этих электронных ключей поступают сигналы управления работой логических элементов. На информационные входы первых систем поступают значения булевых переменных. На информационные входы вторых системы логических элементов И поступают результаты выполнения логических операций других блоков. На управляющие входы этих систем поступают сигналы, управляющие работой электронных ключей. Выходные сигналы с логических элементов И систем поступают на входы дизъюнкторов.

Блок 10 хранения результатов БХР содержит оперативное запоминающее устройство, двоичные счетчики, формирующие адреса столбцов и строк. Для формирования адресов строк и столбцов на входы счетчиков поступают прямоугольные импульсы. По этим адресам будут записаны результаты логических операций, которые поступают на вход оперативного запоминающего устройства. Сигналы управления оперативного запоминающего устройства выбора кристалла и считывания/записи соответственно при записи принимают нулевые значения [3].

Устройство выполнения логических операций разработано как специализированный модуль, который позволяет выполнить основные логические операции. Специализированные вычислительные модули эффективно решают задачи обработки и сортировки массивов, упорядочения данных, распределения ресурсов между локализованными центрами, ускоренное выполнение арифметических и логических операций.

Список литературы

1. Угрюмов Е. П. Цифровая схемотехника. – СПб.: БХВ – Санкт-Петербург, 2000. – 528 с.: ил.

2. Хорошевский В.Г. Архитектура вычислительных систем. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 520 с.

3. Пат. 2288500 Рос. Федерация. Устройство выполнения логических операций / Шевелев С.С., Кобелев Н.С., Лопин В.Н., Кобелев В.Н., Шевелева Е.С., Фетисова Е.В.; заявитель и патентообладатель Юго-Зап. гос. ун-т; – №2005118723/09; заявл. 16.06.2005; опубл. 27.11.2006, Бюл. №33.

УДК 621.395.4

Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА ДЕСКРИПТОРА ДАННЫХ ПО СТАТИЧЕСКОМУ СЛОВАРЮ ХАФФМАНА

Представлена алгоритмическая последовательность дескрипции формата статического Deflate.

Рассмотрим методику декодирования статического Deflate (первый и второй бит первого байта блока – 01). В данном случае набор символов в словаре строго определен и не меняется в различных блоках. Размер и диапазон кодов для набора литералов алфавита и длин повторов представлены в таблице.

Литерал	Размер в битах	Диапазон кодов
0 – 143	8	00110000 – 10111111
144 – 255	9	110010000 – 111111111
256 – 279	7	0000000 – 0010111
280 – 285	8	11000000 – 11000111

Например, код 0000000 принадлежит диапазону 0000000–0010111, является символом 256 и означает конец блока.

Все коды литералов находятся друг за другом (см. табл.), коды символов следуют в обратном порядке. Для нахождения истинных литералов в диапазоне 00110000–10111111 необходимо из найденного кода Хаффмана вычесть 00110000, в диапазоне 110010000–111111111 из найденного кода вычесть 100000000. Коды для дистанций переводятся в десятичное счисление и вычисляются. Окончанием блока всегда является литера 256.

Отметим, что коды Хаффмана расположены последовательно ортогонально и лексикографически, т.е. установление каждого последующего бита, начиная со старшего, однозначно определяет размер и диапазон литералов. Например, считывание первых двух битов – 00 означает возможную длину кода 7 или 8, третий однозначно определяет длину и диапазон. Данное свойство присуще всей логике нахождения кодов словарей Хаффмана (в т.ч. и динамического).

Методику восстановления исходных байтов можно представить следующим образом:

1. Чтение первых двух бит.

2. Если 00, то это диапазоны литералов 0-143 или 256-279. Если 11, то это диапазоны 144-255 или 280-285. Переход к пункту 3:

а) если следующий бит 0, то это семибитный код диапазона 256-279. Это диапазон длин повторов. Читать 7 бит. Найти значение по формуле 256 + {7 бит}. Определить количество дополнительных бит. Считать дополнительные биты. Определить длину повтора. Если это литерал 256, закончить обработку блока – выход. Если не 256, то считать 5 бит для дистанции в обратном порядке. Определить количество дополнительных бит. Читать дополнительные биты дистанций. Вычислить дистанцию. Отсчитать дистанцию от последнего найденного байта влево, копировать число байтов, равное длине повтора, вставить содержимое в конец вслед за последним найденным;

б) если следующий бит 1, то это восьмибитный код диапазона 0-143. Определить исходный байт по формуле {8 бит} – 00110000.

3. Если 11, то это диапазоны литералов 144-255 или 280-285. Читать следующий бит:

а) если бит равен 0, то это девятибитный диапазон 110010000–110011111. Читать 9 бит. Вычислить исходный байт по формуле {9 бит} – 100000000;

б) если бит равен 1, то это восьмибитный диапазон 11000000–11000111. Это литерал длины повтора. Читать 8 бит. Определить количество дополнительных бит по таблице. Читать дополнительные биты. Определить длину. Читать 5 бит для дистанции. Определить дополнительные количество бит для дистанции по таблице. Читать дополнительные биты. Вычислить дистанцию. Отсчитать дистанцию от последнего найденного байта влево, копировать число байтов, равное длине повтора, вставить содержимо в конец вслед за последним найденным.

4. Повторить пункт 1.

Таким образом, алгоритм дескриптора является цикличным, условием выхода из которого становится код 0000000.

---

1. Deutsch P. GZIP file format specification version 4.3 [Electronic resourse]. – URL: http://ftp.uu.net/graphics/png/documents /zlib/zdoc-index.html.

УДК 621.395.4

Е.А. Шиленков

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОПРЕДЕЛЕНИЕ ДЕСКРИПТОРА И ФОРМАТА СЛОВАРЯ СЖАТЫХ ДАННЫХ

Изложена методика определения служебных бит смещений и длин повторов для словарей Хаффмана в формате Deflate.

Рассмотрим начальные байты для блоков Deflate. Первый байт блока всегда имеет следующую битовую структуру:

№ бита	7	6	5	4	3	2	1	0
Значение 1	-	-	-	-	-	0	1	0
Значение 2	-	-	-	-	-	1	0	0
Значение 3	-	-	-	-	-	0	1	1
Значение 4	-	-	-	-	-	1	0	1

Нулевой бит указывает на конечный блок: если он равен 0, то блок не конечный, и после следующего разделителя имеются еще блоки; если 1, то блок последний. Первый и второй биты устанавливают тип используемого словаря: статический – 01 и динамический – 10. В случае если первый и второй биты равны 00, сжатия нет, если они – 11, то данный байт не принадлежит блоку Deflate.

Рассмотрим условия дескриптора Deflate со сжатием (второй и третий бит первого байта 01 или 10).Следует отметить, что все комбинации бит символов дерева Хаффмана, применяемого в Deflate, записаны в обратном порядке: младший бит слева, старший справа. Символ может быть расположен внутри двух смежных байтов (табл. 1).

Таблица 1

Формат байтов в кодах Хаффмана

№ байта блока	байт N								байт N+1							
№ бита	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
№ бита по Хаффману	3	4	5	6	7	0	1	2	4	5	6	7	8	0	1	2
№ символа	символ M					символ M-1			символ M+1					символ M		

Начиная с третьего бита первого байта, происходит восстановление символа по Хаффману. Основной особенностью работы данного алгоритма является выявление повторяющихся последовательностей, начиная с трех байт, и замена их на комбинацию «длина + дистанция». Длина есть количество повторяющихся символов, идущих друг за другом, а дистанция – число символов, которое необходимо побайтно отсчитать назад до начала повтора.

К полному набору из 256 литералов (в одном байте восемь бит, следовательно, весь возможный алфавит равен 256) добавлены комбинации длин повторов (257-285) (табл. 2).

Таблица 2

Соответствие литерала длине повтора

Code	Extra Bits	Length(s)	Code	Extra Bits	Length(s)	Code	Extra Bits	Length(s)
257	0	3	267	1	15,16	277	4	67–82
258	0	4	268	1	17,18	278	4	83–98
259	0	5	269	2	19–22	279	4	99–114
260	0	6	270	2	23–26	280	4	115–130
261	0	7	271	2	27–30	281	5	131–162
262	0	8	272	2	31–34	282	5	163–194
263	0	9	273	3	35–42	283	5	195–226
264	0	10	274	3	43–50	284	5	227–257
265	1	11,12	275	3	51–58	285	0	258
266	1	13,14	276	3	59–66			

Символы 257-264 однозначно определяют длину повторяющихся байтов. Начиная с 265-го, необходимо учитывать дополнительные биты (Extrabits), которые идут побитно. Например, для символа 266 дополнительный бит 0 определит длину повтора 13. Символ 256 означает конец блока. Максимальная длина повторяющихся символов – 256 байт. После появления кодов длин повторов и их возможных дополнительных бит следуют коды для дистанций (табл. 3).

Символы 0-3 однозначно определяют дистанции. В остальных случаях появляются дополнительные биты, точно задающие дистанции, например для девятого символа дополнительные биты 111 определят длину дистанции 32.

Таблица 3

Соответствие кода дистанции повтора

Code	Extra Bits	Distance	Code	Extra Bits	Distance	Code	Extra Bits	Distance
0	0	1	10	4	33–48	20	9	1025–1536
1	0	2	11	4	49–64	21	9	1537–2048
2	0	3	12	5	65–96	22	10	2049–3072
3	0	4	13	5	97–128	23	10	3073–4096
4	1	5,6	14	6	129–192	24	11	4097–6144
5	1	7,8	15	6	193–256	25	11	6145–8192
6	2	9–12	16	7	257–384	26	12	8193–12288
7	2	13–16	17	7	385–512	27	12	12289–16384
8	3	17–24	18	8	513–768	28	13	16385–24576
9	3	25–32	19	8	769–1024	29	13	24577–32768

Представленные таблицы соответствия литералов/длин и дистанций актуальны для статического и динамического словарей Deflate.

---

1. Deutsch P. GZIP file format specification version 4.3 [Electronic resourse]. – URL: http://ftp.uu.net/graphics/png/documents /zlib/zdoc-index.html.

УДК 004.633.2

А.С. Якушев, Д.Н. Караколючка, М.В. Алешечкин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

КЛАССИФИКАЦИЯ ФОРМАТОВ ФАЙЛОВ ДЛЯ ЗАДАЧ СЕЛЕКЦИИ ДОКУМЕНТОВ

Рассмотрены основные форматы файлов, произведена их классификация по признаковым и содержательным составляющим, производится описание методов распознавания различных типов файлов.

Задача подготовки представленной из Интернета коллекции документов и файлов для более детальной селекции в рамках персональной поисковой системы заключается в методиках определения содержимого файлов, т.е. в определении и присвоении к определенному классу различной информации, содержащейся внутри документа. Для каждого типа данных необходим свой способ выявления, обработки и анализа содержимого. Поэтому основная за-

дача в селекции и обработке документов заключается в способах определения содержательной части документа, для чего на первых этапах необходимо определение формата файла. Определив формат файла, возможно частично уменьшить цикл обработки внутреннего содержания файла путем откидывания процедур, не относящихся к данному типу файлов.

Для того чтобы правильно работать с файлами, программы должны иметь возможность определять их тип. По историческим причинам в разных операционных системах используются разные подходы для решения этой задачи. Для дальнейшей классификации форматов файлов необходимо дать определение файла. Файл – это логический блок информации, определенный в соответствии с требованиями используемой в ОС файловой системы и представленный в одном из допустимых форматов, определяемых программой, в которой образован данный блок информации, размещенный в оперативной памяти компьютера либо на одном из допустимых в ОС носителей информации и снабженный атрибутами, необходимыми для его поиска, считывания и записи средствами операционной системы [1]. Также для решения поставленной выше задачи необходимы знания форматов и их классификаций. Формат – спецификация структуры данных, записанных в компьютерном файле. Формат файла иногда указывается в его имени как часть, отделённая точкой (обычно эту часть называют расширением имени файла, хотя, строго говоря, это неверно). Например, окончание имени (расширение) «.txt» обычно используют для обозначения файлов, содержащих только текстовую информацию, а «.doc» – содержащих текстовую информацию, структурированную в соответствии со стандартами программы Microsoft Word. Файлы, содержимое которых соответствует одному формату (реже – одному семейству форматов), иногда называют файлами одного типа.

Тип файла – это информация для быстрой идентификации содержимого файла операционной системой и пользователем без необходимости считывания всего содержимого файла. Благодаря этой информации пользователь приблизительно знает тип содержащейся информации в файле, а в операционной системе может быть сопоставлена программа для обработки файлов данного типа.

Общепринятая в вычислительной технике концепция файла – неструктурированная последовательность байтов. Компьютерные

программы, сохраняющие в файлах структурированные данные, должны как-то преобразовывать их в последовательность байтов и наоборот.

Различные форматы файлов могут различаться степенью детализации, один формат может быть «надстройкой» над другим или использовать элементы других форматов. Например, текстовый формат накладывает только самые общие ограничения на структуру данных. Формат HTML устанавливает дополнительные правила на внутреннее устройство файла, но при этом любой HTML-файл является в то же время текстовым файлом.

Определение типа файла может производиться по следующим критериям:

- Спецификации.

Для многих форматов файлов существуют опубликованные спецификации, в которых подробно описана структура файлов данного формата, то, как программы должны кодировать данные для записи в этот формат и как декодировать их при чтении.

- Расширение имени файла.

Некоторые операционные системы, например CP/M, DOS и Microsoft Windows, используют для определения типа файла часть его имени, т. е. «расширение имени файла». В старых операционных системах это были три символа, отделённые от имени файла точкой (в файловых системах семейства FAT имя и расширение хранились отдельно, точка добавлялась уже на уровне ОС); в более новых системах расширение может являться просто частью имени, и тогда его длина ограничена только неиспользованной длиной имени.

- Магические числа.

Другой способ, широко используемый в UNIX-подобных операционных системах, заключается в том, чтобы сохранить в самом файле некое «магическое число» – последовательность символов, по которой может быть опознан формат файла.

- Метаданные.

Некоторые файловые системы позволяют сохранять дополнительные атрибуты для каждого файла, т. е. «метаданные». Эти метаданные можно использовать для хранения информации о типе файла. Недостатком этого метода является плохая переносимость,

т.к. при копировании файлов между файловыми системами разных типов метаданные могут быть потеряны.

Типы данных, определённые стандартом MIME, широко используются в различных сетевых протоколах, однако в файловых системах они пока применяются редко.

Классификация файлов – это распределение файлов по группам в зависимости от того, какая информация в них заложена.

Файлы бывают следующих видов:

– текстовые файлы (doc, docx, docm, dox и др.);
– видеофайлы (avi, avp, mpeg, mpeg4, zmv и др.);
– аудиофайлы (mp1, mp2, mp3, mxl, nki и др.);
– музыкальные файлы (amz, vpl);
– растровые изображения (001, 73i, pc1, omf и др.);
– векторные изображения (abc, cdmt, cdd, gsd и др.);
– файлы таблиц (ast, bks, wks и др.);
–файлы игр (555, ai, nv, omod и др.);
– системные файлы (aos, ann, mod, msc и др.);
– файлы БД (4dd, maf, accde и др.);
– сжатые файлы (rar, bz, zip, zi и др.);
– исполняемые файлы (exe, ex4, esh и др.);
– файлы разработчиков (mlb, mxml, magik и др.);
– файлы образов (2mg, adf, iso и др.);
– резервные копии (113, mddata, mpb и др.);
– CAD-файлы (123, igs, ipj и др.);
– файлы данных (1pe, mpx, mpz и др.);
– GIS файлы (3d, jpr, lan и др.);
– файлы 3D-изображений (mc5, mdd, mesh и др.);
– файлы разметки документа (4ui, mdi, mft и др.);
– файлы плагинов (mat, mda, mfx, nbm и др.);
– Web-файлы (mvr, ap, nzb и др.);
– файлы шрифтов (abf, mf, pfr, txt и др.);
– закодированные файлы (hex, mim, rdi и др.);
– прочие файлы (mgo, mmo, mrk и др.) [2].

Проведя классификацию форматов файлов, было замечено, что расширения файлов для разных типов файлов могут совпадать.

Также замечено, что в определенных типах файлов может содержаться информация из других типов (например, «.doc»; данное расширение показывает нам, что это текстовый документ. Но во

внутреннем содержании может быть и графическая информация, и информация, введенная с помощью MathType, и многое другое). Факт совпадения названий расширений для разных типов файлов и факт содержания в документе информации, не соответствующей типу расширения, может привести к сбоям и ошибкам при классификации форматов файла, что, в свою очередь, отрицательно скажется в последующей обработке и приведению файла к универсальному виду. Также есть возможность свободного изменения расширения файлов, что имеет две стороны: положительную и отрицательную. С одной стороны, возможность изменения расширения позволяет открыть файл при помощи схожих программ, работающих с другим расширением. Но с точки зрения улучшения информационного поиска это может привести к ухудшению или вовсе неправильному ответу на поисковый запрос пользователя. Так как по формату файла, сохраненного под одним расширением, поисковая машина будет делать вывод о принадлежности данного файла к соответствующей группе и, соответственно, производить дальнейшую обработку и преобразования с целью универсализации файлов, а данный файл будет относиться к другой группе, для которой требуются другие методы универсализации.

Распределение форматов по группам и классам позволит нам воспользоваться уже имеющимися преобразователями в универсальный код. Например, для текстовых документов разработан стандарт юникод (Unicode) – стандарт кодирования символов, позволяющий представить знаки почти всех письменных языков. Данный стандарт позволяет произвести перекодировку в универсальный вид файлов, содержащих символы, заложенные в базу программы. Для приведения к универсальному виду других типов файлов необходимы также программные средства, производящие конвертирование в универсальный вид. Идеальным случаем является одно программное средство, которое позволяет производить преобразование всех типов файлов в универсальный вид.

---

1. Первый социальный словарь [Электронный ресурс]. – URL: http://webotvet.ru/.

2. База расширений файлов [Электронный ресурс]. – URL: http://www.filetypes.ru.

СЕКЦИЯ 4
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ И ОБЪЕКТОВ

УДК 81.93.29

А.С. Алисов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АУТЕНТИФИКАЦИЯ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Показан принцип двухфакторной аутентификации.

Современные тенденции развития социотехнических систем во многом связаны с массовым внедрением механизмов удаленного взаимодействия пользователя и центра предоставления услуг, и это неудивительно, ведь мы живем в эру бурного развития ИТ-сферы и интернет-технологий, в эру, когда люди стараются затратить минимум времени для достижения желаемого эффекта. Банки пользуются всеми доступными возможностями для привлечения клиентов, и стоит отметить, что услуги, предоставляемые системами дистанционного обслуживания, востребованы как у крупных компаний, так и у физических лиц. Однако не стоит забывать, что речь в данном случае идет о счетах и банковских картах, а также операциях по ним, следовательно, такая информация должна быть надежно защищена и доступна только клиенту банка.

Для получения возможности совершать или искажать транзакции от лица законного держателя банковского счета, а именно к этому в основном и стремятся злоумышленники, используются методы и схемы, позволяющие каким-либо образом получить доступ к данным клиента, его идентификаторам, паролям – это фишинг, социальная инженерия, подставные сайты, кей-логгеры и т.д. Таким образом, необходимо предусмотреть надежный механизм аутентификации, сбалансированный по требованиям защищенности, удобству использования и оправдывающий финансовые вложения.

В настоящее время и изначально использовались следующие методы аутентификации:

– классический способ, основанный на том, что клиент знает: аутентификация по логину и паролю (однофакторная аутентифи-

кация). В этом случае для получения доступа к интернет-банку пользователь вводит логин и пароль, которые передаются на сервер банка. Сервер сверяет полученную информацию с хранимыми записями, и, если запись найдена и совпадает, пользователь получает доступ. Суть данного способа заключается в том, что и пользователь, и владелец сервера должны знать пароль пользователя;

– способ аутентификации, основанный на том, что пользователь имеет (например, пластиковая карта, электронный цифровой сертификат или токен);

– многофакторная аутентификация.

Существуют также методы биометрической аутентификации, не нашедшие применения в системах ДБО российских банков.

Понятно, что классический способ является примером слабой аутентификации, поэтому для обеспечения должного уровня защищенности применяется ряд дополнительных мер:

– введение лимита на количество попыток входа в систему; как правило, после трех неудачных попыток ввода пароля возможность входа пользователя в систему временно блокируется, либо для разблокировки пользователю необходимо обратиться в отделение банка с удостоверяющими его личность документами;

– ограничение срока действия пароля;

– уведомление клиента через sms-сервисы о совершенных транзакциях, о входе в личный кабинет с указанием ip-адреса и/или других параметров устройства, с которого осуществлялся вход.

Для усложнения задачи вычисления пары логин/пароль путем простого перебора используется так называемый тест «капча» (Captcha).

Примечание: CAPTCHA (от англ. Completely Automated Public Turing test to tell Computers and Humans Apart – полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) – компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером.

Более надежный метод – многофакторная аутентификация. В данном случае кроме своего логина и пароля клиенту необходимо ввести также дополнительный сеансовый код, который может быть получен различными способами: в виде sms-сообщения на номер

мобильного, указанного при регистрации клиента в банке без возможности изменения номера со стороны клиента; в виде пластиковой карты, выданной в офисе банка, на которую нанесены коды под защитным слоем или бумажной ленты, а также такие коды могут быть сгенерированы специальным устройством типа OTP-токен (one time password (от англ.) – одноразовый пароль). Здесь возможны варианты, когда на каждое действие, будь то вход в личный кабинет или подтверждение операции, требуется ввод OTP-кода, в иных случаях OTP-код требуется только при входе в систему.

На сегодняшний день на российском рынке представлено многообразие средств для реализации механизма многофакторной аутентификации различного уровня защищенности. Например, ОАО «Российский Сельскохозяйственный банк» (Россельхозбанк) – один из крупнейших банков РФ, 100% акций которого находятся в собственности государства, предоставляет своим клиентам два вида систем ДБО – «Банк-Клиент» и «Интернет-Клиент». Основным отличием этих систем является способ предоставления услуги. «Банк-Клиент» – специальное программное обеспечение, установленное на рабочей станции Клиента. При этом вся информация хранится локально. «Банк-Клиент» периодически связывается с Банком (через сеть Интернет или посредством телефонной линии), обмениваясь с ним данными. «Интернет-Клиент» подразумевает под собой работу с Банком через сеть Интернет посредством веб-браузера на сайте Банка, при этом информация не хранится на рабочей станции Клиента.

В первом случае на компьютер пользователя устанавливается клиентское приложение, использующее электронно-цифровую подпись для обеспечения защищенности обмена данными. Во втором случае на руки клиенту выдается OTP-токен. Например, OTP-токен Digipass 810 фирмы VASCO, выполненный в виде беспроводного устройства с небольшим экраном, клавиатурой и картридером. Наличие картридера и клавиатуры предусматривает использование смарт-карты и ввод пин-кода, что повышает уровень защиты. В качестве сервера аутентификации используется также продукт фирмы VASCO – контроллер VACMAN, интегрируемый в уже существующую информационную систему. VACMAN в автоматическом режиме обрабатывает поступающие запросы со скоро-

стью до 9000 запросов в секунду, обеспечивая доступ к сервисам банка только корректно авторизованным пользователям.

Взаимодействие клиента с сервером происходит следующим образом:

– клиент вводит аутентификационные данные на сайте и отправляет запрос на доступ к своей странице интернет-банка, в том числе сгенерированный при помощи digipass OTP-код;.

– с сайта аутентификационная информация передается на проверку серверу аутентификации VACMAN;

– VACMAN выполняет проверку подлинности аутентификационной информации и возвращает результаты проверки приложению, и в случае успешного прохождения процедуры аутентификации пользователь получает доступ к своей странице в интернет-банке.

Принцип двухфакторной аутентификации, реализованный в данном случае на платформе криптосервера VACMAN, представляется довольно гибким решением, поддерживающим в зависимости от конфигурации большое количество механизмов аутентификации: PKI-карты, цифровые сертификаты, USB-токены, аутентификация с использованием мобильного телефона. Разнообразие производителей, представляющих сегодня достаточно широкий спектр механизмов аутентификации для систем ДБО, позволяет найти индивидуальный подход к каждому клиенту, учитывающий его требования к защищенности, удобству использования и стоимости предоставляемых услуг.

---

1. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей Authentication: From Passwords to Public Keys First Edition. – М.: Вильямс, 2002. – С. 432.

УДК 81.93.29

А.С. Алисов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ FLASH-НАКОПИТЕЛЯ

Показаны различные варианты использования flash-накопителя.

Методы аутентификации с применением аппаратных средств основаны на том, что человек для прохождения известной процедуры обязан иметь при себе некий специальный предмет, без которого удачный исход данной процедуры невозможен. Такой механизм аутентификации известен уже очень давно, и, наверное, наиболее распространенным его представителем сегодня является механический замок с ключом. Характерные черты компьютерной аутентификации такие же, как и в случае с замком: ключ содержит в себе базовую секретную информацию – совокупность пропилов, борозд и уникальный номер, который выступает в роли имени пользователя и свзявыет конкретный замок с конкретным ключом. Зная конфигурацию ключа, можно сделать его дубликат, зная устройство замка, ключ можно подобрать, кроме того, ключ можно забыть дома или просто-напросто потерять.

Для того чтобы система аутентификации обеспечивала необходимый уровень защищенности, необходимо использование надежных паролей большой длины с включением заглавных и прописных букв, цифр, других символов из таблицы ASCII или даже включение символов из нескольких алфавитов. Это представляет некоторые сложности, люди записывают пароль в блокнот или вовсе клеят листок с паролем на рамку монитора, в результате таких действий механизм аутентификации теряет весь свой смысл. Вместе с тем, по результатам исследования, опубликованных журналом "Information Security/ Информационная безопасность", подавляющее большинство респондентов полагают, что утечка персональных данных может серьезно навредить тому, чьи данные оказались скомпрометированы в результате инцидента, – так считают 77,2% опрошенных. Всего лишь 18,6% опрошенных полагают, что утечка персональных данных, скорее всего, не может навредить. Затруднились ответить 4,2% респондентов.

Поэтому в качестве достойной альтернативы обычной парольной аутентификации механизм аутентификации с использование flash-накопителя будет интересен как для рядовых пользователей, так и для представителей малого и среднего бизнеса.

Использование программно-аппратного средства для доступа к ПК снимает с пользователя задачу придумывания и запоминания

сложного пароля, позволяет не вводить пароль вручную при каждом входе в систему.

Молдавская компания Tesline-Service S.R.L. занимается разработкой программного обеспечения Rohos, позволяющего использовать стандартный flash-накопитель в качестве аутентификатора для входа в систему или доступа к защищенному хранилищу. После записи на flash-накопитель программы-клиента и ее настройки функциональность носителя данных не утрачивается. Флэшку можно дополнительно защитить PIN-кодом на случай кражи или утери, дубликат такого USB-ключа невозможно изготовить путем простого копирования данныхю. Кроме того, USB-ключ может быть привязан к конкретному компъютеру, где он был создан. Все это, конечно же, не ставит каких-то нерешаемых задач по взлому для подготовленного злоумышленника, и система аутентификации с использованием flash-накопителя уступает по показателям защищенности смарт-картам и OTP-токенам. Однако простота в использовании, дешивизна внедрения, немалый ряд сопутствующих полезных функций являются несомненными преимуществами данного метода многофакторной аутентификации.

Итак, если речь идет о безопасности в большой компании, которая готова потратить деньги на специализированные устройства, какими являются смарт-карты и USB-токены, то именно они будут наилучшим выбором. При этом важно помнить, что понадобится еще и специалист для их настройки и обслуживания.

Если же цель состоит в том, чтобы ограничить доступ к информации на личном компьютере или повысить надежность паролей в офисе, то вариантом, оправдывающим требуемые финансовые вложения, будет использование flash-накопителя в качестве аутентификатора.

---

1. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей Authentication: From Passwords to Public Keys First Edition. – М.: Вильямс, 2002. – С. 432.

УДК 004.056.55

А.Ю. Блинов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРОТОКОЛ SSL И БЕЗОПАСНОСТЬ ЕГО ИСПОЛЬЗОВАНИЯ

В данной статье рассматривается протокол SSL и изучены проблемы его практического применения. Актуальность данной тематики обусловлена наличием проблемы передачи конфиденциальной информации по открытым каналам.

Вопросы безопасности информации, ее сохранности и защищенности её передачи по каналам связи являются наиболее волнительными в наш век развитых информационных технологий. Безопасность канала связи зависит не только от протокола защиты, но и от его реализации в конкретной системе. О таком методе и пойдет далее речь.

SSL является криптографическим протоколом, разработанным для проверки подлинности и шифрования сетевого подключения. Данный протокол обеспечивает невозможность перехвата и изменения данных, отправляемых и получаемых через сеть.

Безопасность в протоколе достигается путем организации защищенного канала, в котором реализуется полное шифрование всех входящих и исходящих сообщений, и при этом серверная сторона всегда аутентифицирована, пользовательская сторона аутентификацию производит в зависимости от настроек. Надежность канала достигается путем проверки целостности передаваемых данных с привлечением MAC (message authentication code).

При реализации протокола в приложении SSL используется поверх любого другого протокола транспортного уровня, инкапсулируя в себе протоколы приложений, такие как HTTP, FTP, XMPP и SMTP. Для каждого инкапсулированного протокола обеспечиваются условия для их функционирования уже после аутентификации и шифрования канала между клиентом и сервером. Также следует учесть, что поверх SSL могут накладываться и другие протоколы. Данную особенность можно использовать для усиления защищенности канала. Примером может служить использование SSL совместно с VPN .

При обнаружении ошибки в протоколе SSL предусмотрена процедура ее обработки путем извещения партнера той стороной, что обнаружила ошибку, и попыткой ее разрешить до разрыва соединения.

Среди плюсов данного протокола есть и минусы. Так как SSL невозможно использовать отдельно от программных средств, то именно ошибки при реализации протокола могут стать наиболее уязвимым местом защиты, но в таком случае ответственность за это лежит на разработчике приложения, а не на самом протоколе, что заставляет с особой тщательностью проверять программный код при разработке.

Еще одним слабым местом протокола является зависимость SSL от различных криптографических параметров. Шифрование RSA служит только для пересылки сессионных ключей и аутентификации сервера и клиента, а последующий обмен информацией уже ведется с помощью высокопроизводительных симметричных шифров. Таким образом, если используемые симметричные шифры могут быть подвергнуты атаке и данная атака будет успешна, то SSL-соединение уже не может считаться защищенным.

Против протокола SSL может быть предпринят ряд атак, однако SSL будет устойчив к ним при условии, что в процессе обмена используются только доверенные серверы для обработки информации. Сервер должен иметь подписанный сертификата, а клиент обязан проверить сертификат сервера.

Протокол SSL является эффективным решением проблемы защиты пользовательских данных при их распространении по открытым каналам связи. Но без соответствующей практической реализации, в которой будут предусмотрены возможные проблемы, связанные с SSL, данный протокол не способен обеспечить должный уровень защищенности конфиденциальных данных, а также может являться источником повышенной уязвимости системы обмена данными.

---

1. Семенов Ю.А. Протокол SSL. Безопасный уровень соединителей. – М., 2000. – 26с.

УДК 658.512.011.56:004.42+621.391

М.Ю. Рытов, В.А. Воронин

ФГБОУ ВПО «Брянский государственный технический университет»

АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОТ УТЕЧКИ ИНФОРМАЦИИ В РЕЧЕВОЙ ФОРМЕ

В статье рассмотрена автоматизированная система, которая позволяет моделировать различные варианты систем защиты речевой информации.

Несмотря на значительно возросшую роль автоматизированных информационных систем (АИС), речевая информация в потоках сообщений по-прежнему носит превалирующий характер (до 80% всего потока) [1]. Вследствие этого защита речевой информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта. В основном деятельность по защите речевой информации направлена на постановку акустической и виброакустической помехи или усиления акусто-непроницаемости помещения.

В современных системах оценки защиты речевой информации происходит только анализ уже имеющейся системы защиты, т.к. нет возможности подобрать средства защиты без их предварительной установки. Данные факты приводят к тому, что при построении системы защиты она получается излишне дорогой и имеет ряд недостатков, связанных с наличием посторонних шумов в зачищаемом помещении.

Эти проблемы частично можно разрешить с помощью применения автоматизированной системы проектирования комплексной защиты речевой информации объекта информатизации с возможностями создания модели помещения и анализа элементов защиты путем внесения в данную модель характеристик разных элементов.

На данный момент в процессе построения системы защиты объекта информатизации от утечки по акустическому и виброакустическому каналам можно выделить следующие основные этапы:

– сбор данных об объекте информатизации (помещении) и анализ объекта;

– определение каналов утечки информации (далее КУИ) и их характеристик;

– определение состава средств защиты речевой информации;

– введение в эксплуатацию средств защиты в комплексе.

Существуют различные программно-аппаратные комплексы, предназначенные для решения задачи оценки акустозащищенности объекта информатизации, все они схожи в принципах функционирования. Рассмотрим основные принципы их работы на примере комплекса «Спрут-мини».

При работе с данным комплексом сбор данных и их анализ осуществляется квалифицированным оператором. На основе анализа данных определяются возможные КУИ и производится инструментальная оценка акустозащищенности. Принимая во внимание выявленные КУИ, на основе инструкции по эксплуатации комплекса определяются контрольные точки.

С использованием аппаратуры комплекса осуществляется измерение показателей сигнала и шума в октавных полосах частот, результатом измерения являются уровни сигнала и шума в децибелах (дБ). На основе полученных данных программно-аппаратный комплекс «Спрут-мини» производит расчет показателей защищенности объекта информатизации, показатели заносятся в отчет, предоставляемый оператору. На данном шаге завершается работа комплекса.

Используются следующие основные методы и методики, применяемые для получения показателей защищенность.

Метод ***парциальных отношений сигнал-шум***. Основным недостатком данного метода являются значительные затруднения, если требуется обеспечить некий минимальный уровень защиты, при котором разрешается, например, словесная разборчивость 5% или 10%, при этом невозможно установить предмет ведущегося разговора [2].

Боле перспективной группой методов являются так называемые ***формантные методы*** разборчивости речи. При рассмотрении формантных методов можно выявить определенную несогласованность в них, причинами которых являются ошибки при сопоставлении различных коэффициентов восприятия [1]. В работе [1] по-

казано, что наиболее корректна методика М.А. Сапожкова, хотя и требуются доработки.

Из вышесказанного можно сделать вывод, что существующие подходы к построению системы защиты речевой информации обладают рядом недостатков:

– отсутствие автоматизации сбора информации на подготовительном этапе;

– используемые методы либо узко применимы, либо не совсем корректны;

– отсутствие автоматизированных процедур проектирования системы защиты от утечки речевой информации.

Разрешение данных проблем возможно при использовании автоматизированной системы защиты акустической информации АСЗАИ (рис).

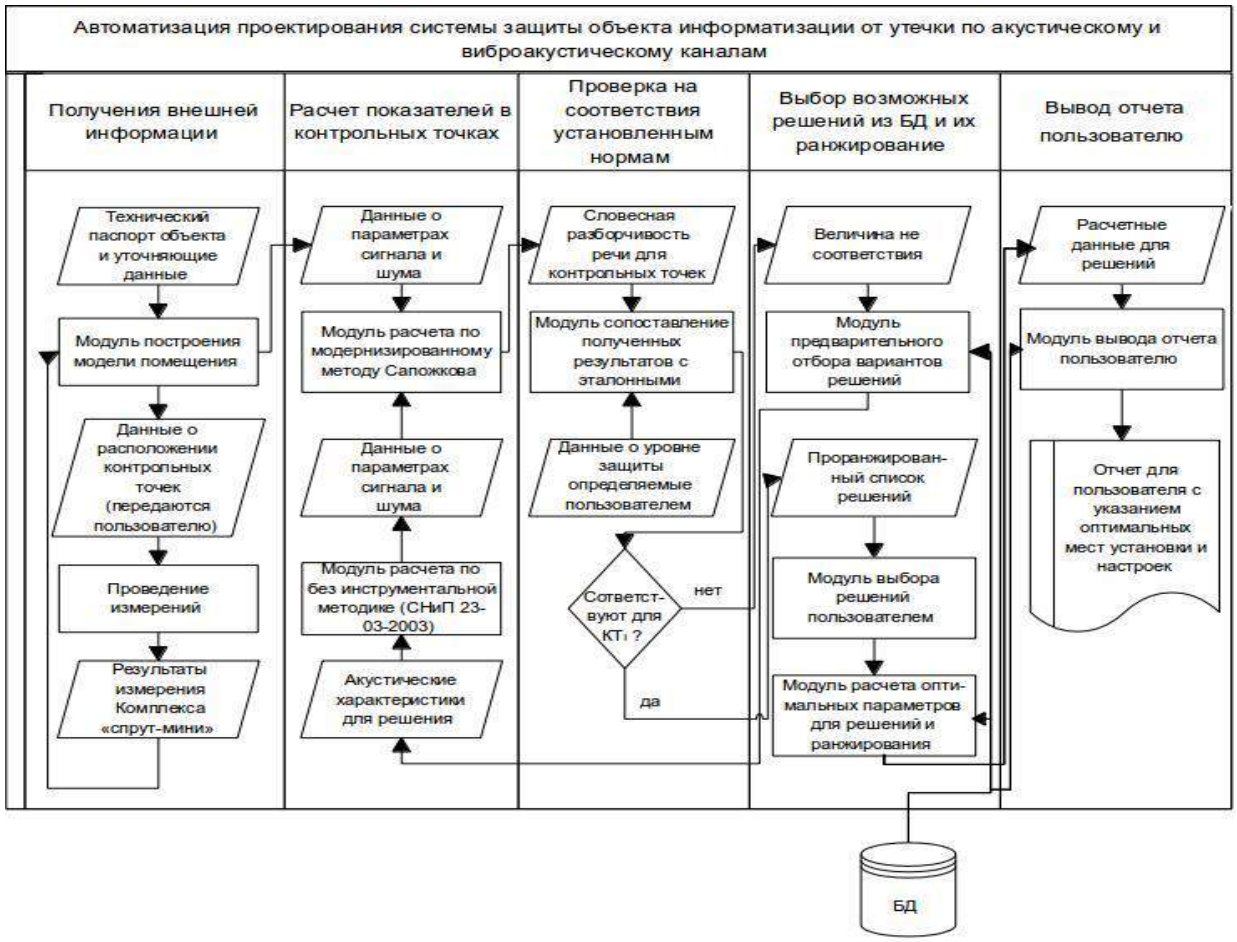


Рис. Структурно-функциональная схема программного комплекса

Комплекс АСЗАИ работает следующим образом. Для получения внешней информации и построения модели помещения оператору необходимо предать системе информацию о конструктивных особенностях помещения, нуждающегося в защите. Далее на основании переданых данных программный комплекс выстраивает модель помещения и выделяет ключевые объекты, для которых характерно образование КУИ. Для этих объектов на основании нормативных документов создается инструкция по проведению измерений. Данные проведенных измерений из комплекса «Спрут-мини» также заносятся в модель помещения.

В результате получается модель, отображающая структуру защищаемого объекта, а также занесенные в нее контрольные точки для расчета уровня сигнала и шума. Расчет показателей в контрольных точках осуществляется при помощи форматной методики разборчивости речи, которая основывается на модернизированном методе Сапожкова с использованием семейства новых коэффициентов восприятия.

В результате работы комплекса АСЗАИ генерируется отчет, включающий в себя оценку состояния защищенности речевой информации на объекте информатизации в виде уровней словесной разборчивости речи в контрольных точках, а также рекомендации по установке и настройке средств защиты речевой информации.

Список литературы

1. Топоровский П. Защита речевой информации: проблемы и решения // Защита информации. Конфидент. – 2001. – № 4. – С. 12.

2. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Спецтехника. – 2000. – № 4. – С. 17-19.

3. СНиП 23-03-2003. Санитарные нормы и правила. Защита от шума. – Введ. 2004–01–01. – М.: ГУП ЦПП, 2004. – 43 с.

4. Дидковский В.С., Дидковская М.В., Продеус А.Н. Акустическая экспертиза каналов речевой коммуникации: монография. – Киев: Имэкс-ЛТД, 2008. – 420 с.

УДК 519.8:004.056

М.Ю. Рытов, О.М. Голембиовская, А.П. Горлов

ФГБОУ ВПО «Брянский государственный технический университет»

ПРОЕКТИРОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛИЗИРОВАННОЙ ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ САПР

В статье рассмотрена автоматизация процесса проектирования КСЗИ путем создания специализированной объектно-ориентированной САПР.

Широкое использование в процессе информатизации общества современных методов и средств обработки информации создало не только объективные предпосылки повышения эффективности всех видов деятельности личности, общества и государства, но и ряд проблем защиты информации, обеспечивающей требуемое ее качество. Сложность решения этой проблемы обусловлена необходимостью создания целостной системы комплексной защиты информации, базирующейся на стройной её организации и регулярном управлении. Комплексная система защиты информации – это организационно-техническая система, в которой действуют в единой совокупности правовые, организационные, технические, программно-аппаратные и другие нормы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки.

Понятие защиты информации в настоящее время ассоциируется, как правило, с проблемами обеспечения информационной безопасности в автоматизированных системах обработки данных (АСОД). Информатизация социально-экономических и политических процессов современного общества обусловливает развитие и всестороннее использование автоматизированных систем, предназначенных для организации хранения, пополнения и предоставления информации в соответствии с запросами пользователей, во всех аспектах деятельности человечества.

Рассматривая концептуальную модель процесса защиты информации [1], становится очевидным, что защита информации – динамический процесс.

Чем совершеннее современные способы несанкционированного доступа и более реальны источники угроз, тем более актуальным ставится проблема создания необходимого рубежа защиты информации. В то же время, чем грамотнее выбраны и реализованы направления и способы защиты, тем дальше отходят угрозы от защищаемой информации. Рубеж защиты «плавает» во времени в зависимости от тех или иных вышеназванных факторов.

Таким образом, проектировать (разрабатывать заново или в большинстве случаев, как показывает практика, модифицировать существующую) комплексную систему защиты информации (КСЗИ) следует для конкретного момента времени, объективно оценивая положение рубежа защиты. В целях обеспечения соответствия КСЗИ современному уровню обеспечения безопасности и для снижения трудоемкости, обеспечения качества проектных решений, а главное, сокращения сроков её проектирования целесообразно применять специализированные системы автоматизированного проектирования (САПР). В настоящее время задача автоматизации проектирования КСЗИ зачастую сводится к обработке экспертных данных с выдачей решений общего рекомендательного характера [2].

На основе анализа накопленного опыта по исследованию и практической разработке автоматизированных систем проектирования сложных технических машиностроительных объектов, специализированных объектно-ориентированных САПР, САПР технологических процессов [3] была предложена концепция построения специализированной САПР КСЗИ [4].

При создании САПР КСЗИ была реализована следующая структурно-функциональная схема, представленная на рисунке.

На начальных этапах проектирования происходит получение модели объекта защиты, в основу которой положено структурирование информации, обрабатываемой в АСОД, и определение характеристик процесса проектирования, определяется категория АСОД и виды обрабатываемой информации, возможные людские, материальные и финансовые ограничения КСЗИ, технические характеристики объектов. Далее выполняется моделирование возможных угроз информации в АСОД и ранжирование их.

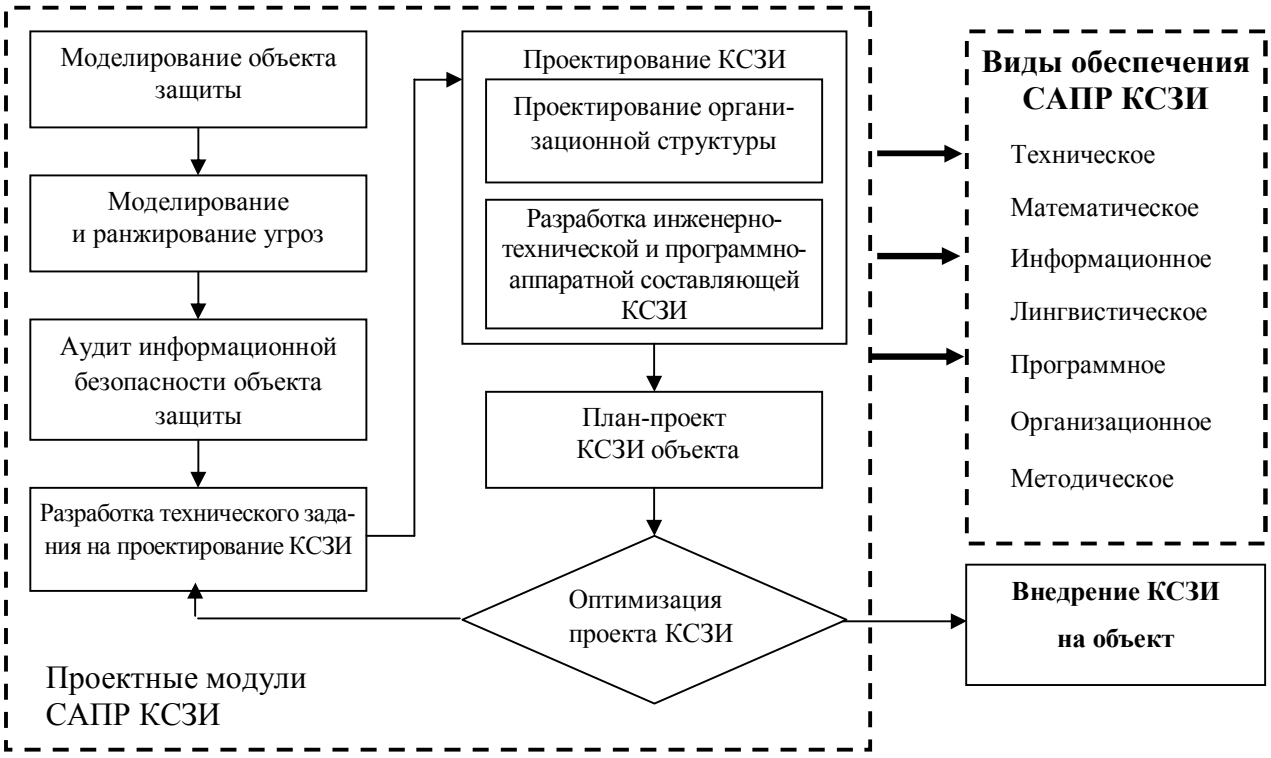


Рис. Структурно-функциональная модель САПР КСЗИ

На следующем этапе осуществляется аудит информационной безопасности АСОД на основе требований международных стандартов по информационной безопасности и нормативных документов Российской Федерации. В ходе проведения аудита проводится анализ используемой на защищаемом объекте информации, определяются её виды, степень конфиденциальности, ценность, актуальность и важность и выявляются виды угроз, которым может быть подвергнута защищаемая АСОД, и возможные каналы утечки информации.

В результате проведения аудита информационной безопасности АСОД происходит оценка эффективности действующей системы защиты информации и принимается решение о направлениях её модернизации или разработки принципиально новой модели КСЗИ. Результатом этого этапа является техническое задание (ТЗ) на проектирование КСЗИ для системы обработки данных.

Далее, в соответствие с ТЗ, выполняется выбор методов и средств, разрабатываются способы защиты информации и соответствующие организационные структуры, которые объединяются в единую совокупность КСЗИ, обеспечивающую защиту инфор-

мации от потенциально возможных и выявленных в ходе аудита угроз и каналов утечки. Затем производится оптимизация разработанного плана КСЗИ и в случае необходимости выполняется его корректировка.

Для построения математической модели выбора средств защиты информации АСОД была использована модель с полным перекрытием Клементса-Хофмана [4]. Данная модель позволяет оценить защищенность информационной системы, рассчитать затраты на построение системы защиты, а также определить оптимальный вариант построения системы информационной безопасности.

Результатом работы САПР КСЗИ является разработка документированного организационо-технического проекта КСЗИ АСОД, определяющего комплексное использование правовых, организационных, инженерно-технических, программно-аппаратных и криптографических методов, средств и способов защиты информации АСОД.

Список литературы

1. Аверченков В.И., Рытов М.Ю. Организационная защита информации. – Брянск: Изд-во БГТУ, 2010. – 184 с.

2. Аверченков В.И., Каштальян И.А., Пархутик А.П. САПР технологических процессов, приспособлений и режущих инструментов: учеб. пособие для вузов. – Минск: Вышэйш. шк., 1993. – 288 с.

3. Аверченков В.И. Аудит информационной безопасности. – Брянск: Изд-во БГТУ, 2010. – 210 с.

4. Аверченков В.И., Рытов М.Ю. Автоматизация проектирования комплексных систем защиты информации: монография. – Брянск: Изд-во БГТУ, 2012. – 147 с.

УДК 004.056

Е.С. Волокитина

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

В настоящее время все большее распространение приобретает перевод оказываемых услуг в электронный вид, в том числе и медицинских. Приводится анализ существующего состояния информационной безопасности в системе здравоохранения.

В последние годы остро встал вопрос защиты персональных данных (ПДн) граждан, обрабатываемых в информационных системах персональных данных (ИСПДн). Особое место среди систем этого класса занимают медицинские информационные системы (МИС), поскольку в них обрабатываются персональные медицинские данные – сведения о состоянии здоровья граждан, которые относятся к врачебной тайне.

К врачебной тайне относится следующая информация:

– сведения о факте обращения гражданина за оказанием медицинской помощи;
– анамнез;
– диагноз;
– состояние пациента, информация о ходе его лечения;
– назначения и рекомендации;
– состояние психического здоровья;
– личные и семейные тайны, доверенные врачу;
– и т.д.

За разглашение врачебной тайны предполагается дисциплинарная, административная или уголовная ответственность в соответствии с действующим законодательством Российской Федерации, законодательством субъектов РФ [1].

«Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)»[2].

Следовательно, все учреждения системы здравоохранения являются операторами ПДн, а сведения врачебной тайны там, где по этим данным можно определить принадлежность ПДн конкретному человеку, т.е. идентифицировать гражданина, входят во множество ПДн.

Уровень требований и ответственности за разглашение ПДн включает в себя требования по защите сведений, составляющих врачебную тайну.

Согласно требованиям федерального закона «О персональных данных» необходимо защищать электронную медицинскую карту. Понятие «электронной медицинской карты» связано с комплексом задач, охватывающих документирование с помощью информаци-

онных технологий процессов диагностики и лечения конкретного пациента, а также процессов диспансеризации, ведения здорового образа жизни и другой информации, связанной со здоровьем конкретного человека.

Переход от бумажной формы к электронной форме медицинских карт займет достаточное время, а также часть документации будет вестись в электронной форме, а часть останется на бумажном носителе.

Также особенностью электронного способа ведения медицинских карт является их одновременная доступность многим участникам лечебно-диагностического процесса, что выдвигает задачу формализации требований к коллективной работе с ними. Помимо этого, учитывая различные пути занесения информации в медицинскую карту, необходимо обеспечить доверие пользователей к электронным медицинским записям. Для этого необходима реализация следующих требований:

– присвоение электронным медицинским записям статуса официального медицинского документа, т.е. обладающего юридической силой;

– реализация неизменности и достоверности электронных записей (электронных документов) на протяжении всего периода их хранения;

– обеспечение персонифицируемости и неотказуемости, т.е. возможность однозначно определить ее автора, несущего ответственность за ее медицинское содержание и происхождение записи.

В настоящее время существует много различных автоматизируемых информационных систем, однако существуют проблемы их внедрения. И проблемы, именно связанные с выполнением требований по обеспечению безопасности вводимых данных и применением средств защиты информации.

Основные проблемы, которые возникают при выборе и эксплуатации медицинской информационной системы:

- Для выполнения требований, представленных выше, необходимо внедрение электронной подписи (ЭП) в разрабатываемые МИСы. Однако на данный момент продуктов, удовлетворяющих данным требованиям, просто не существует.

- Еще одной проблемой МИС является необходимость разграничения данных на уровне системы управления базой данных. Не всем пользователям нужно знакомиться со всей информацией. А некоторым даже необходимо только добавлять информацию, без права прочтения (например, при внесении анализов или внесении результатов УЗИ и т.д.). Четкого разграничения, кому и с какими правами необходимо получать в доступ в информационную систему, во многих учреждениях здравоохранения просто не существует. Согласно существующему законодательству разграничение доступа должно быть сертифицированным. К сожалению, разработчики и пользователи МИС не обеспокоены данным вопросом.
- Следующей проблемой является то, что многое оборудование, подключаемое к ПЭВМ, работает не под управлением нераспространённых операционных систем. Следовательно, выбор средств защиты становится практически невозможным в связи с тем, что в основном средства защиты информации выпускаются для операционных систем, например семейства Windows.
- Некоторые медицинские системы самостоятельно принимают решения о необходимости тех или иных действий на основе вычисления рисков и деления пациентов на группы, но нигде не производится расчет рисков принятия такого автоматизированного решения.
- А самой большой проблемой является то, что информационные системы в учреждениях здравоохранения уже построены без учета требований по безопасности (сервера на основе системLinux, уже приобретённые МИС без сертифицированного разграничения и возможностью доступа в нее всем без ограничений).

---

1. Об основах охраны здоровья граждан в Российской Федерации [Электронный ресурс]: федер. закон №122-ФЗ от 22 авг. 2004 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

2. О персональных данных [Электронный ресурс]: федер. закон №152-ФЗ от 27 июля 2006 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 004.93

А.В. Драганов

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ФОНОВОГО КАДРА В СИСТЕМАХ ВИДЕОАНАЛИТИКИ ПРИ ДЛИТЕЛЬНОМ ПЕРИОДЕ НАБЛЮДЕНИЯ

Рассмотрены внешние факторы, влияющие на работу детекторов активности и движения в системах видеонаблюдения. Предложен способ синтеза фоновых изображений при невозможности их прямого получения.

Основными детекторами, применяемыми в системах наблюдения, являются детекторы активности и движения. Детектор активности реагирует на любые изменения в кадре, которые могут быть вызваны множеством причин. Детектор движения должен реагировать на наличие устойчивого перемещения группы точек изображения по полю кадра. Если детектор движения является одним из важнейших компонентов охранных систем, то детектор активности в большинстве случаев играет вспомогательную роль, инициируя обнаружение движения и слежения за объектом. Однако в отдельных случаях системы видеонаблюдения могут использоваться и в целях мониторинга обстановки на объекте. Либо вообще целью её работы может быть детектирование медленных изменений в сцене, что выдвигает на первые роли именно проблему отслеживания изменений в течение длительных промежутков времени.

Чаще всего на практике используется два способа реализации детекторов активности и движения – метод вычитания предыдущего кадра (неадаптивный метод) и метод вычитания кадра фона, относящийся к адаптивным методам обнаружения [1]. Известны недостатки способа вычитания предыдущего кадра, главный из которых заключается в малой чувствительности в отношении медленно движущихся или невозможности детектирования временно неподвижных объектов, не относящихся к заднему плану. Таким образом, его применение для систем контроля объекта может не дать результата.

Несмотря на то, что метод вычитания фонового кадра лишён этого недостатка, его использование также сопряжено с определёнными трудностями. Основным способом детектирования изме-

нений в сцене является в общем случае слежение за изменениями в яркости/цвете пикселя (группы пикселей), а на эти параметры могут оказывать влияние явления, не связанные с появлением в поле зрения камеры целевого объекта. Из этого вытекают и прочие сложности использования шаблона фонового кадра, особенно с увеличением времени наблюдения.

Как известно, идеальными условиями для развёртывания системы видеонаблюдения является закрытое помещение без окон, с постоянным искусственным освещением и невысокой посещаемостью. В таком случае характеристики сцены являются стабильными и независимыми от внешних факторов, что позволяет легко создать так называемый фоновый кадр, позволяющий использовать метод вычитания фона из текущего кадра для детектирования активности, движения, реализации датчика оставленных предметов и других. Однако на практике часто встречается противоположная ситуация. Систему наблюдения приходится разворачивать либо в большом оживлённом помещении с круглосуточным режимом работы, имеющим большую площадь остекления, либо вообще на улице при аналогичном графике работы. В таких случаях на работу детекторов могут оказывать влияние такие естественные факторы, как:

– внезапные изменения в освещённости всей сцены или её части, вызванные облачностью;

– существенное изменение вида сцены при наступлении тёмного времени суток, даже при наличии достаточного искусственного освещения ввиду перераспределения характерных полей яркости/контрастности;

– перемещение по полю кадра теней при естественном освещении в течение дня или, например, от фар автомобиля в ночное время;

– наличие в поле кадра динамических объектов фона, таких как облака, листья деревьев, трава, другие объекты при воздействии на них ветра. То же относится и к бликам на воде, если таковая поверхность имеется в кадре. Аналогичный циклический эффект может наблюдаться и при собственных колебаниях камеры на ветру, в случае её размещения на упругом деформируемом основании;

– дождь или туман;

– при особенно длительных периодах наблюдения приходится учитывать даже изменения во внешнем виде сцены, связанные с естественной сменой времён года, например с появлением/исчезновением листвы, выпадением снега и прочее (рис.1).

Рис. 1. Пример сезонных изменений в фоновом кадре

И наконец, одной из главных проблем в описанных ситуациях развёртывания системы, связанной с режимом работы объекта, может оказаться возможность (точнее, невозможность) получения «чистого» фонового кадра в произвольный момент времени.

Благодаря большому вниманию разработчиков многие из названных проблем, так или иначе, решены. Например, развитие адаптивного способа обнаружения переднего плана/фона, основанного на статической модели фона, в котором фоновые пиксели текущего кадра моделируются как произвольная переменная, отвечающая гауссовому распределению [2], позволяет добиться хороших результатов для «отфильтровывания» теней, в том числе подвижных, а также естественного изменения в освещённости сцены.

Для решения проблемы получения фонового кадра можно предложить использование способа, аналогичного описанному в [3]. Похожую технологию, но для обработки фотоизображений, предлагает шведская компания Scalado (приложение Remove). Она представляет собой специальную программу, позволяющую с высоким качеством удалять движущиеся объекты из последовательности видеокадров, постепенно заменяя область, занятую объектом, неподвижным задним фоном. Результат работы такой программы приведён на рисунке 2. Если использовать данный алго-

ритм, фиксируя уже обработанные области, и задать в качестве критерия окончания работы полное удаление всех подвижных объектов в кадре, в результате можно получить достоверный синтезированный кадр, с большой долей вероятности содержащий только фоновые объекты. Кроме того, если сформировать выборку из подобных изображений, сделанных через большие интервалы времени, и провести повторную обработку, то появляется возможность отследить и исключить из изображения квазифоновые объекты – малоподвижные или временно неподвижные объекты, не относящиеся к истинному фону.

Рис. 2. Пример работы программы по удалению движущегося объекта

Создание на основе таких синтетических фоновых кадров библиотеки изображений, сгруппированных по различным условиям освещённости либо другим критериям, позволит использовать их для анализа сцен на охраняемом объекте в широком диапазоне изменений внешних условий.

Список литературы

1. Юдинцев В.А. Роль видеоаналитики для систем наблюдения // Системы безопасности. – 2008. – №3. – С. 120-125.

2. KaewTraKulPong P. and Bowden R. An Improved Adaptive Background Mixture Model for Realtime Tracking with Shadow Detection [Electronic resourse]. – URL: http://info.ee.surrey.ac.uk/CVSSP/Publications/papers/KaewTraKulPong-AVBS01.pdf.

3. Granados M., Kim K.I., Tompkin J. Background Inpainting for Videos with Dynamic Objects and a Free-moving Camera [Electronic resourse] // In Proc. European Conference on Computer Vision (ECCV), 2012. – URL: http://www.mpiinf.mpg.de/~granados/projects/vidbginp/index.html.

УДК 004.057.4

П.В. Зуев

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРОТОКОЛ ПЕРЕДАЧИ ЭЛЕКТРОННОЙ ПОЧТЫ – SMTP

Рассмотрен протокол передачи электронной почты SMTP.

SMTP (Simple Mail Transfer Protocol – простой протокол передачи почты) является надёжным и эффективным сетевым протоколом для доставки сообщений электронной почты. Впервые описан в RFC 821 (RFC – Request For Comments), последний раз обновился в RFC 5321, где также описан ESMTP (ExtendedSMTP) – расширение для SMTP-протокола.

Наиболее часто как транспорт для передачи почты используется протокол TCP, но SMTP может работать с любым надёжным каналом передачи данных. Рассматриваемый протокол имеет возможность доставки почты через сети (SMTPmailrelaying) с разной структурой хостов и протоколов. Сообщение передаётся не напрямую, а через промежуточных агентов. Весь путь до адресата может состоять из протоколов TCP, доступных друг другу, хостов TCP/IPInternet-сетей, хостов в средах LAN, использующих отличные от TCP протоколы.

В наше время практически во всех сетях, входящих в Internet, есть промежуточные агенты. В связи с этим два сообщения, отправленные на один и тот же адрес, могут избрать разные пути доставки. Как правило, конкретный маршрут задаёт системный администратор.

С помощью SMTP почта может передаваться другому процессу из другой сети с помощью доступных для обеих сетей шлюзов.

Схема работы протокола SMTP напрямую показана на рис. 1.

Схема работы протокола SMTP через промежуточных агентов представлена на рис. 2.

Как только у клиента SMTP появляются сообщения для передачи, он обеспечивает двухсторонний канал связи с сервером SMTP. Задачей клиента является доставка сообщения на сервер (или на несколько серверов) SMTP или сообщение о невозможности доставки.

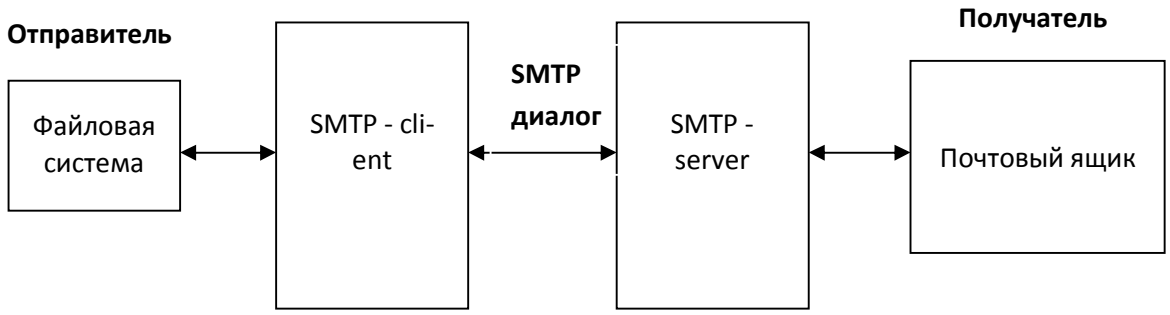


Рис. 1. Схема работы протокола SMTP напрямую

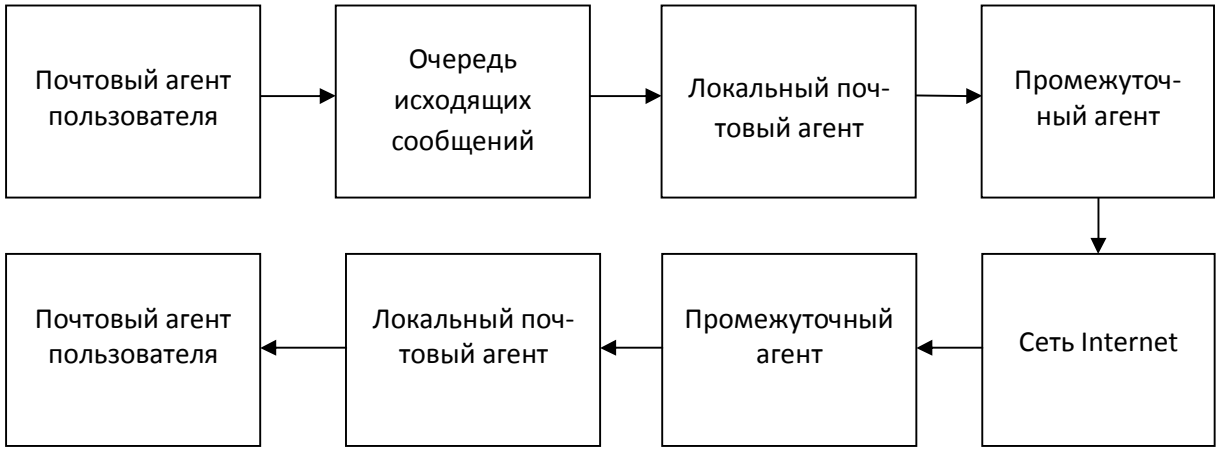


Рис. 2. Схема работы протокола SMTP через промежуточных агентов

В некоторых случаях доменные имена определяются самим клиентом SMTP. В этом случае они будут соответствовать конечному получателю. Если же реализация SMTP связана с протоколами прикладного уровня для доступа к электронной почте (POP, IMAP), доменное имя определит лишь промежуточного получателя, через которого будет транслироваться почта.

При организации канала передачи SMTP клиент начинает почтовую транзакцию. В неё входят команды, которые определяют отправителя, получателя и само письмо. На каждую команду сервер реагирует, после чего может ожидать дальнейших команд, выдать сообщение об успешности действия либо о возникшей ошибке. После передачи клиент SMTP может начать следующую передачу команд или инициировать разрыв соединения. Будучи соединённым с сервером, клиент также может выполнять дополнитель-

ные функции: проверку почтовых адресов, поиск адреса в списке рассылок и т.д.

Вся почтовая транзакция разделена на три этапа.

1. Команда MAIL. Эта команда начинает новую транзакцию, обнуляя таблицы состояний и буферы. После получения команды сервер возвращает сообщение 250 ОК. В случае если транзакцию начать не удалось, сервер выводит ошибку – постоянную (повторится при следующей отправке команды) или временную (адрес абонента доступен при следующей попытке). Ошибкам соответствуют сообщения 550 и 553.

2. Команда RCPT. Команда определяет прямой путь к получателю (имя почтового ящика или домена). Получив команду, сервер выводит 250 ОК и сохраняет заданный путь. При ошибке выводится сообщение 550, сопровождаемое строкой типа “nosuchuser – “. Одна из особенностей команды – может быть задан не просто адрес получателя, но и маршрут с заданием всех промежуточных хостов (хотя это не рекомендуется использовать в современных SMTP). Если команда была использована без предшествующей команды MAIL, то сервер возвратит ошибку 503 “Badsequenceofcommands ”.

3. Команда DATA. Сервер возвращает ответ 354 Intermediate, после чего просматривает все строки до индикатора завершения. При успешном приёме сервер данные сохраняет и посылает ответ 250 ОК. Индикатором завершения в протоколе SMTP служит точка в пустой строке. Индикатор завершения служит также предписанием серверу послать данные, на что сервер отвечает 250 ОК при успешности действия. Сбой в команде DATA может произойти, во-первых, из-за неправильного ввода предшествующих команд, и, во-вторых, из-за проблем с транзакцией (не указан адресат, недоступен сервер, сервер отказал в обработке данных из-за политик безопасности). Во втором случае сервер возвращает ответ 354.

---

1. URL: http://www.icmm.ru/~masich/win/lexion/mail/smtp.html.

УДК 004.056.53

И.В. Калуцкий, С.В. Пономарёв

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

НЕДОСТАТКИ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ ВЗЛОМА

Рассмотрены недостатки существующих систем защиты программного обеспечения от взлома.

В настоящее время трудно представить человека, у которого не имеется компьютера или который не умеет с ним взаимодействовать с помощью программного обеспечения или аппаратных устройств. У каждого пользователя есть свои интересы и предпочтения к ПО, которое способны его удовлетворять. К примеру, существуют программы для создания собственной мелодии или даже мультфильма. Над созданием программной основы работает множество компьютерных фирм и корпораций, которые стараются удовлетворить требования людей, занимающихся какой-то сферой деятельности.

Естественно, что многие из разработчиков не спешат раздавать свой продукт бесплатно и хотят получить прибыль. Но каким образом можно удостовериться, что пользователь хочет именно купить программу, а не получить ее бесплатно? Ответом на вопрос стало создание и внедрение в программные продукты защитных механизмов с целью исключения возможности бесплатного получения пользователем продукта. Первым механизмом аутентификации стал пароль к программе, который поставлялся вместе с компакт-диском в закрытой упаковке, что исключало знание пароля посторонними лицами. Затем с развитием науки и техники стали появляться все более совершенные механизмы защиты.

Однако некоторые пользователи не разделяют взглядов компаний на приобретение их ПО и пытаются обмануть системы защиты. Многие пользователи занялись изучением функционирования защитных механизмов с целью снятия и получения бесплатной программы, которой спешили поделиться с другими пользователями.

Главный недостаток существующих защитных механизмов – это использование готовых программных (ASProtect, UPX) или аппаратных (HASP, Hardlock) решений для обеспечения защиты сво-

их программных продуктов. Недостатком является тот факт, что многие из них полностью изучены и потому не представляют особой защиты. В настоящее время можно без особого труда найти руководство для взлома системы защиты и обойти ее за несколько минут. Также в Интернете можно найти огромный арсенал средств, которые позволяют взламывать уже известные защиты всего одним кликом мышки.

Рассмотрим систему защиты Armadillo, которая хорошо себя зарекомендовала в защите программного обеспечения [1]. Достоинствами данной системы является использование отладочных средств самой системы (Win32 DebugAPI), динамическое шифрование/дешифрование кода программы и др. Недостатком протектора является большой объемов оперативной памяти, что приводит к снижению производительности компьютера. Также данный механизм был полностью изучен злоумышленниками, которые составили руководства и разработали программы для автоматического устранения данной защиты, что значительно уменьшает ее эффективность.

Многие из современных “коробочных” решений содержат грубые ошибки реализации, которые позволяют не только обойти систему защиты, но и нарушают работоспособность защищаемой программы [2].

В условиях рынка программного обеспечения разработчики программ стараются выпустить свой продукт раньше конкурентов и потому считают применение готовых защитных механизмов вполне естественным. Именно этим фактором и пользуются злоумышленники, которые быстро взламывают давно изученные защитные механизмы и занимаются распространением нелицензионных копий программ.

Создание новой системы защиты

Недостатки существующих систем защиты заставляют разработчиков программного обеспечения искать новые способы защиты их интеллектуальной собственности. Необходимо создание простой, эффективной и качественной системы защиты, в которой будут исправлены недостатки существующих программных решений. Примером такой системы может служить система, основной идеей

которой является использование программных модулей, которые будут встраиваться в защищаемую программу и контролировать ее сохранность. В этих модулях будут содержаться наиболее устойчивые к взлому способы и техники.

Достоинство данной системы заключается в том, что раскрытие самого кода системы или защитного модуля не приведет к существенным проблемам. Это станет возможным благодаря тому, что каждый модуль будет уникальным и не единственным, и потому знание работы одного модуля никоим образом не способно скомпрометировать саму систему защиты. Также это решит проблему обеспечения программных продуктов, предназначенных для широких масс, так как можно внедрять разные модули в разные копии программ. Благодаря этому при вскрытии одной копии программы устойчивость защиты других программных продуктов не пострадает. Еще одним достоинством является то, что каждый модуль может быть разработан непосредственно под саму программу, что позволяет избежать конфликтов в ее работе и обеспечить ее защищенность. Также, как отмечалось ранее, можно создавать не один и не два защитных модуля, а множество. Единственным условием для их устойчивости является отсутствие похожих модулей.

Достоинства предложенной системы защиты:

– благодаря применению защитных модулей существует возможность написания собственных защитных механизмов, что позволит создавать разнообразные защитные механизмы;

– в данной системе реализуется применение комплексных мер защиты в отличие от существующих систем защиты. Благодаря этому возможно создание более устойчивых защитных механизмов, так как в основе их будут применяться известные и собственные механизмы защиты;

– благодаря использованию защитных модулей исключается возможность дискредитирования всей системы защиты. Это возможно благодаря тому, что каждый защитный модуль является уникальным и изучение злоумышленником одного модуля никоим образом не позволит ему вскрыть другой.

Недостатком данной системы могут быть лишь ошибки в реализации. Например, ошибки в реализации защитного модуля могут позволить злоумышленнику изучить и нейтрализовать защиту. Од-

нако, как упоминалось ранее, в случае нейтрализации одного защитного модуля его можно заменить другим, в результате чего злоумышленнику придется вновь пытаться нейтрализовать защиту. Благодаря этому данная система защиты является простой и эффективной.

---

1. Касперски Крис, Рокко Ева. Исскуство дизассемблирования. – СПб.: БХВ-Петербург, 2008. – 896 с.

2. Все о протекторах и упаковщиках [Электронный ресурс]. – URL: http: //www.xakep.ru/magazine/xs/057/074/1.asp.

УДК 004

О.А. Силаков, М.О. Таныгин, И.В. Калуцкий

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Рассмотрены проблемы, стоящие перед службой безопасности критически важных объектов в связи с отсутствием стандартизированных на высоком законодательном уровне методов и средств обеспечения безопасности последних.

Вопросы обеспечения безопасности критически важных объектов (КВО) на сегодняшний день весьма актуальны и обсуждаемы. Причины достаточно просты, но при этом весьма серьезны: на данный момент нет единых правил обеспечения информационной безопасности критически важных объектов, даже в проекте Федерального закона РФ «О безопасности критической информационной инфраструктуры Российской Федерации» в терминах и определениях присутствуют неточности (он так и не принят по сей день) [1], отсутствует единая проработанная методика инженерно-технической защиты таких объектов, не определена государственная структура, которая должна отвечать за эту безопасность, а главное, – за разработку нормативно-методической документации по обеспечению безопасности КВО [2].

Прежде всего необходимо определиться с терминологией и разобраться, что именно понимается под «критически важным объектом». Федеральные и ведомственные документы помимо терми-

на «критически важный объект» оперируют также терминами «опасный производственный объект», «потенциально опасный объект», «особо опасные и технически сложные объекты», «стратегические объекты», «особо важные объекты», «режимные объекты» и т.д. Отсутствие единой терминологии, за которым стоит, как правило, отсутствие единства понимания, – не единственная и не самая большая проблема в вопросе обеспечения антитеррористической и противокриминальной защиты КВО. Гораздо важнее, что отсутствует единый документ, определяющий критерии отнесения объектов государственной и негосударственной собственности к критически важным и процедуры их включения в перечень критически важных объектов, а имеющееся многообразие ведомственных определений, требований и критериев способно скорее помешать защите объектов от террористической и других видов угроз, нежели помочь. Сложившаяся ситуация приводит к тому, что вопросы защиты критически важных объектов рассматриваются не единообразно. Различные ведомства, которым государство поручило защиту КВО, не имея в качестве основы единой нормативной базы, определяют необходимые им организационные и технические меры безопасности самостоятельно, в меру специализации и квалификации своих сотрудников. Зачастую они осуществляются как придется [3].

Вернемся к определению, которое дано в распоряжении правительства РФ от 27 августа 2005 г. N 1314-р: «критически важные объекты» – объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени.

Как можно судить по этому определению, к критически важным относится достаточной большой перечень весьма разнообразных объектов. В связи с этим становятся очевидными трудности в выработке унифицированных методик по обеспечению безопасности таких объектов на любом из уровней, – будь то физическая охрана, инженерно-техническая защита, программно-аппаратная и др.

Как уже было отмечено, на сегодняшний день контроль антитеррористической и противокриминальной защиты критически важных объектов в стране поручен нескольким ведомствам. Поскольку требования у каждого ведомства свои, результатом проводимых ими проверок становится не повышение антитеррористической защищенности объектов, а издерганность сотрудников проверяемых предприятий, которые не понимают, что важно, а что нет и на что им тратить свое рабочее время. Исправить положение может только наличие единой проверяющей структуры и единых требований к обеспечению безопасности критически важных объектов [3].

Другая сторона вопроса – распределение ответственности в рамках самого предприятия. На абсолютном большинстве отечественных предприятий инженерно-техническая защита и информационная безопасность разделены: первая находится в ведении либо специально созданного управления, либо привлеченной специализированной структуры, вторая – в лучшем случае в ведении службы безопасности предприятия, а то и в ведении ИТ-департамента. Каждая служба действует независимо от другой и преследует свои цели. Скоординировать их действия очень сложно. Между тем безопасность – это проблема комплексная, и решаться она должна комплексно. Поэтому службы инженерно-технической защиты и службы информационной безопасности следует объединить. Причем не просто путем передачи обеих сфер ответственности в ведение одного "топ-менеджера", а на уровне рабочей структуры, на уровне руководителей подразделений, которые непосредственно занимаются разработкой внутриведомственных нормативов и контролем их реализации. Для такой объединенной службы безопасности должен быть разработан единый комплект документов [3].

Как отмечают специалисты [1], помимо обозначенных выше трудностей и проблем начинают появляться другие, которые являются следствием первых. Например, сформировалось мнение, что требования к аккредитации организаций завышены. Вполне очевидно, что для объектов с "высокой" категорией опасности наличие лицензий и допуска к государственной тайне (ГТ) вполне обоснованно, а вот для "низкой" и "средней" имеет смысл пересмотреть. Уже сейчас на рынке ИБ проявляется тенденция оттока хороших

специалистов из проектов по ИБ, если требуется допуск к ГТ. Все хотят отдыхать за границей.

Как видно, проблематика защиты КВО, и информационной безопасности на них, в частности, весьма разнообразна и порождает определенные трудности для специалистов по ИБ, а также разногласия в трактовке тех или иных документов и требований. Фактически на сегодняшний день все сообщество IT-безопасности ожидает результатов рассмотрения законопроекта с учетом сделанных в 2013 году замечаний и предложений. Разрешение обозначенных проблем крайне важно для систематизации и повышения надежности защиты критически важных объектов на всех уровнях обеспечения физической и информационной безопасности.

Список литературы

1. Замечания и рекомендации по проекту ФЗ по безопасности критической информационной инфраструктуры [Электронный ресурс]. – URL: http://www.securitylab.ru/blog/personal/80na20/32232.php.

2. Кто все-таки будет отвечать за ИБ КВО – ФСТЭК или ФСБ? [Электронный ресурс]. – URL: http: //www.securitylab.ru/blog/personal/Business_ without_danger/38795.php.

3. Основы государственной политики в области обеспечения безопасности населения РФ и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов [Электронный ресурс]. – URL: http: //www.secuteck.ru/ articles2/event/aktyalnie-problemi-obespecheniya-bezopasnosti-kriticheski-vajnih-obektov.

УДК 004.056

Е.В. Морозов, М.О. Таныгин, И.В. Калуцкий

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ АТАКИ ТИПА «ПЕРЕПОЛНЕНИЕ БУФЕРА» НА СИСТЕМУ ПЕРЕДАЧИ ЗАЩИЩЁННЫХ АУТЕНТИФИЦИРОВАННЫХ СООБЩЕНИЙ

В статье рассмотрена атака типа «переполнение буфера» – одна из атак на систему передачи защищённых аутентифицированных сообщений, обусловленная фиксированным размером буфера приёмника. Приводятся результаты имитационного моделирования данного типа атаки и целесообразные значения параметров алгоритма формирования защищённых сообщений.

В любой реальной системе передачи сообщений, защищённых от несанкционированного прочтения и подмены, при наличии помех в канале связи и при активности злоумышленников, реализующих различные атаки на систему, вероятность успешной и безошибочной передачи данных не может равняться единице. Но для реального применения системы, особенно такой, в которой используются защитные механизмы, необходимо оценить основные её рабочие характеристики и найти зависимость между параметрами алгоритма формирования таких соотношений.

Примером алгоритма формирования защищённых сообщений может быть алгоритм, описанный в работе [1]. Область его применения – сообщения небольшой, от нескольких битов до нескольких байтов, длины. В основе его лежит «связывание» таких небольших сообщений в одно большое за счёт буферизации в приёмнике. Однако при этом буферизироваться могут не только сообщения, выданные источником, но и сообщения, введённые в канал связи злоумышленником с целью нарушить работоспособность нашей системы. Для возможности реагирования на такие факты было решено ограничить размер буфера приёмника.

Такое ограничение, помимо всего прочего, снижает трудозатраты при последующем построении цепочек командных слов: максимально число вариантов равно соотношению $N^{(M-1)}$, где M – длина буфера или пула командных слов; N – ширина буфера. Из общего количества легальной является только одна цепочка. С другой стороны, ограничение ширины буфера провоцирует атаку типа «переполнение буфера», при которой злоумышленник формирует случайным образов посторонние командные слова и передаёт их в приёмник. Данные посторонние слова проходят первичную сортировку по условиям алгоритма опознания легальных слов [1], и часть из них окажется в буфере. Чем больше будет сформировано посторонних сообщений за время передачи пула, тем выше вероятность его переполнения.

Когда переполнение произойдёт, системе передачи сообщений не останется ничего другого, как повторить передачу всего пула целиком. Если переполнение будет происходить часто, мы можем говорить об отказе в обслуживании рассматриваемой системы, и нам необходимо скорректировать параметры системы с целью

уменьшения вероятности возникновения описанной ситуации. С другой стороны, в ситуации, когда помех нет, нет действий злоумышленников, пытающихся передать в приёмник собственные данные, выдав их за данные легального источника, не целесообразно вводить дополнительные аутентифицирующие и контрольные поля большого размера. Следовательно, алгоритм формирования защищённых сообщений должен учитывать характеристики канала, изменяя в зависимости от них свои параметры: размеры дополнительных полей, что, в свою очередь, будет влиять на защищённость сообщений.

Таким образом, необходимо выявить такие соотношения полей командного слова, которые бы позволяли обеспечивать частоту возникновения ошибки «переполнение буфера», не превышающую требуемого в системе порога.

Для выявления соотношений между параметрами алгоритма передачи защищённых сообщений, параметрами канала и вероятностью возникновения ошибки «переполнение буфера» была составлена математическая модель, подробно описанная в работе [2]. В качестве параметров данной модели выступили: M – длина буфера или пула командных слов, N – ширина буфера, L – длина поля кода синхронизации, K – соотношение между интенсивностью формирования посторонних командных слов и интенсивностью формирования легальных слов. Повторять все выкладки здесь не имеет смысла. Остановимся лишь на анализе результатов, представленных в вышеозначенной работе.

Во-первых, анализируя зависимости между вероятностью переполнения буфера $p_{\text{пр}}$ и длиной пула слов M при фиксированных N, L и K, можно выделить на нём две области: область роста, где соотношение можно записать как $p_{\text{прев}} \approx \text{C1} \times M^{\text{C2}}$ (где C1 и C2 – константы, определяемые величиной интенсивности выдачи посторонних слов K), и область насыщения, при которой рост M уже незначительно влияет на рост вероятности $p_{\text{пр}}$.

Во-вторых, изменение параметра K практически нивелируется обратно пропорциональным изменениям вероятности записи посторонних командных слов в буфер $p_{\text{зап}} = 2^{-L}$. То есть значение вероятности переполнения буфера при каких-либо значениях L и K

незначительно отличается от этой же вероятности при значениях $(L+1)$ и $2 \cdot K$ при любых N и M.

В-третьих, анализируя зависимости вероятности переполнения буфера от M и N при фиксированных значения произведения $2^{-L} \cdot K$, приведённые на рисунках 1 и 2 (вероятность переполнения буфера по ширине отображается оттенком серого, белый соответствует интервалу от 0,9 до 1, чёрный – от 0 до 0,1), можно сделать вывод, что при фиксированных вероятностях переполнения буфера наблюдается линейное соотношение между шириной буфера N и длиной буфера M. То есть любой зафиксированной частоты переполнения буфера длине поля синхронизации и интенсивности получения посторонних слов соответствует определённое соотношение между шириной и глубиной буфера.

Иными словами: $N \approx \alpha \cdot M$, где $\alpha = f(2^{-L} \cdot K, v)$ – функция от параметра $2^{-L} \cdot K$ и наблюдаемой частоты переполнения буфера v (которая при большом числе циклов передачи практически равна рассчитанной вероятности переполнения).

Используя найденные соотношения можно варьировать длину пула при фиксированной ширине буфера, достигая требуемой вероятности переполнения какого-либо яруса. Для этого достаточно контролировать частоту возникновения ошибок «переполнение буфера» и в соответствии с найденными соотношениями менять параметры алгоритма.

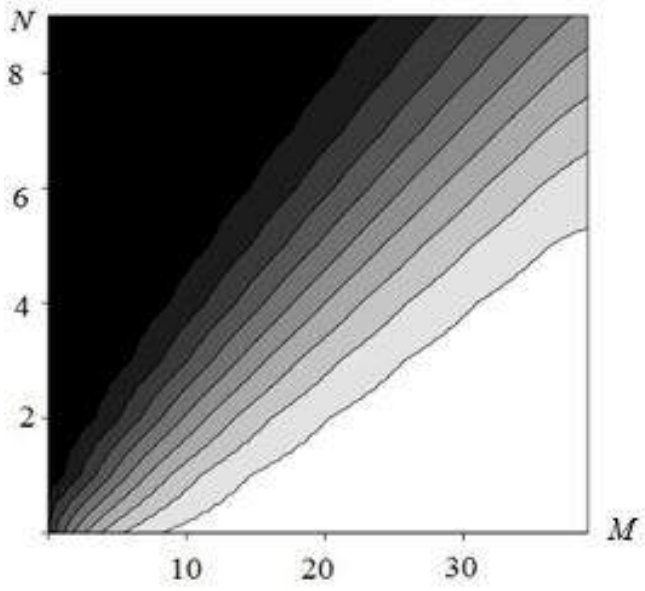


Рис. 1. Зависимость (в оттенках серого) вероятности переполнения буфера от длины буфера M и ширины N при $2^{-L} \cdot K = 0{,}25$

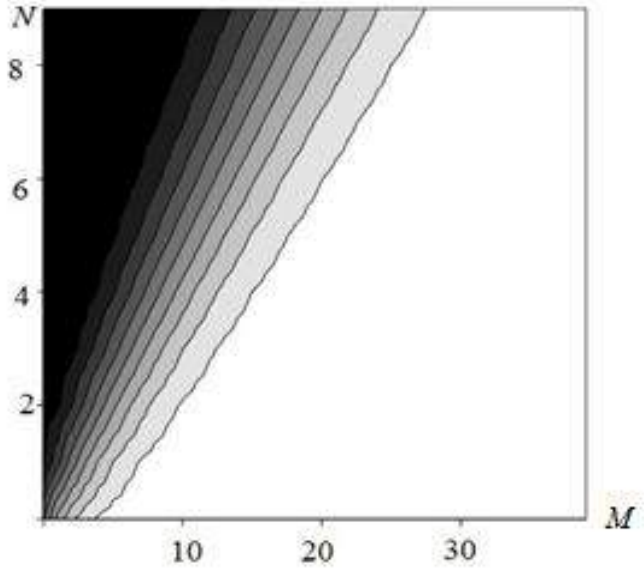


Рис. 2. Зависимость (в оттенках серого) вероятности переполнения буфера от длины буфера M и ширины N при $2^{-L} \cdot K = 0{,}5$

Анализ результатов моделирования также показал, что для достижения целевой частоты возникновения ошибок «переполнение буфера» целесообразно сначала изменять размер поля синхронизации L как величину, оказывающую наибольшее влияние, а затем добиваться требуемых значений варьированием соотношения между длиной и шириной буфера приёмника.

Сопоставление значений вероятности переполнения буфера на множестве значений параметров моделирования позволяет сказать, что оптимальными соотношениями являются $2^{-L} \times K = 0{,}5$ и $M/N = 2$. При таких параметрах изменение значения интенсивности выдачи посторонних сообщений злоумышленником (а именно он является величиной, недетерминированной в нашем исследовании) в пределах десятков процентов будет вызывать изменения вероятности возникновения ошибок «переполнение буфера» в пределах 5 – 10%, что, на наш взгляд, является приемлемым для реальной системы передачи данных.

---

1. Tanygin M.O. Method of Control of Data Transmitted Between Softwareand Hardware // Комп'ютерні науки та інженерія : материали IV Міжнародної конференції молодих вчених CSE–2010 – Львів: Видавництво Львівскої політехніки, 2010. – С.344 – 345.

2. Таныгин М.О. Моделирование системы передачи аутентифицированных командных слов // Современные тенденции технических наук: материалы междунар. заоч. науч. конф. – Уфа, 2011. – С.28 – 30.

УДК 004.056

Е.В. Морозов, М.О. Таныгин, И.В. Калуцкий

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АНАЛИЗ ВОЗМОЖНЫХ ОШИБОК В СИСТЕМЕ ПЕРЕДАЧИ ЗАЩИЩЁННЫХ СООБЩЕНИЙ

В статье рассмотрены основные ошибки, возникающие в системе передачи сообщений ограниченной длины, и описаны основные типы атак на них. Приводятся условия возникновении ошибок и варианты реации системы на их возникновение.

В настоящее время существует множество алгоритмов и методов контроля целостности, аутентичности и обеспечения конфиденциальности передаваемых по открытым каналам сообщений. При этом, несмотря на их многообразие, объединяет их то, что ориентированы они на сообщения достаточно большой длины. При этом существует класс систем, в которых длина предаваемого блока данных ограничена несколькими байтами и даже битами. Это, например, системы передачи команд от программного обеспечения в аппаратные средства, системы радиоидентификации и т. д. Для них применение традиционных криптографических алгоритмов и схем становится проблематичным, так как оно не способно обеспечить ни контроль целостности, ни аутентичность, так как размер избыточных информационных полей при этом может превышать длину передаваемого блока данных.

Для подобных систем необходимо адаптировать схемы имитозащиты, объединяя передаваемые сообщения в пулы, вырабатывая контрольные разряды как для пула целиком, так и для отдельных слов, его составляющих. Подобный алгоритм был подробно описанный в работах [1, 2]. В его основе лежит дописывание к каждому информационному слову (которое предварительно зашифровывается) из пула служебных последовательностей: хэша и кода синхронизации, представляющего из себя зашифрованный в соответствии с секретным словом номер текущего слова в пуле.

Весь пул, а также посторонние командные слова (ПКС), которые могут быть получены приёмником, буферизируются и распределяются по ярусам. Ярусом мы называем расшифрованный номер текущего слова. В результате анализа хеш-последовательностей

выделяются цепочки командных слов – последовательности командных слов, значения хешей которых удовлетворяют требованиям алгоритма. Если выделена одна цепочка, равная по длине пулу командных слов, то слова, её формирующие, опознаются как легальные.

В реальной системе передачи сообщений буфер будет представлять оперативное запоминающее устройство, следовательно, его объём будет ограничен. Таким образом, может произойти ситуация, при которой ещё до поступления в буфер последнего слова количество слов на одном из ярусов окажется выше допустимого значения. Причём среди командных слов этого яруса может и не оказаться легального. Подобную ситуацию в настоящей работе мы будем называть «переполнение буфера».

Ограничение в ёмкости ярусов буфера, с одной стороны, снижает трудозатраты при последующем построении цепочек командных слов: максимально число вариантов равно соотношению $N^{(M-1)}$, где M – длины буфера или пула командных слов, N – ширина буфера или ёмкость одного яруса. Из общего количества цепочек командных слов легальной является только одна. С другой стороны, ограничение ширины буфера провоцирует атаку типа «переполнение буфера», при которой злоумышленник формирует случайным образов посторонние командные слова (ПКС) и передаёт их в приёмник. Данные ПКС проходят первичную проверку, и часть из них окажется в буфере. Чем больше будет сформировано ПКС за время передачи пула, тем выше вероятность его переполнения.

Когда переполнение произойдёт, системе передачи сообщений не останется ничего другого, как повторить передачу всего пула целиком. Если переполнение будет происходить часто, мы можем говорить об отказе в обслуживании рассматриваемой системы. Таким образом, необходимо выявить такие соотношения полей командного слова, которые бы позволяли обеспечивать частоту возникновения ошибки «переполнение буфера», не превышающего требуемого в системе порога.

Все M слов, выданные легальным источником в текущем пуле, при условии отсутствия сбоев в интерфейсных линиях всегда образуют цепочку. Таким образом, мы можем сказать, что при

условии отсутствия коллизий все командные слова легального источника пула будут опознаны и обработаны, то есть невозможна потеря отдельных слов цепочки и замена их словами посторонних источников. Коллизией же при выборе будем называть ситуацию, при которой помимо цепочки из таких легальных командных слов будет сформирована альтернативная цепочка, в которой от 1 до M слов будет выдано посторонним источником.

Простейшая коллизия, когда при выполнении алгоритма выбора командных слов из буфера образуется 2 цепочки, приведена на рисунке, где $S_{j(1),1}^{\text{инф}}$, $S_{j(2),2}^{\text{инф}}$, … $S_{j(M),M}^{\text{инф}}$ – командные слова легального источника; $j(1)$ – $j(M)$ – номера, под которыми 1-е … M-е командные слова легального источника были записаны в буфер; e – номер яруса, на котором возникла коллизия; $S_{p,e}^{\text{пс}}$ – слово постороннего источника; p – номер, под которым посторонное слово поступило в буфер.

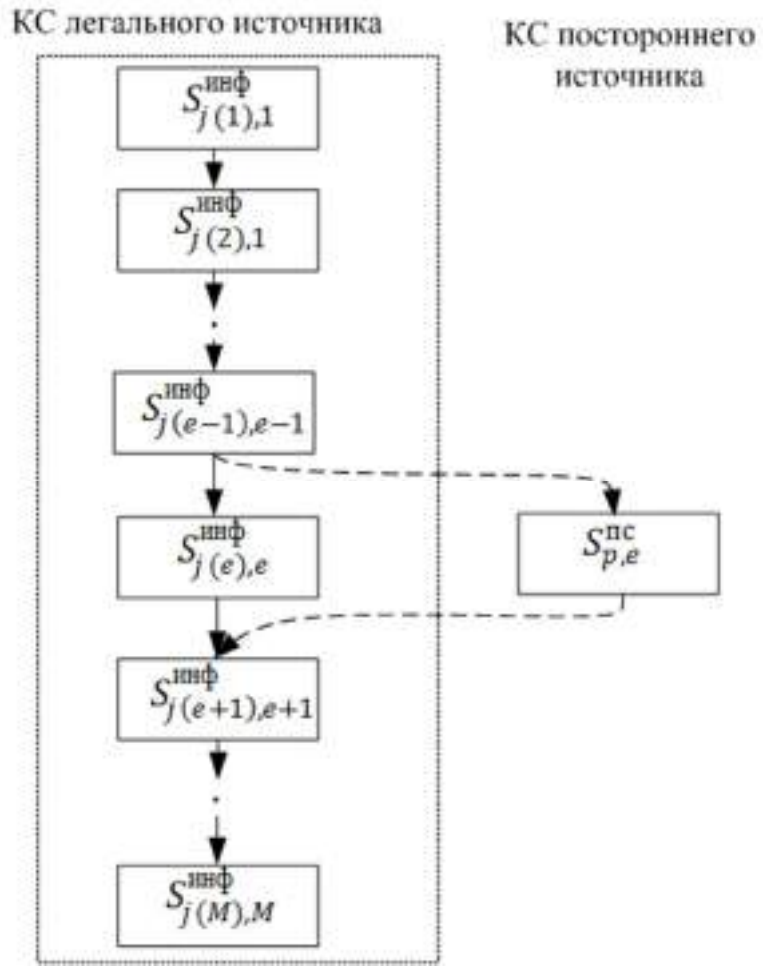


Рис. 1. Простая коллизия при выборе командного слова из буфера

Подобная коллизия может возникнуть при выполнении следующих условий:

$$S_{j(e),e}^{\text{пс}} \neq S_{p,e}^{\text{пс}};$$
$$F_{\text{хеш}}(S_{j(k),\,k}^{\text{инф}}, S_{j(k-1),\,k-1}^{\text{инф}}, \ldots S_{j(e+1),e+1}^{\text{инф}}, S_{j(e),e}^{\text{инф}}, S_{j(e-1),e-1}^{\text{инф}}, \ldots S_{j(1),1}^{\text{инф}}) = F_{\text{хеш}}(S_{j(k),\,k}^{\text{инф}}, S_{j(k),\,k}^{\text{инф}}, \ldots S_{j(e+1),e+1}^{\text{инф}}, S_{p,e}^{\text{пс}}, S_{j(e-1),e-1}^{\text{инф}}, \ldots S_{j(1),1}^{\text{инф}}), \quad (1)$$
$$k = (e+1) \ldots \text{M};$$
$$j(e-1) < p < j(e+1).$$

В этом случае результатом работы алгоритма выбора командного слова из буфера будут две цепочки командных слов:

– первая (правильная) – $S_{j(1),1}^{\text{инф}}$, $S_{j(2),2}^{\text{инф}}$, … $S_{j(e-1),e-1}^{\text{инф}}$, $S_{j(e),e}^{\text{инф}}$, $S_{j(e+1),e+1}^{\text{инф}}$,… $S_{j(M),M}^{\text{инф}}$;

– вторая (ложная) –$S_{j(1),1}^{\text{инф}}$, $S_{j(2),2}^{\text{инф}}$, … $S_{j(e-1),e-1}^{\text{инф}}$, $S_{p,e}^{\text{пс}}$, $S_{j(e+1),e+1}^{\text{инф}}$,… $S_{j(M),M}^{\text{инф}}$,

где $S_{j(1),1}^{\text{инф}}$, $S_{j(2),2}^{\text{инф}}$, … $S_{j(M),M}^{\text{инф}}$.

Следует отметить, что слова, принятые приёмником, не рассматриваются по отдельности, а только как неотъемлемая часть цепочки из M слов. Поэтому обе цепочки имеют все основания быть опознанными как выданные легальным источником. Поэтому в случае, когда алгоритм выявил две или более конкурирующие цепочки сообщений, требуется повторная передача источником всего пула командных слов.

Этот факт даёт основание для ещё одного типа атак на предлагаемую систему – атаку типа «провокация коллизии». По своему проведению она аналогична атаке «переполнение буфера» и заключается в формировании злоумышленником случайных ПКС и передаче их в приёмник. Однако необходимость повторной передачи пула командных слов здесь обусловлена не переполнением одного из ярусов, а формированием двух и более конкурирующих цепочек (при условии, что их составляют неидентичные командные слова).

В случаях же частого появления коллизий в процессе построения цепочки из легальных командных слов отправляющей стороне необходимо рассмотреть ряд факторов, влияющих на появление коллизий, и учесть их при повторной передаче командных слов.

Такими факторами могут являться размеры информативной части и имитоприставки, которые зависят от количества посторонних слов. При возникновении коллизий в целях исключения угрозы «провокация коллизии» необходимо увеличить размер имитоприставки, что существенно снизит вероятность возникновения коллизий.

---

1. Tanygin M.O. Method of Control of Data Transmitted Between Softwareand Hardware // Комп'ютерні науки та інженерія : материали IV Міжнародної конференції молодих вчених CSE–2010. – Львів: Видавництво Львівскої політехніки, 2010. – С.344 – 345.

2. Таныгин М.О. Моделирование системы передачи аутентифицированных командных слов // Современные тенденции технических наук: материалы междунар. заоч. науч. конф. – Уфа, 2011. – С.28 – 30.

УДК 004.715

А.С. Ржищев

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ЗАЩИТА РОУТЕРА ОТ ЗЛОУМЫШЛЕННИКОВ

Описаны методы защиты роутера от несанкционированного доступа.

Во многих организациях и учебных заведениях имеются роутеры, которые «раздают» интернет по Wi-Fi. Естественно, встает вопрос о защите личной информации, передаваемой по такому каналу связи.

Что же будет, если к вашей Wi-Fi-сети подключится злоумышленник? Во-первых, он сможет пользоваться вашим Интернетом, и бывают случаи, когда у вас падает скорость при работе с Интернетом. Во-вторых, при использовании различных программ-снифферов он сможет похищать ваши пароли от сайтов, смотреть посещение сайтов ваших браузеров, перехватывать ку́ки и т.п. И в-третьих, если в вашей сети Wi-Fi есть папки или файлы, открытые для общего доступа, злоумышленник получит доступ к ним.

Для улучшения качества защиты информации в этом процессе предлагается использовать некоторые методы защиты роутеров от атак:

1. Отключить WPS или поставить стороннюю прошивку для отключение WPS.

2. Поставить пароль с шифрованием WPA2.

3. Скрыть идентификатор сети SSID.

4. Сделать фильтрацию по mac-адресу.

5. Поставить ограничение на количество подключаемых устройств к роутеру.

6. Выставить ограниченный радиус действия Wi-Fi-сигнала роутера (на этаж или на помещение).

7. Сменить стандартные настройки (логин и пароль к роутеру и IP-адрес роутера).

Рассмотрим каждый метод по отдельности.

1. WPS или Wi-Fi Protected Setup (защищённая установка) – полуавтоматическое создание беспроводной сети Wi-Fi. Уязвимость WPS заключается в том, что если в точке доступа активирован WPS с PIN (который по умолчанию включен в большинстве роутеров), то подобрать PIN-код для подключения можно за считанные часы. PIN-код состоит из восьми цифр, следовательно, существует 10^8 (100000000) вариантов PIN-кода для подбора. Однако количество вариантов можно существенно сократить. Дело в том, что последняя цифра PIN-кода представляет собой некую контрольную сумму, которая высчитывается на основании семи первых цифр. Таким образом количество вариантов уже сокращается до 10^7 (10000000). Кроме того, уязвимость протокола позволяет разделить пин-код на две части, 4 и 3 цифры, и проверять каждую на корректность отдельно. Следовательно, получается 10^4 (10000) вариантов для первой половины и 10^3 (1000) для второй. В итоге это составляет всего лишь 11 000 вариантов для полного перебора.

2. WPA и WPA2 (Wi-Fi Protected Access) представляет собой обновлённую программу сертификации устройств беспроводной связи. Технология WPA пришла на замену технологии защиты беспроводной Wi-Fi-сети WEP. На данный момент лучше, чем открытая точка доступа, шифрование WEP и WPA.

3. Каждой беспроводной сети назначается свой уникальный идентификатор (SSID), который представляет собой название сети. При попытке пользователя войти в сеть драйвер беспроводного

адаптера прежде сканирует эфир на предмет наличия в ней беспроводных сетей. При использовании режима скрытого идентификатора (как правило, этот режим называется Hide SSID) сеть не отображается в списке доступных, и подключиться к ней можно только в том случае, если, во-первых, точно известен ее SSID, а во-вторых, заранее создан профиль подключения к этой сети.

4. Фильтрация по mac-адресу позволяет повысить уровень безопасности беспроводной сети. Для реализации данной функции в настройках точки доступа создается таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы в данной сети.

5. Поставив данное ограничение, можно оставить то количество устройств, которые работают в данной Wi-Fi-сети.

6. Ограниченный радиус действия Wi-Fi-сигнала роутера дает возможность пользоваться сетью Wi-Fi на небольшом расстоянии или в конкретном отведенном месте (помещении).

7. При настройке Wi-Fi-сети нужно менять стандартные настройки логина, пароля и IP-адреса роутера. Как правило, данным методом пренебрегают, тем самым оставляя «дыру» для злоумышленников.

При использовании всех этих методов защиты вероятность проникновения будет, но очень «маленькая». Злоумышленнику понадобится очень много времени и терпения для взлома сети.

Список литературы

1. Джим Гейер. Беспроводные сети. Первый шаг. – М.: Изд-во: «Вильямс», 2005.

2. Джон Росс. Настройка Wi-Fi-соединения. – М.: НТ Пресс, 2007.

3. Пролетарский А. В., Баскаков И. В., Чирков Д. Н. Беспроводные сети Wi-Fi. – М.: НТ Пресс, 2007.

4. Ватаманюк А.И. Беспроводная сеть своими руками. – СПб.: Питер, 2006.

5. Настройка Wi-Fi соединения. Беспроводная сеть. – М.: НТ Пресс, 2011.

УДК 004.056

Е.С. Савенкова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОБЗОР КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Представлены способ обеспечения безопасности информационных систем, принципы системы защиты информации, комплексный подход.

Информационной системой называется комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, а также системный персонал, обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей.

Безопасность информационной системы – это свойство, заключающееся в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации. Для обеспечения целостности и конфиденциальности информации необходимо создать защиту информации от случайного уничтожения или несанкционированного доступа к ней.

Для обеспечения безопасности информационных систем применяют системы защиты информации, которые представляют собой комплекс организационно-технологических мер, программно-технических средств и правовых норм, направленных на противодействие источникам угроз безопасности информации.

Системы защиты информации должны базироваться на основных принципах. Первым и наиболее важным является принцип непрерывности совершенствования и развития системы информационной безопасности. Суть этого принципа заключается в постоянном контроле функционирования системы, выявлении ее слабых мест, потенциально возможных каналов утечки информации и несанкционированного доступа, в обновлении и дополнении механизмов защиты в зависимости от изменения характера внутренних и внешних угроз, в обосновании и реализации на этой основе наиболее рациональных методов, способов и путей защиты ин-

формации. Таким образом, обеспечение информационной безопасности должно представлять собой непрерывный процесс.

Также обеспечение защиты информационных систем должно быть комплексным. Комплексный подход является наиболее эффективным. При комплексном подходе методы противодействия угрозам интегрируются, создавая архитектуру безопасности систем. Необходимо отметить, что любая система защиты информации не является полностью безопасной, поэтому приходится выбирать между уровнем защиты и эффективностью работы информационных систем.

В качестве главной цели создания комплексной системы защиты информации можно определить ее надежность. При этом надежной может считаться система безопасности, реальное состояние которой перекрывает угрозы в полной мере и не требует дополнительных мер. Надежность защиты информации прямо пропорциональна системности, т. е. при несогласованности между собой отдельных составляющих риск нарушения безопасности в технологии защиты и уязвимости системы в целом увеличивается. Комплексность решений состоит в объединении в одно целое локальных СЗИ, в качестве которых могут быть рассмотрены, например, виды защиты информации (правовая, организационная, инженерно-техническая).

Работы по защите информационных систем в нашей стране ведутся уже достаточно продолжительное время. Накоплен существенный опыт. Но основным направлением поиска новых способов обеспечения безопасности информации является не просто создание соответствующих механизмов, а реализация регулярного процесса при комплексном использовании всех имеющихся средств защиты, который осуществлялся бы на всех этапах всего жизненного цикла систем обработки информации. При этом все используемые средства, методы и мероприятия наиболее рациональным образом должны объединяться в единый целостный механизм. Однако система должна обеспечивать защиту не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала, а также нештатных ситуаций технического характера.

Следовательно, можно сформулировать вывод, что проблема обеспечения желаемого уровня защиты информации весьма сложная и требует для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов по защите информации.

Список литературы

1. Когаловский М. Р. Перспективные технологии информационных систем. – М.: ДМК Пресс; Компания АйТи, 2003. – 288 с.

2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие. – М.: Изд-во Горячая линия – Телеком, 2004. – 280 с.

3. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: учебное пособие. – М.: Изд-во ИНФРА-М, 2001. – 304 с.

УДК 004.056

Е.С. Савенкова

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Показан требуемый уровень безопасности, методы оценки уровня защищенности, объект оценки, системы контроля защищенности.

Поддержание требуемого уровня безопасности является актуальным вопросом для многих учреждений, как государственных, так и частных. Проблемным является вопрос создания защищенной информационной системы, которая бы и обеспечивала гарантированный уровень защиты, и оптимально соответствовала бы нуждам организации.

В действительности оценить защищенность информационной системы достаточно сложно. Для решения этой задачи применяются качественные методы оценки уровня защищенности. Это означает, что в результате мы получаем не количественную – информационная система защищена на «5» баллов, а качественную оцен-

ку – информационная система соответствует определенному классу или определенному уровню защищенности.

Количественные методы оценки не нашли своего применения на практике.

Классы же защищенности являются официально признаваемой оценкой защищенности информационных систем, и упоминание о них встречается в разных стандартах защищенности. Например таких, как ГОСТ ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть1. Введение и общая модель, ГОСТ ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Часть 2. Функциональные требования безопасности.

В части 1, в частности, сказано, что «для достижения большей сравнимости результатов оценок их следует проводить в рамках полномочной системы оценки, которая предписывает стандарты, контролирует качество оценок и определяет нормы, которыми необходимо руководствоваться...». Сам контекст оценки представлен на рисунке 1.

Рис. 1. Контекст оценки

Результаты оценки должны быть обоснованными. Следовательно, оценка должна приводить к объективным и повторяемым результатам, что позволит использовать их в качестве доказательств. Взаимосвязь понятий, используемых при оценке, представлена на рисунке 2.

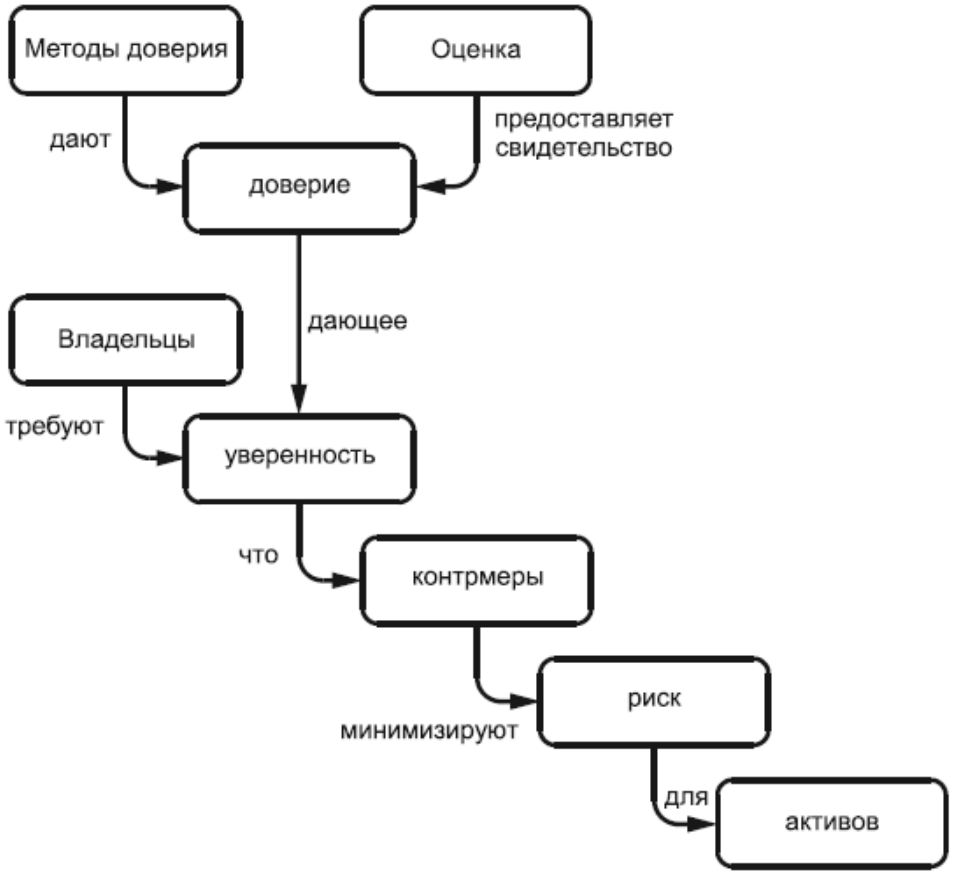


Рис. 2. Взаимосвязь понятий при оценке

В процессе оценки объекта оценки (ОО) эффективности защиты должны обязательно учитываться как объективные обстоятельства, так и вероятностные факторы. Сам процесс оценки ОО показан на рисунке 3.

Для ответа на вопрос, насколько эффективно работает система защиты информации и какова реальная защищенность информационной системы, служат:

- системы контроля защищенности;
- средства контроля эффективности защиты информации.

О данных средствах говорится в ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении».

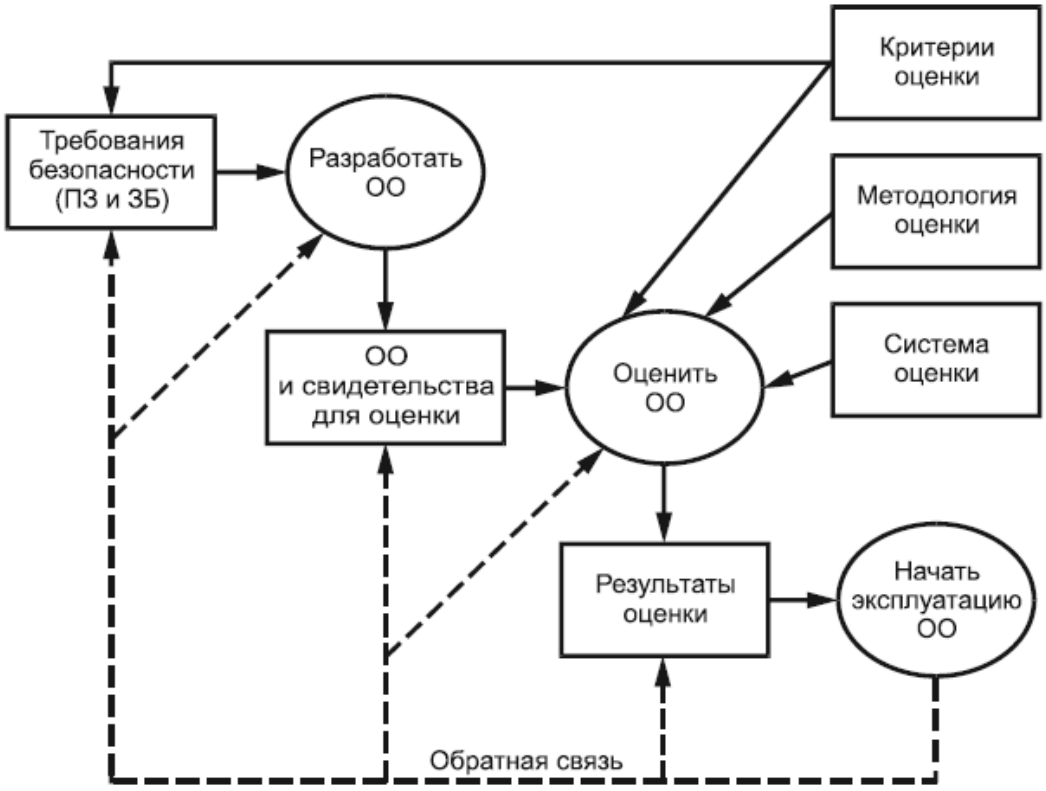


Рис. 3. Процесс оценки ОО

Таким образом, корректная оценка защищенности информационных систем необходима как для выполнения сравнения аналогичных по назначению и уровню сложности систем, так и для мониторинга динамики уровня защищенности конкретной информационной системы во времени.

Список литературы

1. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 1. Введение и общая модель. – М.: Госстандарт России, 2002.

2. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 2. Функциональные требования безопасности. – М.: Госстандарт России, 2002.

3. Биячуев Т.А. Безопасность корпоративных сетей / под ред. Л.Г. Осовецкого. – СПб.: Изд-во СПб ГУ ИТМО, 2006. – 161 с.

УДК 687.3

В.П. Добрица[1], Д.А. Стребков[1], А.А. Карпов[2]

[1] ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2] ООО Центр системной безопасности «ЩИТ-ИНФОРМ»

ОЦЕНКА ОПАСНОСТИ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ИЗ ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА ЭТАПЕ ПРЕДВАРИТЕЛЬНОГО ЭКСПЕРТНОГО АНАЛИЗА

Рассмотрен метод определения степени опасности каждого элементарного канала утечки информации из автоматизированной системы в условиях неопределенности о возможностях и составе применяемого комплекта специальных технических средств. Метод базируется на теории графов, методе анализа иерархий.

Стремительное совершенствование специальных технических средств добывания информации (в частности, средств радиоперехвата, средств разведки побочных электромагнитных излучений и наводок, электронных устройств перехвата информации, внедряемых в технические средства и т.п.) [1] и автоматизированных систем обработки и анализа информации (далее – анализируемых систем), построенных на базе современных электронно-вычислительных машин (ЭВМ), принтеров, факсов и другого оборудования, значительно повышает степень опасности утечки информации ограниченного доступа по техническим каналам [2].

Для своевременного выявления наиболее опасных («уязвимых» для СТС) элементов из состава анализируемой системы (АС) на основе существующих методик (базирующихся на визуальном осмотре, инструментальном контроле, рентгеновском контроле и др.) целесообразно проведение предварительного экспертного анализа [1, 2, 3], позволяющего ограничить пространство поиска опасных («уязвимых») элементов и связей между элементами АС для последующего выборочного или целевого технического контроля. При этом для предварительного анализа при известных параметрах специальных технических средств (СТС) применяются методы, базирующиеся на известных математических моделях [3], а в условиях неопределенности о параметрах СТС применяются экспертные методы [4].

Однако решение задачи по своевременному выявлению «уязвимых» элементарных технических каналов утечки информации из АС, являющейся структурно-сложной (иерархической) системой, в условиях неопределенности о возможностях и составе применяемого комплекта СТС на основе существующих методов является затруднительным.

При этом под элементарными техническими каналами утечки информации (ТКУИ) из структурно-сложной АС понимаем электромагнитные, электрические и т.п. связи между элементами разного уровня и функционального назначения, связи между элементами АС и внешними устройствами, внешней средой, а также возникающие за счет этих связей побочные электромагнитные излучения и др.

Под *e*-м техническим каналом утечки информации понимаем канал добывания (перехвата) противоборствующей стороной защищаемой информации с применением СТС *e*-го типа ($TC^{\theta,e}$).

Предлагается метод определения степени опасности каждого элементарного технического канала утечки информации ТКУИ из структурно-сложной АС в условиях повышения неопределенности о возможностях и составе применяемого комплекта СТС. Метод базируется на многоуровневой модели влияния элементарных ТКУИ на потенциальную угрозу утечки ценной информации, теории графов [5], методе анализа иерархий [6].

Модель влияния элементарных ТКУИ на потенциальную угрозу утечки ценной информации из структурно-сложной АС в условиях неопределенности базируется на представлении АС в виде направленного графа, отображающего возможные элементарные ТКУИ на разных уровнях АС с оценками их степени влияния на потенциальную угрозу утечки информации из АС.

В качестве возможных ТКУИ в условиях применения СТС *e*-го типа в рассматриваемой модели выделены элементарные ТКУИ, возникающие за счет:

– электрической, электромагнитной (ЭМ) и т.п. связи между анализируемым *i*-м элементом (подсистемой) (*n+1*)-го уровня

$x_{i,n+1} \in x_{i,n}$ и внешней средой $Q_{внеш.}$ (*e*-й элементарный ТКУИ $u^{e,i,n}_{i,n+1/Q_{внеш.}}$);

– электрической, электромагнитной и т.п. связи между элементом $x_{i,n+1} \in x_{i,n}$ и элементом $x_{z,n+1} \in x_{i,n}$ (*e*-й элементарный ТКУИ $u^{e,i,n}_{i/z,n+1}$), в том числе за счет внедрения устройства перехвата информации;

– электрической, ЭМ и т.п. связи между элементом $x_{i,n+1} \in x_{i,n}$ и $x_{\text{j},n+1} \in x_{z,n}$ (*e*-й элементарный ТКУИ $u^{e,i,n/z,n}_{i,n+1/\text{j},n+1}$, являющийся частью интегрального ТКУИ $u^{e,i,n-1}_{i/\text{z},n}$).

В предложенной модели для оценки степени влияния каждого *e*-го элементарного ТКУИ *(n+1)*-го уровня на потенциальную угрозу утечки информации из элемента (подсистемы, системы) $x_{i,n}$ ($\mu^{e,n,i}_{n+1}$) применяется метод анализа иерархий.

Оценка степени влияния анализируемого элементарного ТКУИ *(n+1)*-го уровня ($u^{e,i,n}_{i,n+1/Q_{внеш.}}$ или $u^{e,i,n}_{i/z,n+1}$) на интегральную утечку информации по *e*-му техническому каналу из АС ($x_{i,n=1}$) базируется на полученных оценках степени влияния (опасности) анализируемого элементарного ТКУИ для каждого уровня АС и весовых оценках опасности каждого типа СТС.

Таким образом, предложен метод определения количественной оценки степени опасности и обнаружения на основе полученных оценок элементарного канала утечки информации из структурно-сложной анализируемой системы в условиях повышения неопределенности. Метод базируется на моделях влияния элементарных каналов утечки информации из состава структурно-сложной анализируемой системы на потенциальную угрозу утечки ценной информации, теории графов, методе анализа иерархий и учитывает особенности утечки информации из автоматизированных систем обработки и анализа информации в современных условиях.

Список литературы

1. Хорев А.А. Организация защиты информации от утечки по техническим каналам // Специальная техника. – 2006. – № 3.

2. Симоньян Т.А. Средства вычислительной техники в защищенном варианте // Специальная техника. – 2002. – № 2.

3. Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам // Специальная техника. – 2006. – № 6.

4. Аникин И.В. Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть // Информационные технологии. – 2010. – № 1.

5. Франк Г., Фриш И. Сети, связь и потоки: [пер. с англ.] / под ред. Д.А. Поспелова. – М.: Связь, 1978.

6. Саати Т., Кернс К. Аналитическое планирование. Организация систем: [пер. с англ.]. – М. Радио и связь, 1991.

УДК 004.42

А.С. Федорова, И.В. Калуцкий

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

БЕЗОПАСНОСТЬ IT-СФЕРЫ ПРИ ВНЕДРЕНИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Показана необходимость внедрения технологии виртуализации во многие сферы использования информационных технологий.

Виртуализация за небольшой промежуток времени приобрела огромное значение в IT-сфере. Многие уже сумели оценить огромную экономию от внедрения технологии виртуализации в свой бизнес. И поэтому, чем больше появляется технологий, связанных с виртуализацией, тем больше внимания необходимо уделять для осуществления безопасности виртуальных сред. Существует мнение, что виртуализированная среда является более безопасной, нежели традиционная, так как существует изоляции между ВМ, и совсем немного известно об успешных атаках на гипервизор. Также считают, что для обеспечения безопасности виртуализированной среды необходимо использовать те же средства защиты информации, что и в традиционных физических средах. А суть состоит в том, что новая среда является более сложной, и добавление виртуализации в существующие традиционные среды требует новых подходов и решений для обеспечения надежной защиты всей системы. Поэтому необходимо использовать как уже известные

методы защиты информации для традиционной среды, так и новые, но уже ориентированные на защиту виртуальной среды.

В данной статье мы рассмотрим преимущества в безопасности IT-сферы, связанные с внедрением технологии виртуализации. Приведем некоторые преимущества для безопасности компьютеров при использовании технологии виртуализации:

- Централизованное хранение, используемое в виртуальных средах, предотвращает потерю важных данных, в случае если устройство потеряно, украдено или взломано.
- При должном изолировании виртуальных машин друг от друга неполадки и сбой в одной ВМ не повлияют на работоспособность сервисов и приложений других ВМ.
- При вирусной атаке на ВМ есть возможность выполнить откат к предыдущему состоянию, которое существовало до атаки.
- Благодаря виртуализации можно сократить аппаратное обеспечение, что, в свою очередь, приведет к улучшению физической безопасности, поскольку из-за меньшего количества устройств в конечном счете будет и меньше центров обработки данных.
- Виртуализация серверов позволяет улучшить обработку инцидентов сбоя сервера, возможно вернуться к предыдущему состоянию с целью изучения того, что произошло до и во время атаки.
- Улучшение системного и сетевого администрирования, а также управление доступом за счет четкого разграничения обязанностей администраторов безопасности, серверов и сети. Доступ к настройкам серверов виртуализации и иных объектов виртуальной инфраструктуры предоставляется только тем сотрудникам, которым он необходим для выполнения их должностных обязанностей (администраторам ВИ и администраторам ИБ). При этом управление настройками безопасности доступно только администраторам ИБ, а администрирование серверов виртуализации и иных объектов ВИ – только администраторам ВМ.
- Программное обеспечение гипервизора является небольшим и не очень сложным, поэтому проще проверить его код на наличие ошибок и дефектов, и соответственно площадь атак на гипервизор меньше и, следовательно, меньше возможных потенциальных уязвимостей.

- Виртуальные коммутаторы (vswitch) повышают уровень безопасности за счет устойчивости к таким видам атак, как подмена мас-адресов, атака на основе случайного кадра и другие атаки. Так как все настройки виртуальной машины хранятся в файлах ВМ, то соответственно и изменить мас-адрес может только администратор виртуальной среды.
- Экономия времени и средств при помощи масштабирования виртуальной среды посредством тиражирования эталонной настроенной виртуальной машины. Эта технология позволяет более эффективно управлять ОС для обеспечения соответствия требованиям политики безопасности организации.

Стоит отметить, что все вышесказанные преимущества рассматривались с позиции «при должном» изолировании виртуальных машин от хостов.

Тем не менее помимо проанализированных преимуществ при обеспечении безопасности одним из самых уязвимых мест виртуализированной среды является трудность изолирования ресурсов виртуальной машины и хостовой среды. Обеспечение безопасного взаимодействия виртуальной машины и хостовой среды является ключевым моментом при обеспечении защиты информационных процессов в виртуальной среде.

На более ранних этапах развития технологии виртуализации проблеме разделения ресурсов виртуальной и хостовой сред не уделялось особого внимания. На современном этапе в связи с возросшими требованиями к безопасности эта проблема является особенно актуальной. Большинство современных процессоров поддерживают аппаратную виртуализацию, что в совокупности с последними версиями программного обеспечения значительно повысило уровень разграничения ресурсов. Так, например, компания VMware, являющаяся ведущим поставщиком ПО виртуализации, уделяет данной проблеме особое внимание. 24 января 2014 года VMware представила документ под названием «Security of the VMware vSphere Hypervisor», который описывает инфраструктуру безопасности непосредственно хоста ESXi на уровне ядра и интерфейсов. Одним из важнейших механизмов целостного обеспечения безопасности архитектуры ESXi является изоляция ресурсов виртуальной и хостовой среды. Это включает в себя изоляцию памяти,

изоляцию устройств, изоляцию сети и сетевых устройств. Также данной проблеме уделяют внимание и такие известные компании в мире виртуализации, как Citrix, Microsoft.

В сфере повышения уровня изоляции ресурсов физической и виртуальной сред перспективным становится разделение различных информационных процессов между ними. Например, обработка конфиденциальной информации внутри виртуальной среды, а выполнение рутинных задач, как то информационный поиск в сети Интернет, обмен мгновенными сообщениями, в физической среде (под управлением хостовой операционной системы).

Подводя итог вышесказанному, можно утверждать, что внедрение технологии виртуализации во многие сферы использования информационных технологий сулит достаточно большие преимущества как в целом, так и в плане повышения уровня информационной безопасности при условии применения соответствующих средств защиты информации для виртуальных сред.

Список литературы

1. Amy Larsen DeCarlo, Myth vs. Reality: Controlling VM Sprawl in the Cloud [Электронный ресурс]. – 2012. – URL: http://searchcloudprovider.techtarget.com/tip/Myth-vs-reality-Controlling-VM-sprawl-in-the-cloud (дата обращения: 27.02.2014).

2. Mishchenko Dave. VMware ESXi: Planning, Implementation and Security. Cengage Learning, 2011.

3. Vmware [Электронный ресурс]. – 2014. – URL: http://www.vmware.com/ru. (дата обращения: 1.03.2014).

УДК 004.056.55

А.С. Уманец

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ПРОТОКОЛЫ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Показана возможность защиты персональных данных от того, чтобы они не попали в чужие руки.

XXI век привнес в жизнь простых людей массу новых возможностей и полезных изменений в бытовой жизни. Так, например, нам уже совсем не обязательно выходить из дома для того, чтобы совершить какую-либо покупку – достаточно открыть стра-

ницу в Интернете и нажать несколько клавиш. Электронные платежи все больше входят в нашу жизнь. Но удобство имеет и обратную сторону, т.к. не всегда пользователь системы электронных платежей может быть уверен в том, что его данные не попадут в чужие руки.

Участники электронной торговли всегда предпринимали множество мер для обеспечения информационной безопасности персональных данных в сети Интернет.

Прежде всего это обучение владельцев банковских и электронных карт минимальным навыкам для обеспечения собственной же безопасности: пользование только знакомыми и проверенными интернет-ресурсами, изучение порядка доставки товаров и предоставления услуг, проверка использования сертифицированных протоколов, гарантирующих безопасность передаваемой информации.

Безусловно, кроме этих элементарных методов защиты используются и специализированные технологические средства.

Так, например, ставший практически обязательным в интернет-торговле протокол SSL (Secure Socked Layer) позволяет всем участникам торговли спокойно передавать самую разную информацию. При попытке перехвата данных они будут закрыты шифром, взломать который за короткий промежуток времени попросту невозможно.

Протокол SSL использует технологию шифрования с открытым ключом и цифровые сертификаты для опознания сервера, участвующего в транзакции, а также защиты информации в процессе ее передачи от одной стороны к другой по каналам Интернета. При этом транзакции протокола SSL не требуют идентификации клиента.

Как именно происходит взаимодействие между клиентом и сервером? Вначале клиент посылает сообщение серверу, который отвечает и отправляет клиенту свой цифровой сертификат в качестве средства идентификации. Прежде чем продолжить транзакцию, клиент и сервер договариваются по поводу сеансовых ключей. Ключи сеанса – симметричные закрытые ключи, которые используются только в данной транзакции. Как только ключи выбраны, сеанс связи между клиентом и сервером продолжается, при этом используются ключи сеанса и цифровые сертификаты.

Итак, хотя протокол SSL надежно защищает информацию, передаваемую через Интернет, он не может уберечь частную информацию, хранимую на сервере продавца, например номера кредитных карт. Когда продавец получает данные кредитной карты вместе с заявкой на покупку, информация расшифровывается и сохраняется на сервере до тех пор, пока она не будет выполнена. Если сервер не защищен и данные не зашифрованы, то возможен несанкционированный доступ к персональным данным и дальнейшее использование их в мошеннических целях.

В дополнение к использованию протокола шифрования передаваемых данных используются такие хорошо известные способы идентификации держателя карты, как проверка CVV2/CVK2-кодов (CVV2-код для карт платежной системы Visa, а CVK2 – для MasterCard).

К способам идентификации стоит добавить проверку адреса AVS (Address Verification Service). Данная процедура в большей степени характерна для североамериканского рынка электронной коммерции, но тем не менее с ней приходилось сталкиваться и держателям карт российских банков, пытавшимся воспользоваться картами для оплаты товаров с доставкой на территории США.

Также необходимо отметить, что вопрос безопасности волнует не только держателя карты, производящего оплату товара в интернет-магазине, но и интернет-магазин, а больше всего — платежные системы, которые вкладывают огромные средства для обеспечения безопасности платежей и защиты от мошенничества.

Многочисленные попытки международных платежных систем сделать расчеты в области электронной коммерции максимально безопасными привели к появлению разработанного платежной системой Visa International протокола 3-D Secure.

Технология 3-D Secure представляет собой протокол аутентификации владельца карты при проведении покупок в сети Интернет, предназначенный для обеспечения безопасности интернет-платежей: проверка личности осуществляется в онлайн-режиме.

Основным действующим принципом технологии 3-D Secure стала гарантия безопасности проведения расчетов в системе электронной коммерции.

Реализуется технология 3-D Secure на основе трех доменов, в которых начинается и завершается жизненный цикл транзакции.

Это домен эмитента, в котором происходит аутентификация держателя, домен эквайера, включающий в себя банк-эквайер и интернет-магазин, и, наконец, домен взаимодействия, содержащий службы и сервисы платежной системы.

Протокол 3-D Secure работает следующим образом.

Во-первых, происходит проверка личности владельца карты в реальном времени, которая начинается после ввода номера карты на платежной странице электронного магазина, откуда покупатель перенаправляется на сервер своего банка-эмитента. Для проверки используется пароль, известный только владельцу карты и банку.

Во-вторых, банком-эмитентом по результатам проверки формируется ответное сообщение, которое банк-эмитент защищает от изменений, используя цифровую подпись.

В-третьих, происходит защита персональных данных пользователя, для чего используются защищенные страницы платежного сервера, на котором сохраняется введенная информация. В то же время получатель платежа не имеет доступа к этой информации, что является лучшей защитой от ее хищения.

Таким образом, 3-D Secure не только обеспечивает безопасное проведение платежа, но и разграничивает риски участников транзакции за счет четкого разделения функций при обработке платежной операции: банк-эмитент проверяет личность держателя карты, поскольку именно он располагает информацией о клиенте, а банк-эквайер автоматически организует связь с системой аутентификации эмитента, используя для этого сервисы платежных систем.

Доля торговых сделок, осуществляющихся через Интернет, неуклонно растет из года в год, увеличиваются обороты от продажи товаров и услуг в Сети, пропорционально растет и количество мошеннических операций. Именно поэтому развитие способов защиты электронных платежей становится крайне важным на сетевом рынке и, возможно, вскоре будет занимать больший сегмент в сфере информационной безопасности.

---

1. Ревенков П.В. Защита информации в национальной платежной системе // Рассчеты и операционная работа в коммерческом банке. – 2013. – Т. 1027. – №4. – С.85-87

2. Безопасность по протоколу. Что такое 3-DSecure? [Электронный ресурс]. – URL: http://blog.chronopay.ru/?p=217.

СЕКЦИЯ 5
ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ЦЕЛЯХ РАЗВИТИЯ РЕГИОНА

УДК 621.397.13

Е.Г. Лозовская

Южный федеральный университет, Ростов-на-Дону

МОДЕЛЬ СИСТЕМЫ СТЕРЕОТЕХНИЧЕСКОГО ЗРЕНИЯ ДЛЯ ИЗМЕРЕНИЯ РАЗНОВЫСОТНОСТИ ГЕОМЕТРИЧЕСКИХ ОБЪЕКТОВ

Представлена модель системы стереотехнического зрения для измерения разновысотности геометрических объектов.

Цель исследований состоит в измерении и оценке погрешности бесконтактного определения разновысотности головок ТВС на основе реконструкции трехмерной сцены по серии стереопар изображений от видеокамер на ПЗС-матрицах с разных ракурсов наблюдения в водной среде в активной зоне реактора энергоблока АЭС.

Научная новизна состоит в том, что впервые разработана математическая модель системы стереотехнического зрения, основанная на основе одной регистрирующей видеокамеры на ПЗС-матрице, которая позволяет измерить координаты точек в глобальной системе координат (ГСК) относительно каждого положения видеокамеры.

Основным направлением в атомной энергетике является создание высоконадежных комплексов для управления технологическими процессами цифрового телевидения. Фактором, влияющим на безопасность атомной электростанции, является разновысотность головок тепловыделяющих сборок (ТВС), характеризующая их искривление, которое при определенных значениях делает невозможным эксплуатацию активной зоны реактора.

Совершенствование бесконтактных методов определения разновысотности головок тепловыделяющей сборки (ТВС) атомного реактора на основе реконструкции трехмерных изображений предполагает разработку математических моделей стереосистем видеокамер для оценки методической погрешности измерения геометри-

ческих параметров, обусловленной несовершенством метода измерений и упрощениями, допущенными при косвенных измерениях. Основным критерием качества контроля разновысотности головок ТВС является минимизация погрешности измерения.

Исследуемым объектом является сота ТВС с 7-ю головками, представляющими собой прямые полые цилиндры, внешний и внутренний диаметр которых фиксированы. Модель проецирующей видеокамеры характеризуется фокусным расстоянием, размерами и разрешением матрицы.

Разработанная в среде MathCad модель ориентирована на использование видеокамеры D20-017 (Система телевизионная специальная СТС-ТТО-3).

Головки ТВС при виде сверху представляют собой окружности, поэтому при создании идеализированной модели сота представляется регулярной структурой в виде правильного шестиугольника с семью точками в центре и его вершинах на окружности радиусом R, являющимися ее центрами тяжести. Измерение разновысотности геометрических объектов осуществляется применением методов фотограмметрии на основе стереопары изображений.

Видеокамера перемещается по кругу и последовательно формирует изображения с 6-ти ракурсов. Для формирования трехмерной информации о сцене используются 15 стереопар, полученных как комбинации изображений 6-ти положений видеокамер. Оптический центр видеокамеры располагается на окружности, центром которой является ось штанги. Отметим, что ось штанги является перпендикуляром к плоскости шестиугольника в его геометрическом центре. Высота подвеса видеокамеры над сотой определяется исходя из одновременного наблюдения всех 7 точек в «соте».

В предложенной математической модели трехмерные координаты 7-ми точек задаются в глобальной системе координат в виде матриц для всех положений видеокамеры.

Переход от глобальной к стандартной системе координат осуществляется поворотом координатных осей и последующим смещением начала координат.

В стандартной системе координатами проекций точек трехмерного пространства являются координаты (x,y) в плоскости изображения видеокамеры.

Предложенная математическая модель позволяет определять номер пикселя, в котором находится центр тяжести головки ТВС.

При этом, имея координаты точек в естественных единицах фотоприемника в дискретных системах координат, можно вычислить векторы трехмерных координат точек в стандартной системе координат видеокамеры. Координаты точек в разных положениях видеокамеры будут различны. Это объясняется смещением оптической оси видеокамеры.

И, наконец, модель регистрирующей видеокамеры рассчитывает координаты точек в глобальной системе для всех положений видеокамеры, которые являются несколько отличными от истинных. Это связано с дискретизацией при определении координат точек в пикселях.

При этом модель позволяет определить абсолютную и относительную погрешности измерений, а также дисперсию и математическое ожидание результатов измерений.

Разработанная модель формирования пары стереоизображений одной видеокамерой позволяет установить связи между координатами точек сцены и их изображениями, определить параметры системы регистрации и трехмерной структуры сцены группы ТВС.

Получены соотношения для пересчета координат из глобальной в стандартную систему координат; рассчитаны координаты в естественных единицах фотоприемника; реконструированы трехмерные координаты точек в стандартной системе на основе координат их проекций в изображениях стереопары; произведен обратный пересчет координат из стандартной системы координат в глобальную.

Разработанная модель позволяет оценить влияние на погрешность параметров системы: радиуса вращения видеокамеры вокруг соты, высоты подвеса (угла наклона видеокамеры), фокусного расстояния, размерности и разрешения матрицы.

Кроме того, в модели исследуется влияние на погрешность измерения разновысотности неточности установки видеокамер, а

именно углового смещения видеокамеры по вертикали и по горизонтали.

Разработанная модель может быть применена как для видеокамер на ПЗС-матрицах, так и для видеокамер на видиконах.

Список литературы

1. Методы компьютерной обработки изображений / под ред. В.А. Сойфера. – М.: Физматлит, 2001. – 784 с.

2. Балабаев С.Л., Радецкий В.Г., Румянцев К.Е. Телеметрический метод контроля разновысотности цилиндрических объектов // Известия ЮФУ. Технические науки. – 2008. – Т. 80. – № 3. – С. 94-110.

3. Балабаев С.Л., Радецкий В.Г., Румянцев К.Е. Видеосистема бесконтактного контроля разновысотности объектов // Известия ЮФУ. Технические науки. – 2006. –Т. 64. – № 9-1. – С. 157-161.

УДК 621.396.9; 528.7

В.Г. Андронов, Н.И. Черняева

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

АППРОКСИМАЦИЯ КЕПЛЕРОВСКОЙ МОДЕЛИ НЕВОЗМУЩЁННОГО ДВИЖЕНИЯ КОСМИЧЕСКИХ АППАРАТОВ

В статье представлена методика аппроксимации координат и составляющих скорости орбитального движения КА степенными временными полиномами в задачах фотограмметрической обработки космических изображений.

Кеплеровская модель невозмущённого движения космического аппарата (КА) дистанционного зондирования Земли (ДЗЗ) позволяет определять его геоцентрические координаты и составляющие скоростей и значения шести элементов орбиты (большой полуоси, эксцентриситета, наклонения орбиты, аргумента перигея, истинной аномалии на экваторе, долготы восходящего узла) на заданные моменты времени по их известным начальным значениям на момент включения t_0 съёмочной аппаратуры в заданную дату съёмки [1]. Однако используемые при этом зависимости имеют тригонометрический вид и алгоритмический характер и достаточно громоздки в вычислительном отношении, что заставляет искать эквивалентные им модели, имеющие меньший уровень вычислительных затрат. Одним из эффективных подходов является применение

аппроксимационных зависимостей [2]. В этой связи цель работы состоит в исследовании зависимости уровня методических ошибок от степени используемых полиномов.

В соответствии с этим зададим (табл.1) координаты и составляющие скорости движения КА ДЗЗ в космическом пространстве на дату 1 марта 2013 года и t_0 =4 часа 00 минут 15,364 секунды.

Таблица 1

Начальные значения координат и составляющих скорости движения КА ДЗЗ

X, м	Y, м	Z, м	$\dot{X}$,м/с	$\dot{Y}$,м/с	$\dot{Z}$,м/с
3281154,09	2684186,65	5226990,03	–6773,88	305,53	4126,35

Далее в соответствие с кеплеровской моделью невозмущённого движения КА рассчитаем значения геоцентрических координат и составляющих скорости движения КА ДЗЗ (табл.2) с интервалом времени в одну секунду и длительности 60 секунд.

Таблица 2

Табличные значения координат и составляющих скорости КА

Время, с	X	Y	Z	X`	Y`	Z`
14415,364	3281154,095	2684186,654	5226990,035	–6773,88	305,533	4126,352
14416,364	3274584,908	2684251,061	5231106,019	–6778,164	301,55	4119,525
14417,364	3268011,406	2684311,97	5235215,216	–6782,439	297,567	4112,693
14418,364	3261433,597	2684369,381	5239317,619	–6786,705	293,583	4105,856
14419,364	3254751,727	2684424,084	5243475,227	–6791,027	289,538	4098,91
14420,364	3248165,264	2684474,446	5247563,925	–6795,275	285,553	4092,063
14421,364	3241574,52	2684521,31	5251645,814	–6799,514	281,568	4085,21
14422,364	3234979,501	2684564,675	5255720,89	–6803,745	277,583	4078,351
14423,364	3228380,217	2684604,542	5259789,146	–6807,967	273,597	4071,488
14424,364	3221776,675	2684640,91	5263850,578	–6812,179	269,611	4064,619
14425,364	3215168,885	2684673,78	5267905,18	–6816,383	265,624	4057,744
14426,364	3208556,853	2684703,151	5271952,947	–6820,578	261,638	4050,865
14427,364	3201940,589	2684729,023	5275993,874	–6824,764	257,651	4043,98
14428,364	3195320,101	2684751,396	5280027,956	–6828,941	253,663	4037,09

Продолжение табл. 2

Время, с	X	Y	Z	X`	Y`	Z`
14429,364	3188695,397	2684770,27	5284055,188	–6833,11	249,675	4030,195
14430,364	3182066,485	2684782,458	5288075,565	–6837,269	245,687	4023,295
14431,364	3175332,839	2684797,675	5292149,839	–6841,482	241,638	4016,284
14432,364	3168695,473	2684805,999	5296156,385	–6845,624	237,65	4009,373
14433,364	3162053,924	2684810,824	5300156,06	–6849,756	233,661	4002,457
14434,364	3155408,201	2684812,149	5304148,86	–6853,879	229,671	3995,536
14435,364	3148758,312	2684809,976	5308134,778	–6857,994	225,682	3988,609
14436,364	3142104,264	2684804,303	5312113,81	–6862,099	221,692	3981,678
14437,364	3135446,067	2684795,13	5316085,951	–6866,196	217,702	3974,741
14438,364	3128783,729	2684785,646	5320051,196	–6870,284	213,711	3967,799
14439,364	3122117,258	2684766,287	5324009,539	–6874,362	209,721	3960,852
14440,364	3115446,662	2684746,617	5327960,976	–6878,432	205,73	3953,9
14441,364	3108771,95	2684723,447	5331905,501	–6882,493	201,738	3946,942
14442,364	3102093,13	2684696,777	5335843,11	–6886,544	–6886,54	3939,98
14443,364	3095410,21	2684666,608	5339773,797	–6890,587	193,755	3933,012
14444,364	3088621,849	2684632,403	5343756,955	–6894,682	189,703	3925,934
14445,364	3081930,694	2684595,182	5347673,679	–6898,706	185,711	3918,956
14446,364	3075235,464	2684554,462	5351583,466	–6902,722	181,718	3911,973
14447,364	3068536,168	2684510,242	5355486,312	–6906,728	177,725	3904,985
14448,364	3061832,814	2684462,522	5359382,21	–6910,726	173,733	3897,992
14449,364	3055125,41	2684411,303	5363271,158	–6914,714	169,739	3890,994
14450,364	3048413,966	2684356,585	5367153,148	–6918,694	165,746	3883,99
14451,364	3041698,489	2684298,367	5371028,177	–6922,664	161,753	3876,982
14452,364	3034978,989	2684236,65	5374896,239	–6926,626	157,759	3869,969
14453,364	3028255,472	2684171,434	5378757,33	–6930,578	153,765	3862,951
14454,364	3021527,947	2684102,718	5382611,444	–6934,521	149,771	149,771
14455,364	3014796,424	2684030,503	5386458,577	–6938,455	145,777	3848,899
14456,364	3008060,91	2683954,789	5390298,723	–6942,381	141,782	3841,866
14457,364	3001321,414	2683875,576	5394131,879	–6946,297	137,788	3834,828
14458,364	2994475,74	2683791,583	5398015,956	–6950,263	133,732	133,732
14459,364	2987728,245	2683705,318	5401835,008	–6954,161	129,737	3820,63

Окончание табл. 2

Время, с	X	Y	Z	X`	Y`	Z`
14460,364	2980976,793	2683615,555	5405647,053	–6958,049	125,742	3813,577
14461,364	2974221,392	2683522,292	5409452,088	–6961,929	121,747	3806,519
14462,364	2967462,052	2683425,53	5413250,107	–6965,8	117,751	3799,456
14463,364	2960698,78	2683325,27	5417041,106	–6969,661	113,756	3792,388
14464,364	2953931,585	2683221,511	5420825,078	–6973,513	109,76	3785,315
14465,364	2947160,476	2683114,253	5424602,021	–6977,357	105,764	3778,237
14466,364	2940385,46	2683003,497	5428371,928	–6981,191	101,768	3771,155
14467,364	2933606,546	2682889,242	5432134,795	–6985,016	97,772	3764,067
14468,364	2926823,744	2682771,489	5435890,617	–6988,832	93,776	3756,975
14469,364	2920037,06	2682650,237	5439639,389	–6992,638	89,78	3749,877
14470,364	2913246,504	2682525,488	5443381,107	–6996,436	85,783	3742,775
14471,364	2906452,085	2682397,24	5447115,765	–7000,224	81,787	3735,668
14472,364	2899653,81	2682265,494	5450843,359	–7004,004	77,79	3728,557
14473,364	2892851,688	2682130,251	5454563,884	–7007,774	73,794	3721,44
14474,364	2885942,578	2681989,38	5458333,546	–7011,592	69,736	3714,211
14475,364	2879132,73	2681847,088	5462039,811	–7015,344	65,739	3707,084

Полученные значения представляют собой множество табличных значений соответствующих координатных функций, зависящих от времени, что допускают их аппроксимацию любыми известными методами. В работе представлены результаты аппроксимации данных таблицы 2 методом наименьших квадратов со степенью полинома 1, 2 и 3.

Представление координатных функций в виде полиномов второй и третьей степени выглядит следующим образом:

$$\begin{aligned} X(t) &= a_0{}^X + a_1{}^X \cdot \mathrm{t} + a_2{}^X \cdot \mathrm{t}^2; \\ Y(t) &= a_0{}^Y + a_1{}^Y \cdot \mathrm{t} + a_2{}^Y \cdot \mathrm{t}^2; \\ Z(t) &= a_0{}^Z + a_1{}^Z \cdot \mathrm{t} + a_2{}^Z \cdot \mathrm{t}^2; \end{aligned} \quad (1)$$

$$\begin{aligned} X(t) &= a_0{}^X + a_1{}^X \cdot \mathrm{t} + a_2{}^X \cdot \mathrm{t}^2 + a_3{}^X \cdot \mathrm{t}^3; \\ Y(t) &= a_0{}^Y + a_1{}^Y \cdot \mathrm{t} + a_2{}^Y \cdot \mathrm{t}^2 + a_3{}^Y \cdot \mathrm{t}^3; \\ Z(t) &= a_0{}^Z + a_1{}^Z \cdot \mathrm{t} + a_2{}^Z \cdot \mathrm{t}^2 + a_3{}^Z \cdot \mathrm{t}^3, \end{aligned} \quad (2)$$

где $a_0{}^X, a_1{}^X, \ldots, a_3{}^Z$ – коэффициенты полинома.

Значения СКО для координатных функций представлены в таблице 3.

Таблица 3

Ошибки аппроксимации координат КА

№ п/п	Функции составляющих скоростей	СКО аппроксимации, м/с		
		полином 1 степени, м	полином 2 степени, м	полином 3 степени, м
1	$\dot{X}(t)$	5,23	0,0061	0,00043
2	$\dot{Y}(t)$	4,19	0,0054	0,00037
3	$\dot{Z}(t)$	6,15	0,0082	0,00075

Для получения полиномиальных функций составляющих скоростей КА ДЗЗ второго или третьего порядка продифференцируем соответствующие координатные функции (1) и (2) по времени. Получим:

$$\begin{aligned} \dot{X}(t) &= a_1 + 2 \cdot a_2 \cdot \mathrm{t}; \\ \dot{Y}(t) &= a_1 + 2 \cdot a_2 \cdot \mathrm{t}; \\ \dot{Z}(t) &= a_1 + 2 \cdot a_2 \cdot \mathrm{t}. \end{aligned} \qquad (3)$$

$$\begin{aligned} \dot{X} &= a_1 + 2 \cdot a_2 \cdot \mathrm{t} + 3 \cdot a_3 \cdot \mathrm{t}^2; \\ \dot{Y} &= a_1 + 2 \cdot a_2 \cdot \mathrm{t} + 3 \cdot a_3 \cdot \mathrm{t}^2; \\ \dot{Z} &= a_1 + 2 \cdot a_2 \cdot \mathrm{t} + 3 \cdot a_3 \cdot \mathrm{t}^2. \end{aligned} \qquad (4)$$

Значения СКО для составляющих скоростей приведены в таблице 4.

Таблица 4

СКО аппроксимации составляющих скорости КА

№ п/п	Координатная функция	СКО аппроксимации, м		
		полином 1 степени, м	полином 2 степени, м	полином 3 степени, м
1	X(t)	523.9	2,51	0,0015
2	Y(t)	304.6	2,44	0,0029
3	Z(t)	851.9	6,37	0.0064

Анализ данных таблиц 3 и 4 позволяет сделать вывод о том, что при аппроксимации координат КА необходимо выбирать сте-

пень полинома, не меньшую, чем третья, а скоростей – не меньшую, чем вторая.

---

1. Урмаев М.С. Космическая фотограмметрия. – М.: Недра, 1989.
2. Титаров П.С. Практические аспекты фотограмметрической обработки сканерных космических снимков высокого разрешения // ГИС- Ассоциация. Информационный бюллетень. – 2004. – № 3 (45). – С. 25-26, 51.

УДК 621.396.9

В.Г. Андронов, П.А. Шашорин

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

МЕТОДИКА МОДЕЛИРОВАНИЯ СПУТНИКОВОЙ НАВИГАЦИИ НАЗЕМНЫХ ПОДВИЖНЫХ ОБЪЕКТОВ

Представлена методика моделирования процесса определения координат в задачах высокоточной глобальной навигации наземных подвижных объектов.

Сущность моделирования процессов определения координат наземных подвижных объектов заключается в следующем: на карте прокладывается контрольный маршрут движения наземного подвижного объекта из пункта А в пункт В и в заданные моменты времени фиксируются его геодезические координаты B,L,H, в соответствии с которыми по известным формулам [1] определяются его контрольные геоцентрические координаты X,Y,Z; на эти же моменты времени из доступных каталогов берутся известные геодезические и рассчитываются геоцентрические координаты спутников GPS; по координатам спутников GPS и контрольным координатам подвижного объекта в заданные моменты времени рассчитываются значения псевдодальностей от спутников GPS до подвижного объекта, которые в реальных условиях вычисляются по времени задержки прохождения радиотехнических сигналов от спутников до объекта; после этого по значениям псевдодальностей определяются геоцентрические координаты подвижного объекта и сравниваются с контрольными.

В соответствие с этим будем считать, что наземный подвижный объект начинает движение из города Курска в город Москву

15 апреля 2013 года в 08:00 и до момента прибытия в 18.00 попадает в зоны обзора различных спутников GPS (табл.1).

Таблица 1

Координаты центров зон обзора спутников GPS

Название спутника	Гринвичские геоцентрические координаты спутника GPS		
	X, м	Y, м	Z, м
8:00 Курск (Контрольная точка №1)			
GPS BIIA-21	-11326527,8024074	18677004,1979719	14500612,9760462
GPS BIIA-24	22203283,0635011	13569117,0824612	6115590,04737191
GPS BIIA-25	24979127,7188997	9246057,42843908	2066099,70889199
GPS BIIR-4	22248472,8957852	13957955,8926266	3516941,48754271
GPS BIIRM-1	-9022579,29623788	18254839,3912322	17392884,8530336
GPS BIIRM-4	-24292834,2923645	1982167,29040047	10828581,5770274
8:20 (Контрольная точка №2)			
GPS BIIA-21	-3047211,82156515	4296731,23117842	3619240,90136134
GPS BIIA-24	5297832,63721903	3199692,00565093	1618146,76163496
GPS BIIR-4	5375914,2994267	3359609,39291627	866956,263434361
GPS BIIRM-1	-1920349,79574373	4312933,15609864	4304399,41588872
GPS BIIRM-4	-5864801,10543766	581746,224348806	2483549,44960735
8:43 Контрольная точка №3			
GPS BIIA-21	-30465512,87542371	4295491,75623109	3316540,90136112
GPS BIIR-4	5375764,2999184	3356193,39751947	866347,263464103
GPS BIIRM-1	-1920349,79642072	4307691,15642368	4304126,41533451
GPS BIIRM-4	-5864801,10714269	581990,226519032	2483532,44963498
9:00 Фатеж (Контрольная точка №4)			
GPS BIIF-1	-19699553,715145	16302158,8816848	6942950,77291255
GPS BIIF-3	-16727214,4628151	4496315,15206534	20136785,1626179
GPS BIIR-11	25213435,939185	8729407,27499415	2510229,29030945
GPS BIIR-5	10629011,8347578	21922977,0744215	10930055,8751146
GPS BIIRM-2	7017167,88844612	25382722,4024335	2094273,77164468
GPS BIIRM-3	-20055131,6497549	6398711,99662913	16033073,9562332
10:00 (Контрольная точка №5)			
GPS BIIF-3	-16727214,4628151	4496315,15206534	20136785,1626179
GPS BIIR-11	25213435,939185	8729407,27499415	2510229,29030945
GPS BIIR-5	10629011,8347578	21922977,0744215	10930055,8751146
GPS BIIRM-2	7017167,88844612	25382722,4024335	2094273,77164468
GPS BIIRM-3	-20055131,6497549	6398711,99662913	16033073,9562332

Продолжение табл. 1

Название спутника	Гринвичские геоцентрические координаты спутника GPS		
	X, м	Y, м	Z, м
11:00 (Контрольная точка №6)			
GPS BIIF-3	-16727214,4628151	4496315,15206534	20136785,1626179
GPS BIIR-11	25213435,939185	8729407,27499415	2510229,29030945
GPS BIIR-5	10629011,8347578	21922977,0744215	10930055,8751146
GPS BIIRM-2	7017167,88844612	25382722,4024335	2094273,77164468
12:00 Орел (Контрольная точка №7)			
GPS BIIF-2	22060986,669585	14055589,4365436	4867783,45710414
GPS BIIR-8	384090,132999701	26350359,4743541	959979,726127139
GPS BIIRM-1	20830239,251264	16004697,9976514	3142814,7566293
GPS BIIRM-3	11140595,3667664	18896985,5721238	15094355,8887925
GPS BIIRM-5	22000671,5275123	1781533,33608469	14794875,6886809
12:20 (Контрольная точка №8)			
GPS BIIF-2	22060875,666125	14059143,4365436	4866043,45710414
GPS BIIR-8	385690,132999701	26350091,4743285	957731,726613063
GPS BIIRM-1	2067098,251006	16125797,9954451	3142690,75612368
GPS BIIRM-3	11140595,3667664	18896985,5721238	15094355,8887925
GPS BIIRM-5	2204471,5273419	1784590,33606517	1411397,68130854
12:40 (Контрольная точка №9)			
GPS BIIR-8	384876,267998701	26350456,0963541	959989,787627139
GPS BIIRM-1	20830375,765974	16004596,0976514	3142756,7456393
GPS BIIRM-3	11140576,4977667	18896864,9751269	15094475,8974984
GPS BIIRM-5	22001065,5675129	1781875,34568485	14794786,6799809
13:00 Мценск (Контрольная точка №10)			
GPS BIIA-10	7439186,58767184	25790221,9660555	638386,568455711
GPS BIIF-1	16201507,1688773	15420293,0047461	14354711,9938377
GPS BIIRM-6	25984694,8970774	6069349,6935991	1424616,81729673
GPS BIIRM-8	447426,559160516	24072785,6028583	11025761,5917982
13:20 (Контрольная точка №11)			
GPS BIIA-10	7439264,59564184	25790123,9875957	638465,587986717
GPS BIIF-1	-16201876,9875775	15420375,0164478	14353754,8765376
GPS BIIRM-6	25984785,8874778	6069486,9875995	1424785,81875677
GPS BIIRM-8	-447678,345660516	24072798,6987583	11025876,9858988

Продолжение табл. 1

Название спутника	Гринвичские геоцентрические координаты спутника GPS		
	X, м	Y, м	Z, м
13:45 (Контрольная точка №12)			
GPS BIIA-10	7439698,5867184	25790784,0530554	638154,501355711
GPS BIIF-1	-16201876,8548745	15420365,0865461	14354865,9097497
GPS BIIRM-6	25984875,8875774	6069864,8753991	1424985,97649675
GPS BIIRM-8	-447875,56456086	24072874,6985809	11025865,5896982
14:10 Плавск (Контрольная точка №13)			
GPS BIIA-23	25358287,4332578	6856199,82593822	4568667,27299933
GPS BIIA-25	-8466287,44499161	24823817,4882265	2826981,14238825
GPS BIIA-28	26467822,0474024	2157774,73810882	4286506,14281596
GPS BIIR-4	13284727,1588682	22312244,9051963	5937143,74400999
GPS BIIR-9	-24350063,981341	4800820,72733922	10724788,3015848
GPS BIIRM-2	-24420118,2523501	7813088,61350145	7642423,62807119
14:30 (Контрольная точка №14)			
GPS BIIA-23	25358657,5765675	6856356,82567822	4568675,56749945
GPS BIIA-25	-8466356,45689161	24823678,4678265	2826990,16788825
GPS BIIA-28	26467678,0670024	2157876,75887882	4286786,14678596
GPS BIIR-4	13289789,1789656	22312789,9078963	5938900,74890999
GPS BIIRM-2	-24428745,2967556	7813176,65670187	7645768,69879118
14:50 Щекино (Контрольная точка №15)			
GPS BIIA-14	12783786,0429926	21156677,2539255	8592096,10094818
GPS BIIA-23	25875450,6904932	6133246,34487706	2841729,02576315
GPS BIIR-9	-20652324,5863445	6225866,21872855	16392986,0721845
GPS BIIRM-5	-7353098,43991361	18807328,5681201	17332396,2643762
GPS BIIRM-7	-20012096,6146915	2749429,63065514	17203787,6117397
15:00 (Контрольная точка №16)			
GPS BIIA-14	12783082,0428754	21156713,2537532	8592095,10009123
GPS BIIA-23	25875134,6950963	6131234,34409872	2841208,02585326
GPS BIIR-9	-20609713,5846582	6228452,21813564	1631659,07649472
GPS BIIRM-5	-73507654,43984731	18808547,5688561	17331845,2648366
GPS BIIRM-7	-20076856,6146915	2749439,63063414	17421787,6134597

Продолжение табл. 1

Название спутника	Гринвичские геоцентрические координаты спутника GPS		
	X, м	Y, м	Z, м
15:15 Тула (Контрольная точка №17)			
GPS BIIA-22	20589472,6019246	1140712,72861704	16374229,1160638
GPS BIIR-11	8668631,58470128	24264712,8801139	5360804,97847376
GPS BIIR-12	1151986,59153772	25665252,0866705	5930279,89546356
GPS BIIR-13	21810266,7525779	13966758,6754846	4674584,58590231
GPS BIIR-5	22359579,3969705	12629791,3593323	6550693,31144931
GPS BIIR-9	-17744181,4153293	7598128,45183569	19015938,3349954
GPS BIIRM-5	-6464793,63093239	21663896,6674927	14033151,6638117
GPS BIIRM-7	-22159889,8215555	4841726,52786138	13834417,1564809
15:40 (Контрольная точка №18)			
GPS BIIR-11	-8668561,58409632	24286753,8801257	5360009,97856382
GPS BIIR-12	1151124,59145741	25661511,0866196	5930345,89540574
GPS BIIR-13	2180594,7525439	13966424,6736646	4543257,58594578
GPS BIIRM-5	-6467641,63068853	2165532,66749752	14033451,6637146
GPS BIIRM-7	-2215953,82135908	4841643,52787609	13836731,1564128
16:00 (Контрольная точка №19)			
GPS BIIR-11	-86675631,5846539	24264652,8809756	5360927,97234801
GPS BIIR-5	22359712,3969342	12629093,3593323	6550693,31144976
GPS BIIR-9	-17744891,4178993	7598873,45134269	1901127,33497689
GPS BIIRM-5	-64645318,6306547	21663896,6674998	14033151,6638176
GPS BIIRM-7	-22157569,8211255	4841874,52786138	13837617,1569321
16:30 Серпухов (Контрольная точка №20)			
GPS BIIA-26	25345402,8311559	8672976,18849671	399468,67190553
GPS BIIR-2	3874393,16056582	26186419,9008044	964435,610199706
GPS BIIR-7	-17122606,6162022	15859926,8899724	13394656,6443756
GPS BIIR-8	-22135212,2008075	2328848,17726276	14734603,9838621
17:00 (Контрольная точка №21)			
GPS BIIA-26	25345402,8312341	86723844,18849384	39956433,6719764
GPS BIIR-2	38744453,1004782	26189465,9004544	96444344,6101997
GPS BIIR-7	-17125876,6163485	15854957,8847624	13393556,6434556
GPS BIIR-8	-22756532,2454075	23275538,1784276	14733503,9833214

Окончание табл. 1

Название спутника	Гринвичские геоцентрические координаты спутника GPS		
	X, м	Y, м	Z, м
17:30 Подольск (Контрольная точка №22)			
GPS BIIA-24	-18889536,0130266	5704382,24002605	18032163,5309488
GPS BIIR-10	-20048753,2149245	11166510,5236256	13681459,9277418
GPS BIIR-9	-2293774,32691171	20322332,2290648	17218750,5484374
GPS BIIRM-1	15618083,3838147	20064117,5475559	7865485,73658794
GPS BIIRM-8	25987475,1893145	2724561,08787339	5132214,162729
17:40 (Контрольная точка №23)			
GPS BIIA-24	-1294636,01302343	5704746,24746605	18032345,5303588
GPS BIIR-10	-3456753,23562453	14566510,5245556	13461459,9277412
GPS BIIR-9	-2293456,32345856	20556332,2294846	17284753,5484653
GPS BIIRM-1	15618743,3838347	20068467,5434559	78635385,7384645
18:00 Москва (Контрольная точка №24)			
GPS BIIA-24	-20705625,7503584	8928606,3400784	14405543,5282163
GPS BIIA-25	-19833898,5792756	2575269,65750626	17073969,1197339
GPS BIIR-10	-16537059,5371604	11705944,4930378	17434232,6793798
GPS BIIR-9	-228496,415241569	23048329,837983	13272267,5816531
GPS BIIRM-1	15814682,1598288	21345501,8694601	2338479,81049588
GPS BIIRM-8	26543927,5148559	2179836,13552243	471661,155611199

Для расчета псевдодальностей от навигационных спутников до наземных объектов будем использовать известную формулу

$$R = \sqrt{(X - X_n)^2 + (Y - Y_n)^2 + (Z - Z_n)^2}, \quad (1)$$

где X, Y, Z – координаты наземного объекта;

X_n, Y_n, Z_n – координаты n-го навигационного спутника.

Для примера, зная среднюю скорость движения подвижного объекта и траекторию его движения, рассчитаем его положение на маршруте в 12:00.

Пусть объект в этот момент времени находится в контрольной точке №7 (г. Орел) с координатами

X=3115641,3; Y=2268100,4; Z= 5065441,4.

В это время (12.00) ближайшими навигационными спутниками к подвижному объекту будут спутники (см. табл.1) со следующими координатами:

X_1= 22060986,6; Y_1 = 14055589,4; Z_1 = 4867783,4;

X_2= 384090,1; Y_2 = 26350359,4; Z_2 = 959979,7;

X_3=20830239,2; Y_3 = 16004697,9; Z_3 = 3142814,7;

X_4=11140595,3; Y_4 = 18896985,5; Z_4 = 15094355,8.

Далее рассчитываем псевдодальности в 12:00:

R_1^2 = 412664918728794,8 м;

R_2^2 = 609019521189688,4 м;

R_3^2 = 380067314403933,2 м;

R_4^2 = 661495019961029,5 м.

Тогда система уравнений для определения координат искомой точки будет иметь следующий вид [2]:

$$412664918728794,8 = (X - 22060986,6)^2 + (Y - 14055589,6)^2 + (Z - 4867783,4)^2;$$

$$609019521189688,4 = (X - 384090,1)^2 + (Y - 26350359,4)^2 + (Z - 959979,7)^2;$$

$$380067314403933,2 = (X - 20830239,2)^2 + (Y - 16004697,9)^2 + (Z - 3142814,7)^2;$$

$$661495019961029,5 = (X - 11140595,3)^2 + (Y - 18896985,5)^2 + (Z - 15094355,8)^2.$$

Решая данную систему уравнений, получаем координаты подвижного объекта в момент времени 12.00:

X = 3115585,3; Y = 2268075,3; Z = 5065569,9.

Аналогичным образом рассчитываются координаты подвижного объекта для всех контрольных точек.

Результаты вычисления разности расчетных и контрольных координат приведены в таблице 2.

Таблица 2

Абсолютные ошибки вычисления координат подвижного объекта

Контрольная точка	ΔX	ΔY	ΔZ
Курск (Контрольная точка №1)	46,0	30,9	59,9
Контрольная точка №2	-11,5	-100,5	-34,9
Контрольная точка №3	9,6	36,3	-15,4

Окончание табл. 2

Контрольная точка	ΔX	ΔY	ΔZ
Фатеж (Контрольная точка №4)	-82,4	104,8	61,4
Контрольная точка №5	25,1	-13,7	-75,9
Контрольная точка №6	-2,5	-5,1	13,3
Орел (Контрольная точка №7)	56,0	25,1	-128,5
Контрольная точка №8	18,2	51,6	15,6
Контрольная точка №9	22,0	39,9	34,26
Мценск (Контрольная точка №10)	74,3	39,8	69,5
Контрольная точка №11	69,7	-13,8	14,4
Контрольная точка №12	27,22232327	41,67366091	-21,61451128
Плавск (Контрольная точка №13)	79,96633561	-28,8655	-89,82274052
Контрольная точка №14	103,29047952	-11,26654626	22,51051548
Щекино (Контрольная точка №15)	-28,37791379	28,86041565	79,0842363
Контрольная точка №16	-22,47915121	88,08275348	35,25171189
Тула (Контрольная точка №17)	80,9220443	-7,28945832	-77,0662375
Контрольная точка №18	-0,93757472	-12,0784168	3,25011492
Контрольная точка №19	1,8988457	-1,48904846	-3,47287716
Серпухов (Контрольная точка №20)	-40,34424959	-76,04849111	95,28331289
Контрольная точка №21	8,90123768	6,97737234	5,01545359
Подольск (Контрольная точка №22)	59,78410286	-96,57577326	44,47504719
Контрольная точка №23	11,92142653	11,60042077	13,77807674
Москва (Контрольная точка №24)	105,12418395	-112,07803446	-116,00891706

Далее на основе данных таблицы 2 рассчитывается математическое ожидание ошибок:

$$\begin{aligned} \mathrm{M(x)} &= \frac{\sum \Delta X}{\mathrm{n}} = 25{,}489; \\ \mathrm{M(y)} &= \frac{\sum \Delta \mathrm{Y}}{\mathrm{n}} = 1{,}124; \\ \mathrm{M(z)} &= \frac{\sum \Delta \mathrm{Z}}{\mathrm{n}} = 5{,}667, \end{aligned} \qquad (2)$$

а также среднеквадратическое отклонение расчетных величин:

$$\varepsilon_X = \sqrt{\frac{\sum(\mathrm{M}(X)-\Delta\mathrm{X})^2}{X}} = 0{,}085;$$

$$\varepsilon_Y = \sqrt{\frac{\sum(\mathrm{M}(\mathrm{Y})-\Delta\mathrm{Y})^2}{Y}} = 0{,}031; \quad \varepsilon_Z = \sqrt{\frac{\sum(\mathrm{M}(\mathrm{Z})-\Delta\mathrm{Z})^2}{Z}} = 0{,}045. \qquad (3)$$

Таким образом, проведенное математическое моделирование рассматриваемых процессов показало, что предлагаемая методика моделирования спутниковой навигации наземных подвижных объектов обеспечивает методическую точность моделирования геоцентрических координат в единицы сантиметров, что сопоставимо с точностью дифференциальных навигационных измерений.

1. Гурин С.Е. Спутниковые радионавигационные системы ГЛОНАСС/GPS на железнодорожном транспорте. – М.: МИИТ, 2004. – 55 с.

2. Липкин И.А. Спутниковые навигационные системы: учебное пособие. – М.: Мир, 2000. – 288 с.

УДК 330.341.2

В.Г. Андронов, А.С. Шутяев

ФГБОУ ВПО «Юго-Западный государственный университет», Курск

ОСНОВНЫЕ ЗАДАЧИ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В РЕГИОНЕ

Рассмотрены основные сферы использования результатов космической деятельности, обосновывается необходимость применения их на практике, а также влияние на экономику региона в целом.

Эффективное управление, контроль и надзор, координация деятельности различных министерств не мыслимы без обеспечения органов исполнительной власти достоверной, актуальной и оперативной информации о состоянии всех ресурсов региона. Использование результатов космической деятельности – путь к разработке инновационных решений, которые находят применение во многих отраслях экономики.

Поскольку в последнее время все более активно используется термин «результаты космической деятельности», важно разобраться, как космический мониторинг соотносится с результатами космической деятельности. Результаты космической деятельности

представляют собой производный продукт комплексного космического мониторинга.

Космический мониторинг заключается в непрерывном многократном получении информации о качественных и количественных характеристиках природных и антропогенных объектов и процессов с точной географической привязкой за счет обработки данных, получаемых со спутников дистанционного зондирования Земли. Кроме того, современные геоинформационные технологии и создание карт различных масштабов также не мыслимы без использования космических снимков.

К основным сферам применения космических снимков можно отнести (рис.1):

- исследование природных ресурсов;
- мониторинг стихийных бедствий и оценка их последствий;
- строительные и проектно-изыскательские работы;
- городской и земельный кадастр;
- планирование и управление развитием территорий;
- геология и освоение недр;
- промышленность, сельское и лесное хозяйство;
- туризм и другие виды деятельности.

Применение результатов космической деятельности позволит:

– проводить независимый и объективный учет и контроль всех видов ресурсов и всех видов деятельности региона;

– повысить сбалансированность экономики региона за счет увеличения доли информационных систем в структуре промышленного производства и услуг;

– успешно реализовать проект создания особой экономической зоны промышленно-производственного типа области.

Мировой и отечественный опыт, практика ряда регионов России подтверждают, что использование космических технологий оказывает значительный управленческий, экономический, социальный и экологический эффекты, существенно повышает уровень безопасности населения и территорий и позволяет констатировать, что в современных условиях использование спутниковых навигационных технологий на основе множества результатов космической деятельности является одним из действенных антикризисных

механизмов, обеспечивающих значительную экономию финансовых и материальных ресурсов. Комплексное использование результатов космической деятельности в интересах задач управления развитием отдельных отраслей и экономики субъекта Федерации в целом способно придать региональной экономике инновационный характер, усилить рыночные механизмы, повысить качество жизни населения (рис.2).

Рис. 1. Основные направления использования современных космических технологий в интересах социально-экономического развития субъектов Российской Федерации

Такие результаты обусловлены существенными дополнительными возможностями, которые предоставляют такие системы космической отрасли, как:

– глобальная навигационная система ГЛОНАСС;

– системы и комплексы оперативного аэрокосмического мониторинга состояния территорий и объектов;

– системы и средства сбора и комплексной обработки данных.

Что касается Курской области, то сейчас основной проблемой остается отсутствие целостной областной инфраструктуры в сфере использования РКД и в первую очередь инфраструктуры информа-

ционного обеспечения администрации Курской области, органов местного самоуправления, а также системы оказания услуг юридическим и физическим лицам.

Рис. 2. Наиболее значимые составляющие экономического эффекта за счет применения космической информации

Смотря на опыт других регионов страны, можно сделать некоторые выводы о том, что сегодня необходимо Курской области в сфере использования результатов космической деятельности:

- Региону нужны не просто картинки. Необходимы отраслевые решения на базе современных стандартных программных продуктов мирового уровня. Иначе может возникнуть ситуация, когда срок жизни системы будет зависеть от срока работы конкретного разработчика по данному проекту, замену которому на рынке найти будет очень сложно.
- Региону нужна аналитика, дающая объективную картину для принятия взвешенных решений. Эта аналитика может быть получена, в том числе, за счет подключения к федеральным информационным ресурсам профильных министерств и ведомств – Минсельхоза, Рослесхоза и им подобным.

• Региону нужно методическое и технологическое сопровождение проектов – от разработки концепции и эскизного проекта дореализации «под ключ».

• Региону нужен конкретный экономический эффект, выраженный в увеличении поступлений от более рационального использования ресурсов, от увеличения размеров штрафов за выявляемые посредством мониторинга нарушения, от инвесторов за счет повышения прозрачности и более широкого освещения ситуации в регионе.

На основании этого 5 июля 2013 года администрация Курской области вынесла постановление об утверждении областной целевой программы «Использование спутниковых навигационных технологий с использованием системы ГЛОНАСС и других результатов космической деятельности в интересах социально-экономического и инновационного развития Курской области».

На реализацию программы направленно 757897,0 тыс. рублей.

Целью подпрограммы является формирование базовых условий для создания и обеспечения эффективного функционирования областной системы комплексного использования спутниковых навигационных технологий с использованием системы ГЛОНАСС и других результатов космической деятельности в интересах социально-экономического и инновационного развития Курской области [1].

Реализация программы будет осуществляться в 2014-2016 годах в один этап.

Таким образом, комплексное применение спутниковых навигационных технологий с использованием результатов космической деятельности способно придать экономике Курского региона инновационный характер, усилить рыночные механизмы, повысить качество жизни населения, расширить спектр оказываемых услуг в различных отраслях, обеспечить мониторинг и контроль за критически важными, потенциально опасными и социально значимыми объектами на территории Курской области, реализовать меры по устранению чрезвычайных ситуаций.

---

1. Использование спутниковых навигационных технологий с использованием системы ГЛОНАСС и других результатов космической деятельно-

сти в интересах социально-экономического развития Курской области на 2013-2016 годы [Электронный ресурс]: постановление Администрации Курской области от 05.07.2013 № 432-па. – URL: http://www.consultant.ru/.

УДК 528.721.1

В.Г. Андронов [1], Ю.Н. Волобуев [2]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) 18 ЦНИИ МО РФ

ОБОСНОВАНИЕ АКТУАЛЬНОСТИ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ СОЗДАНИЯ ЗАМЕЩАЮЩИХ МОДЕЛЕЙ КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ НОВОГО КЛАССА

Рассмотрены преимущества и недостатки существующих моделей RPC и сформирован облик замещающих моделей нового класса.

В настоящее время космические цифровые снимки, получаемые отечественным спутником Канопус-В, космическими комплексами Ресурс-ДК и Ресурс-П, имеют соответственно высокое (2-4 м) и сверхвысокое (лучше 1 метра) разрешение на местности и уже сегодня используются для картографирования отдельных территорий, создания и обновления цифровых моделей местности и расположенных на ней объектов, мониторинга территорий и решения многих других прикладных, в том числе военных задач, связанных с информационным обеспечением районов военных действий. В то же время анализ известной литературы [1-5] показал, что имеется большая проблема, препятствующая широкому и эффективному использованию отечественных космических снимков в народном хозяйстве и военном деле, которую можно декомпозировать на три составляющие.

Первой является низкая точность геопривязки отечественных снимков в автоматическом режиме по бортовым астронавигационным и инерциальным измерениям и большая трудоёмкость**,** требующаяся для повышения этой точности до надлежащего уровня по наземным опорным точкам. Основная причина такого положения дел – слишком большая масса отечественных КА сверхвысокого разрешения (8 тонн у Ресурса-ДК по сравнению с 2,5 т у WorldView-1), что не позволяет достичь высокой степени динами-

ки и точности угловой ориентации и стабилизации КА при съёмке, обеспечивающих точность геопривязки на уровне пространственного разрешения на местности. Анализ концепции развития российской системы дистанционного зондирования Земли, рассчитанной на период до 2025 г., показывает, что решающих прорывов в этой области пока не намечается.

Вторая составляющая связана с существенным усложнением фотограмметрических моделей, которые наиболее точно описывают процессы формирования маршрутов изображений в оптико-электронных сканирующих системах на матрицах ПЗС, функционирующих в режимах временной задержки и накопления зарядовых пакетов. Способность современных КА выносить линию визирования вдоль, перпендикулярно и поперёк трассы КА, кардинально усложнила геометрию и режимы космической сканерной съёмки. Элементы внешнего ориентирования сканерных изображений стали функцией от времени. Кроме объектовых режимов съёмки вдоль трассы КА с отворотом только по углу крена и длительностью включения несколько секунд, стали широко применяться режимы маршрутной и площадной съёмки с отклонениями линии визирования по углам тангажа, крена и рыскания КА и длительностью включения в десятки и более секунд. В этих условиях фотограмметрические модели приобрели динамический и итерационный характер, что существенно повысило их уровень вычислительной сложности. Поскольку задачи приведения космических сканерных изображений к высоким метрическим характеристикам картографических материалов требуют организации поточечной обработки всех пикселей маршрута изображения, существующие технологии ортотрансформирования отечественных космических сканерных изображений не годятся для решения высокооперативных задач оценки чрезвычайных ситуаций и в военном деле, а также тормозят решение других задач.

Третья составляющая обусловлена усложнением характеристик съёмочной аппаратуры, конструктивных параметров её расположения в корпусе КА, появлением инновационных режимов съёмки и ужесточением конкуренции на мировом рынке космических изображений. Становится мировой тенденцией поставлять

потребителям вместе со снимками и инструментарий их обработки, в числе которого наиболее широкое распространение получили так называемые замещающие модели космических изображений на основе коэффициентов рациональных полиномов. Их получают путём аппроксимации результатов применения строгих фотограмметрических моделей, т.е. на множестве задаваемых и получаемых координат точек снимка и точек земной поверхности находят связывающие их коэффициенты полиномов. Такой подход обеспечивает недоступность для широкого круга потребителей конструктивных характеристик современной и перспективной съёмочной аппаратуры и метаданных съёмки, необходимых для разработки строгих фотограмметрических моделей, монопольное положение на мировом рынке дистанционного зондирования Земли и высокую оперативность обработки снимков по сравнению со сложными тригонометрическими фотограмметрическими моделями.

Анализ известной литературы показал, что существующая в мире тенденция к созданию замещающих моделей на основе коэффициентов RPC в своей глубинной основе преследует главную цель, связанную с обеспечением монопольного положения на мировом рынке ДЗЗ. Этот вывод основывается на следующих объективных фактах.

Во-первых, тенденции развития космических технологий свидетельствуют о том, что не за горами достижение для космических сканерных снимков разрешения на местности до 10 см, которое ранее было вотчиной аэроснимков. А этот уровень разрешающей способности уже позволяет использовать космическую съёмку для оперативного картографирования и обновления так называемых дежурных планов городов с детальностью, соответствующей масштабам 1:2 000 и 1: 1000. Учитывая неуклонный рост производительности космических комплексов ДЗЗ, можно прогнозировать передел в пользу космоса огромного рынка высокоточного мониторинга муниципальных территорий.

Во-вторых, по своей физической сути модели RPC являются вторичными по отношению к фотограмметрическим моделям, не доступным широкому потребителю, поскольку разрабатываются по результатам применения последних. Кроме того, они не имеют

физического смысла и не позволяют моделировать процессы обработки снимков. И во многих публикациях отмечается, что очень часто точность моделей RPC на порядок хуже их прародителей, т.е. фотограмметрических моделей. Просто эти факты широко не раздуваются на фоне имеющегося прорыва в фотограмметрической обработке космических изображений с помощью моделей RPC без использования опорных точек по отношению к масштабам 1:25 000, 1: 10 000 и в ряде случаев к 1:5 000. Представляется, что когда возникнет ситуация, описанная в предыдущем пункте, и с помощью фотограмметрических моделей можно будет выйти на указанные выше масштабы, то для широкого круга потребителей, использующих модели RPC, допустимая точность так и останется на уровне масштаба не выше 1:5 000.

В-третьих, несомненно, что в недалёкой перспективе многие операции фотограмметрической обработки космических изображений, в частности ортотрансформирование, будут выполняться на борту КА и сбрасываться по радиоканалу непосредственно потребителям, уже пригодные к использованию в реальном масштабе времени по назначению, особенно в военном деле. Для этих областей применения космических снимков технологии получения коэффициентов RPC на борту КА представляются неприемлемыми вследствие необходимости применения ручных операций, большой длительности и трудоёмкости этих процессов.

Учитывая изложенное, большую актуальность и практическую значимость представляет исследование и решение проблемы разработки замещающих функциональных моделей отечественных космических сканерных изображений, сочетающих в себе высокую точность, присущую фотограмметрическим моделям, вплоть до уровня пространственного разрешения снимков, низкий уровень вычислительных затрат, характерный для известных замещающих моделей RPC-класса, обеспечивающий ортотрансформирование маршрутов космических сканерных изображений в масштабе времени, близком к реальному, а также разработка методов автоматической калибровки (уточнения) параметров съёмки на борту КА или в ходе наземной обработки без визуализации сформированных изображений и использования опорных точек местности.

Список литературы

1. Погорелов В.В., Шавук В.С. Анализ математических моделей при фотограмметрической обработке космических снимков // Геодезия и картография. – 2009. – № 3.

2. Бакланов А.И. К вопросу о пространственном разрешении и точности привязки изображений космических систем наблюдения высокого разрешения // Геоматика. – 2010. – №3(8). –С. 25-31.

3. Космический аппарат «Ресурс-П» / А.Н. Кирилин, Р.Н. Ахметов, Н.Р. Стратилатов [и др.] // Геоматика. – 2010. – №4. – С. 23-27.

4. Некрасов В.В., Макушева Е.В. Разработка динамической геометрической модели съемки оптико-электронных съемочных систем для перспективных космических комплексов типа «КАНОПУС-В» // Вопросы электромеханики. – 2010. – Т. 119. – №6. – С. 25-30.

5. Перспективный КА «Канопус-В». Технология обработки снимков КА Канопус-В в ЦФС Фотомод [Электронный ресурс] / Геоинформационное агентство «Иннотер». – URL: http://www.innoter.com/articles/Kanopus-V.

УДК 528.721.1

В.Г. Андронов [1], Ю.Н. Волобуев [2]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ (г. Курск) 18 ЦНИИ МО РФ

НА ПУТИ К ЗАМЕЩАЮЩИМ МОДЕЛЯМ КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ НОВОГО КЛАССА: ТРЕБОВАНИЯ К СТРУКТУРНО-ФУНКЦИОНАЛЬНОЙ ОРГАНИЗАЦИИ И УРОВНЮ ВЫЧИСЛИТЕЛЬНЫХ ЗАТРАТ

Представлены научно обоснованные требования к структурно-функциональной организации и уровню вычислительных затрат замещающих космические изображения моделей нового класса.

Анализ математических описаний [1, 2] процедур построения физических и замещающих их моделей космической сканерной съёмки в известных зарубежных и отечественных работах по ДЗЗ и фотограмметрии показывает, что в теории фотограмметрии широко используются две основные схемы построения изображений: прямая схема (модель (2), когда световой пучок проецируется от местности в ФП съёмочной аппаратуры и регистрируется на борту носителя) и обратная схема (модель (1), в случае перепроецирования точек ФП на местность):

$$X = F_X(x, y, Q_F, B, H, t);$$
$$Y = F_Y(x, y, Q_F, B, H, t); \quad (1)$$
$$\begin{cases} x(t) = \Phi_x(X, Y, Z, Q_\Phi, t); \\ y(t) = \Phi_y(X, Y, Z, Q_\Phi, t). \end{cases} \quad (2)$$
$$Z = F_Z(x, y, Q_F, B, H, t),$$

где X, Y, Z, B, L, H – геоцентрические и геодезические координаты точек земной поверхности;

x, y – плоские прямоугольные координаты зарядовых пакетов в системе координат фокальной плоскости;

Q_F, Q_Φ – функционалы связи соответственно геоцентрических и плоских координат точек земной поверхности и фокальной плоскости с элементами внешнего ориентирования (ЭВО) и конструктивными характеристиками съёмочной аппаратуры.

Определяющее влияние на уровень вычислительной сложности моделей (1) и (2) оказывает структурно-функциональная организация используемых в них элементов, в частности моделей ЭВО.

В этой связи для априорной оценки и позиционирования вычислительной сложности фотограмметрических и замещающих их моделей введём показатель качества, который будет характеризовать уровень вычислительных затрат (УВЗ). Количественно УВЗ можно оценить общим числом $\boldsymbol{\Theta}$ стандартных вычислительных операций, требующихся для расчёта геоцентрических координат одной точки земной поверхности. Поскольку вычислительная нагрузка при различных арифметических операциях с числами разная, присвоим весовые коэффициенты для ранжирования простых и сложных вычислительных операций следующим образом: простым арифметическим операциям (деление двух чисел, извлечение квадратного корня из одного числа, сложение, вычитание или произведение двух и более чисел, возведение в любую степень одного числа) присвоим коэффициент 1, операциям с тригонометрическими функциями (взятие синуса, косинуса и т.д.) – коэффициент 2, с итерационными вычислениями – коэффициент 5.

Для дальнейшего сравнительного анализа вычислительной сложности структурно-функциональной организации рассматриваемых фотограмметрических и разрабатываемых на их основе за-

мещающих функциональных моделей вычислим число **Θ** для замещающих моделей RPS-класса, которые в настоящее время имеют самое высокое быстродействие.

Модели RPS-класса имеют следующий вид:

$$x = \frac{P_1(X,Y,Z)}{P_2(X,Y,Z)};$$
$$y = \frac{P_3(X,Y,Z)}{P_4(X,Y,Z)}, \quad (3)$$

где в числителях и знаменателях стоят алгебраические полиномы полной третьей степени, которые связывают геоцентрические координаты X,Y,Z точки земной поверхности с координатами x, y её изображения на снимке. Методика вычисления числа **Θ** состоит в следующем: один раз для всех полиномов вычисляем взятие второй и третьей степени от геоцентрических координат (6 операций с коэффициентом 1), перекрёстные парные произведения координат (3 операции с коэффициентом 1) и координат второй степени на координаты (6 операций с коэффициентом 1), произведение трёх координат (1 операция с коэффициентом 1), что составляет 16 операций с коэффициентом 1. Далее для каждого полинома рассчитываем по 19 произведений соответствующих коэффициентов на полученные общие для всех полиномов множители и сомножители (19× 4 операций с коэффициентом 1) и складываем эти результаты (1× 4 операций с коэффициентом 1). Остаются две операции деления с коэффициентом 1 первого полинома на второй и третьего на четвёртый.

Таким образом, **Θ** =98 и все вычислительные операции носят простой арифметический характер.Учитывая изложенное, рассмотрим более подробно влияние вида и состава структурных элементов фотограмметрических моделей вида (1) на величину **Θ** и номер её УВЗ.

УВЗ №1.

Будем полагать, что первый УВЗ характерен для исходных фотограмметрических моделей, представленных в виде уравнений коллинеарности (1) в геоцентрической системе координат:

$$X = X_S + (Z - Z_S)\frac{F_X}{F_Z}; Y = Y_S + (Z - Z_S)\frac{F_Y}{F_Z}, \quad (4)$$

где $F_X = a_{11}x+a_{12}y+a_{13}f;$
$F_Y = a_{21}x+a_{22}y+a_{23}f;$
$F_X a_{31}x+a_{32}y + +a_{33}f.$

Очевидно, что для внешнего ориентирования каждой строки в гринвичской системе координат необходимо определить для неё три значения X_S, Y_S, Z_S и девять значений a_{ij}, т.е. 12 значений ЭВО. В простейшем для расчётов варианте движения КА по солнечно-синхронной круговой орбите и использования кеплеровской модели прогноза движения КА для вычисления трёх значений X_S, Y_S, Z_S необходимо выполнить 70 вычислительных операций.

Текущие значения углов тангажа, крена и рыскания КА вычисляются по их измеренным дискретным значениям на интервале съёмки с помощью моделей вида $\alpha(t) = \alpha(t_0) + \dot{\alpha}(t_0) \cdot t$ в результате двух простых вычислительных операций с коэффициентом 1. Найденные по этим моделям три текущих значения угловых ЭВО строк в орбитальной системе координат (6 операций с коэффициентом 1) необходимо далее пересчитать в текущие значения элементов a_{ij} матрицы направляющих косинусов $\boldsymbol{A}$, определяющей ориентацию визирной системы координат в гринвичской. Для этого используются десять матриц, для формирования каждой матрицы требуется шесть операций взятия синуса и косинуса с коэффициентом 2, расчёт девяти произведений чисел с коэффициентом 1 и четыре операции сложения с коэффициентом 1, т.е. всего 25×10 операций. Перемножение всех элементов матриц потребует 108 операций с коэффициентом 1. Таким образом, для вычисления всех элементов a_{ij} матрицы $\boldsymbol{A}$ приходится выполнять 358 вычислительных операций.

Заключительные вычислительные процедуры будем называть структурными. Они связаны с простым расчётом трёх значений F_X, F_Y, F_Z с коэффициентом 1 (12 операций), семи других простых операций с коэффициентом 1, и 29 операций вычисления значения Z, в том числе 12 итерационных с коэффициентом 5 (60 операций) и 17 простых с коэффициентом 1.

Структура вычислительных затрат при использовании фотограмметрических моделей в виде уравнений коллинеарности (1), кеплеровской модели движения КА и полиномиальной модели

бортовых измерений углов тангажа, крена и рыскания КА выглядит следующим образом:

Линейные ЭВО: 70; Угловые ЭВО: 358; Структурные вычисления:96.

Обще число **Θ** вычислительных операций: 524.

УВЗ №2.

Будем считать, что второй УВЗ отличается от первого только полиномиальной моделью определения текущих значений линейных ЭВО. Тогда можно считать, что на интервале съёмки в моменты времени t_0, t_1, t_2,…, t_h,…,t_H известны дискретные значения $R_S(t_0), R_S(t_1),\ldots, R_S(t_H)$ вектора гринвичских координат КА $\boldsymbol{R_S}(t_h)=(X_S(t_h), Y_S(t_h), Z_S(t_h))^T$, а модели определения их текущих значений можно привести к виду полиномов $(X_S(t), Y_S(t), Z_S(t))=\xi_0^{(X,Y,Z)}+\xi_1^{(X,Y,Z)}\cdot t+\xi_2^{(X,Y,Z)}\cdot t^2+\ldots$ Очевидно, что вычисление текущих значений каждой координаты КА при использовании третьей степени полинома требует выполнения шести вычислительных операций с коэффициентом 1.

Структура вычислительных затрат при использовании фотограмметрических моделей на основе уравнений коллинеарности (1), полиномиальных моделей определения текущих значений линейных ЭВО и бортовых измерений углов тангажа, крена и рыскания КА выглядит следующим образом:

Линейные ЭВО: 18; Угловые ЭВО: 358; Структурные вычисления: 96.

Обще число **Θ** вычислительных операций: 472.

Нетрудно подсчитать, что общее число **Θ** вычислительных операций при приведении фотограмметрических моделей ко второму УВЗ только за счёт перехода на полиномиальную модель определения текущих значений линейных ЭВО третьей степени уменьшается на 12% по сравнению с первым УВЗ.

УВЗ №3.

Положим, что третий УВЗ отличается от второго аппроксимацией элементов a_{ij} матрицы направляющих косинусов $\boldsymbol{A}$, определяющей ориентацию визирной системы координат в гринвичской системе. Тогда полиномиальные модели определения текущих зна-

чений линейных и угловых ЭВО в гринвичской системе координат будут описываться следующими функциями:

$$(X_S(\mathrm{t}),Y_S(t),Z_S(t))=\xi_0^{(X,Y,Z)}+\xi_1^{(X,Y,Z)}\cdot\mathrm{t}+\xi_2^{(X,Y,Z)}\cdot\mathrm{t}^2+\ldots; \quad (5)$$

$$a_{ij}(\mathrm{t})=\xi_0^{(ij)}+\xi_1^{(ij)}\cdot\mathrm{t}+\xi_2^{(ij)}\cdot\mathrm{t}^2+\ldots \quad (6)$$

При этом для расчёта дискретных значений элементов a_{ij} матрицы направляющих косинусов $\boldsymbol{A}$ могут использоваться как бортовые инерциальные измерения углов тангажа α, крена β и рыскания χ КА в орбитальной системе координат, связанной с центром масс КА, так и технологии астроизмерений по снимкам звёздного неба. Отличия заключаются только в виде и методике расчёта элементов матрицы A(t). В конечном итоге, располагая множеством $\{a_{ij}(t_h)\}$ значений элементов матриц A(t_h), в обоих случаях производится их аппроксимация степенными полиномами от времени и приведение к виду (6). Оценка числа вычислительных операций, характерных для использования фотограмметрических моделей вида (1) и полиномиальных моделей ЭВО третьей степени вида (5) – (6), проведенная по аналогичной схеме, как на предыдущих уровнях, приводит к следующей структуре вычислительных затрат:

Линейные ЭВО: 18; Угловые ЭВО: 54; Структурные вычисления: 96.

Обще число **Θ** вычислительных операций: 168.

Легко подсчитать, что при приведении фотограмметрических моделей к третьему УВЗ общее число **Θ** вычислительных операций уменьшается на 70% по сравнению с первым УВЗ и на 65% - по сравнению со вторым.

УВЗ №4.

Положим, что на четвёртом УВЗ используются полиномиальные модели вида (5) – (6) второй степени при тех же вариантах бортовых астронавигационных и/или инерциальных измерений, а фотограмметрические модели имеют следующий вид:

$$\begin{aligned} X &= X_S(\mathrm{t})-|R_{\text{ЛВ}}(t)|\cdot A(t)\cdot r_{лв}(t);\\ \mathrm{Y} &= \mathrm{Y_S}(t)-|R_{\text{ЛВ}}(t)|\cdot A(t)\cdot r_{лв}(t);\\ \mathrm{Z} &= \mathrm{Z_S}(t)-|R_{\text{ЛВ}}(t)|\cdot A(t)\cdot r_{лв}(t), \end{aligned} \quad (7)$$

где X,Y,Z – геоцентрические координаты точек пересечения линии визирования (ЛВ) с земной поверхностью в гринвичской системе координат;

$|R_{ЛВ}(t)|$ – длина ЛВ от центра проекции S до точки пересечения с земной поверхностью;

вектор $r_{лв}(t) = (x, y, f)^{T}$ – вектор координат датчиков ПЗС в визирной системе координат, центр которой расположен в центре проекции S, а оси параллельны одноимённым осям системы координат фокальной плоскости;

A(t) – матрица направляющих косинусов, описывающая ориентацию системы координат фокальной плоскости в гринвичской системе координат.

Оценка числа вычислительных операций на этом уровне приводит к следующей структуре вычислительных затрат:

Линейные ЭВО: 12; Угловые ЭВО: 36; Структурные вычисления: 45.

Общее число **Θ** вычислительных операций: 93.

Общее число **Θ** вычислительных операций на четвёртом УВЗ уменьшается на 82% и 80%, по сравнению с первым и вторым УВЗ, и на 45% – по сравнению с третьим.

Таким образом, структурно-функциональная аппроксимация исходной фотограмметрической модели до четвёртого УВЗ обеспечивает выход получаемых замещающих функциональных моделей на уровень вычислительной сложности замещающих моделей RPC- класса.

---

1. Kim T. and Dowman I.J. Comparison of two physical sensor models for satellite images: Position-Rotation model and Orbit-Attitude model // Photogrammetric Record. – 2006. – №21(114). – P. 110-123.

2. Fraser C.S. and Hanley H.B. Biascompensation in rational functions for IKONOS satellite imagery // Photogramm. Eng. Remote. – 2003. – №69(1). – P. 53-57.

УДК 681.3

Д.А. Стребков[1], А.С. Сизов[2], С.Ю. Челышов[2]

[1]ФГБОУ ВПО «Юго-Западный государственный университет», Курск

[2]НИЦ ФГУП «18 ЦНИИ» МО РФ

РАСПОЗНАВАНИЕ ДВИЖУЩИХСЯ НАЗЕМНЫХ ОБЪЕКТОВ НА ОСНОВЕ АНАЛИЗА ЧАСТОТНО-ВРЕМЕННОГО ПРЕДСТАВЛЕНИЯ СЕЙСМИЧЕСКОГО СИГНАЛА

Рассмотрено распознавание на основе двухэтапной процедуры обработки вектора пространства признаков, описывающих частотную и частотно-временную структуру сейсмических сигналов от наземных движущихся объектов.

В настоящее время для охраны территории предприятий широко применяются различные технические средства и системы охраны, в том числе быстроразвертываемые системы [1, 2]. При этом особое значение приобретает обеспечение непрерывного наблюдения и достоверной «сигнализации» от быстроразвертываемых систем об обнаружении несанкционированного появления в охраняемой зоне движущихся объектов заданных классов (в частности, «человека»).

Обеспечить высокую скрытность функционирования, простоту развертывания, значительную по площади контролируемую зону позволяют датчики-классификаторы на основе сейсмических сенсоров [1, 2].

В то же время сложная фоноцелевая обстановка в местах развертывания средств охраны, обусловленная движением мешающих объектов различных классов («животное» и пр.), требует повышения достоверности распознавания движущихся объектов требуемых классов («человек», «группа людей»). Применяемые в сейсмических датчиках-классификаторах алгоритмы распознавания базируются на анализе частотного спектра сейсмических сигналов и достигли предельных значений.

В докладе представлены результаты исследований, на базе которых предложена процедура распознавания движущихся объектов с похожими частотными спектрами. Способ базируется на двухэтапной процедуре.

На первом этапе процедуры для снижения размерности области распознавания, количества распознаваемых классов до минимально возможного применяются наиболее информативные составляющие частотного спектра. Затем выбираются два класса объектов, имеющих наибольшее значение апостериорной вероятности [3].

На втором этапе этой процедуры для распознавания объектов с похожими частотными спектрами применяется многомасштабный вейвлет-анализ изменяющейся сигнатуры регистрируемого сейсмического колебания [4]. В качестве признаков применяются отношения дисперсий вейвлет-коэффициентов, распределенных на разных масштабах, а в качестве решающего правила – правило Байеса.

В частности, установлено, что применение в качестве признаков значений дисперсии коэффициентов вейвлет-преобразования с «материнским вейвлетом» Добеши на масштабах j= 8…11 (при длительности интервала анализа сигналов две секунды и частоте дискретизации значений 1 кГц) позволяет проводить распознавание движущихся объектов с похожими частотными спектрами, инвариантное к амплитуде регистрируемого сейсмосигнала.

Таким образом, предлагаемая процедура распознавания, отличающаяся применением на каждом этапе распознавания признаков, описывающих частотную и частотно-временную структуру сейсмических сигналов, позволяет решать задачу распознавания наземных движущихся объектов с похожими частотными спектрами с требуемой достоверностью (более 0,92). Возможности существующих средств цифровой обработки сигналов (микропроцессоры и сигнальные процессоры) позволяют реализовать разработанную процедуру распознавания в автономных датчиках-классификаторах.

Список литературы

1. Барсуков В.С., Рычков С.А. «Умные» датчики для интеллектуальных систем безопасности // Специальная техника. – 2004. – № 6. – С. 14–23.

2. Введенский Б.С. Обзор зарубежных быстроразворачиваемых комплексов для охраны периметров // Специальная техника. – 2003. – № 4. – С. 12–19.

3. Ту Дж., Гонсалес Р. Принципы распознавания образов. – М.: Мир, 1978.

4. Дьяконов В.П. Вейвлеты. От теории к практике. – М.: СОЛОН-Р, 2002. – 448 с.

Научное издание

ИНФОКОММУНИКАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СОСТОЯНИЕ, ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Материалы I Всероссийской
научно-практической конференции

25-26 апреля 2014 г.

Редактор *О.А. Петрова*
Компьютерная вёрстка и макет *А.Е. Серебряковой*

Подписано в печать 10.04.14. Формат 60х84 1/16. Бумага офсетная.
Усл. печ. л. 22,6. Уч-изд. л. 21,4. Тираж 100 экз. Заказ
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.
Отпечатано в ЮЗГУ.