

Федеральное агентство по образованию  
Государственное образовательное учреждение высшего профессионального образования  
«Московский государственный технический университет имени Н.Э.Баумана»

ФАКУЛЬТЕТ \_\_\_\_\_ Информатика и системы управления

КАФЕДРА \_\_\_\_\_ Проектирование и технология производства электронной аппаратуры

## РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА *к магистерской диссертации*

*Распределённая система потокового  
мультимедийного вещания в сетях передачи данных*

Студент-дипломник: \_\_\_\_\_ ( Афанасьев А.В. )  
(подпись) (фамилия, инициалы)

Руководитель проекта: \_\_\_\_\_ ( Власов А.И. )  
(подпись) (фамилия, инициалы)

Консультанты:  
по конструкторской части: \_\_\_\_\_ ( Власов А.И. )  
(подпись) (фамилия, инициалы)

по технологической части: \_\_\_\_\_ ( Власов А.И. )  
(подпись) (фамилия, инициалы)

по исследовательской части: \_\_\_\_\_ ( Власов А.И. )  
(подпись) (фамилия, инициалы)

## **АННОТАЦИЯ**

В работе исследованы принципы мультимедийного вещания в сетях передачи данных, рассмотрены форматы представления мультимедийных данных и моделей их защиты в рамках мультикаст сетей, произведен анализ существующих решений IP-вещания, а также предложен вариант построения системы мультимедийного вещания в рамках сетей передачи данных. Исследованы концепции представления видео в цифровом видео и концепция сжатия цифрового видеопотока. На основе анализа стандарта сжатия H.264 показаны передовые технологии, используемые в сжатии видео. На базе разработанного программного обеспечения построен опытный образец системы мультимедийного вещания, которая введена в опытную эксплуатацию на базе сети студгородка МГТУ им.Н.Э.Баумана. Работа предназначена для инженеров-технологов и радиотехников, научных работников, системных администраторов и может быть полезна для широкого круга людей других специальностей.

## **ABSTRACT**

The work investigates principles of multimedia broadcasting over the data exchange network, describes multimedia data representation formats, types of multimedia data protection from unrestricted access, analyzes existing solutions for multimedia broadcasting and presents possible IP-TV system realization. Also work pay attention to digital video and video compressing concepts. Based on H.264 video compression standard state-of-art video compressing technologies are investigated. On the base of developed concepts IP-TV solution has been built and now works in the MSTU n.a.Bauman campus network. Work is intended for technical specialists, academic people, system administrators and may be useful for a wide range of other specialists.

## СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СОКРАЩЕНИЙ И ТЕРМИНОВ

<b>ADSL</b>	(англ. Asymmetric Digital Subscriber Line — асимметрич-ная цифровая абонентская линия) — модемная техноло-гия, предназна-ченная для решения проблемы последней мили. Преобразует стандартные абонентские телефонные аналоговые линии в линии высокоскоростного до-ступа. Основное преимущество данной технологии в том, что нет необходимости прокладывать кабель до абонен-та. Используются уже проложенные телефонные кабели. Для приёма и передачи данных используются разные ка-налы: приёмный обладает существенно большей пропуск-ной способностью., 5
<b>AES</b>	(англ. Advanced Encryption System — улучшенная си-стема шифрования) симметричный алгоритм блочного шифрования, выбранный в результате конкурса и принятый в качестве стандарта шифрования правительством США, 63
<b>BT.601</b>	Формат цифрового представления интерлейсного ана-логового видео, включающий метод формирования 720 (360) яркостных (цветоразностных) отсчетов на линию при работе с 525 (NTSC) и 625 (PAL/SECAM) линейны-ми сигналами, 90
<b>CABAC</b>	(англ. Context-Adaptive Binary Arithmetic Coding — кон-текстнозависимое бинарное арифметическое кодирова-ние) разновидность энтропийного кодирования. Исполь-зуется в H.264 формате сжатия изображения, 56
<b>CAVLC</b>	(англ. Context-Adaptive Variable-Length Coding — кон-текстнозависимый код переменной длины) разновид-ность энтропийного кодирования. Используется в H.264 формате сжатия изображения, 56
<b>CIF</b>	(англ. Common Intermediate Format — общий промежу-точный формат) формат представления видеосигналов со стандартизованным вертикальным и горизонтальным разрешением в цветовой модели YCbCr. Разработан с це-лью упрощения конвертации между форматами PAL и NTSC, 31

<b>CW</b>	(в стандарте DVB-CSA) (англ. Common Word — общее слово) сессионный ключ симметричного шифрования, используемый для скрамблирования и дескрамблирования транспортного потока, 61
<b>DCT</b>	(англ. Discrete Cosine Transform — дискретное косинусное преобразование) вариант ортогонального преобразования. Применяется в алгоритмах сжатия изображений и видео, 37
<b>DPCM</b>	(англ. Differential Pulse Code Modulation — дифференциальная импульсно-кодовая модуляция) способ преобразования аналогового сигнала в цифровую форму, в котором сигнал оцифровывается, после чего квантуется и сохраняется разница между действительным и предсказанным (на основе предыдущего или предыдущих отсчётов) значением отсчёта, 36
<b>DVB</b>	(англ. Digital Video Broadcasting — вещание цифрового видео) стандарт системы цифрового телевидения, включающий кабельное (DVB-C), спутниковое (DVB-S), эфирное (DVB-T), 60
<b>DVB-CSA</b>	(англ. DVB Common Scrambling Algorithm — общий алгоритм скрамблирования DVB) алгоритм шифрования, применяемый для защиты DVB-вещания от несанкционированного доступа. Кроме DVB-CSA, DVB определяет спецификации стандартов DVB-CA (DVB Conditional Access Module) и DVB-CI (DVB Common Interface), 60
<b>DWT</b>	(англ. Discrete Wavelet Transform — дискретное вейвлет-преобразование) вейвлет-преобразованиям, в которых вейвлеты представлены дискретными сигналами. Применяется в алгоритмах сжатия изображений и видео, 37
<b>ECM</b>	(в стандарте DVB-CSA) (англ. Entitlement Control Message — сообщение управления доступом) данные, передаваемые в вещательном потоке, содержащие информацию необходимую для дешифрации кодового слова CW, 61

<b>ЕММ</b>	(в стандарте DVB-CSA) (англ. Entitlement Management Message — сообщение авторизации абонентов) данные, передаваемые в вещательном потоке, содержащие информацию о подписчике (состоянии счета, списке полученных или запрошенных услуг и проч.), 61
<b>GRID</b>	Согласованная, открытая и стандартизованная среда, которая обеспечивает гибкое, безопасное, скоординированное разделение ресурсов в рамках виртуальной организации, 80
<b>HDTV</b>	(англ. High Definition Television) телевидение высокой четкости, 5
<b>IGMP</b>	(англ. Internet Group Management Protocol — протокол управления интернет-группами) протокол multicast маршрутизации, 29
<b>ITU-R</b>	(англ. International Telecommunication Union — Международный союз электросвязи) международная организация, определяющая стандарты (Рекомендации) в области телекоммуникаций и радио, 31
<b>MPEG</b>	(англ. Motion Picture Experts Group) стандарт ISO для методов сжатия аудио- и видео-файлов и механизмов мультиплексирования и синхронизации разнотипных потоков информации, 35
<b>NTSC</b>	(англ. National Television Standards Committee — Национальный комитет телевизионных стандартов) система цветного телевидения, разработанная в 1953 году в США, 31
<b>PAL</b>	(англ. Phase Alteration Line — строка с переменной фазой) система цветного телевидения, разработанная в ФРГ, 31
<b>PSNR</b>	(англ. Peak Signal to Noise Ratio — пиковое отношение сигнала шуму) соотношение между максимумом возможного значения сигнала и мощностью шума, искажающего значения сигнала. Используется, в частности, для объективной оценки качества видеоизображений, 34

## **QoS**

<b>RSA</b>	(сокр. от Ronald Linn Rivest, Adi Shamir и Leonard Adleman - имён разработчиков алгоритма) криптографический алгоритм с открытым ключом, пригодный и для шифрования и цифровой подписи, 63
<b>RTP</b>	(англ. Real-time Transfer Protocol — протокол передачи реального масштаба времени) сетевой протокол, предназначенный для передачи данных реального масштаба времени (аудио-, видео- телеконференции и проч.), 93
<b>RTP-микшер</b>	Комплекс программных средств осуществляющий получение нескольких RTP потоков данных (от различных источников) и формирующий единый RTP поток по некоторому заданному алгоритму. Используется, например, для организации групповых аудио-видеоконференций, 103
<b>SNMP</b>	(англ. Simple Network Management Protocol — простой протокол управления сетью) протокол, обеспечивающий возможности удаленного управления и мониторинга сетевого оборудования, 103
<b>SSL</b>	(англ. Secured Socket Layer — протокол защищённых сокетов) — криптографический протокол, обеспечивающий безопасную передачу данных по сети передачи данных, 63
<b>STB</b>	(англ. Set Top Box — телевизионная абонентская приставка) устройство, принимающее IP-TV вещание и формирующее сигнал, отображаемый телевизором, 66
<b>Transport Stream</b>	(англ. Transport Stream, TS — транспортный поток) протокол, определённый в ISO/IEC 13818-1, предназначенный для инкапсуляции пакетов данных в транспортные пакеты MPEG-2 TS для передачи по каналам данных с большой вероятностью ошибок передачи (IP-сеть, радиоэфир и проч.), 61

<b>Блочность</b>	(в теории обработки изображений) артефакт сжатия в блоковых алгоритмах сжатия изображений с потерями, проявляющийся на границах макроблоков в следствие использования больших значений коэффициентов квантования, 52
<b>ДКП</b>	см. <b>DCT</b> , 37
<b>ЗНД</b>	Защита от несанкционированного доступа, 59
<b>Интер-предсказание</b>	Предсказание на основе ранее декодированных кадров видеопоследовательности, 46
<b>Интерлейс</b>	(Interlace) техника улучшения качества изображения на ЭЛТ устройствах без использования дополнительной полосы пропускания путём чередования отображения чётных и нечётных строк изображения, 45
<b>Интра-предсказание</b>	Предсказание на основе ранее декодированных отсчётов текущего обрабатываемого элемента (блока, макроблока, слайса, кадра), 46
<b>Кодек</b>	(англ. codec — сокр. от coder/decoder (кодировщик/декодировщик) или compressor/decompressor) устройство или программа, способная выполнять прямое и обратное преобразование потока данных или сигнала, 35
<b>Компенсация движения</b>	Один из методов удаления временной избыточности в видеоданных основанный на сходстве соседних кадров в видеопоследовательности, 36
<b>Макроблок</b>	сегмент изображения $16 \times 16$ отсчётов яркостной составляющей изображения и соответствующего количества отсчётов цветоразностных составляющих (для 4:2:0 YCbCr — блоки $8 \times 8$ Cb и Cr составляющей), 46
<b>Мибит, Кибит</b>	в марте 1999 года Международная электротехническая комиссия ввела новый стандарт по именованию двоичных чисел. Приставки МЭК схожи с СИ: они начинаются на те же слоги, но второй слог у всех двоичных приставок — би (binary — «двоичный», англ.). Стандарт утверждён международно, 9
<b>Мультикаст группа</b>	Адрес соответствующей мультикаст сети (IP или IPv6), служащий идентификатором для группы узлов, 66
<b>Промежуточный формат</b>	см. <b>CIF</b> , 31
<b>СМВ</b>	Система мультимедийного вещания, 79
<b>Слайс</b>	Набор макроблоков в порядке растрового сканирования (не обязательно последовательных), 46

## СОДЕРЖАНИЕ

### СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СОКРАЩЕНИЙ И ТЕРМИНОВ 2

<b>ВВЕДЕНИЕ</b>	<b>10</b>
<b>1 ИССЛЕДОВАНИЕ ПРИНЦИПОВ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ</b>	<b>13</b>
1.1 Анализ принципов мультимедийного вещания в сетях передачи данных . . . . .	13
1.1.1 Классификация технологий доставки информации от сервера до клиента . . . . .	16
1.1.2 Антагонизмы в реализации вещания мультимедийного контента . . . . .	19
1.2 Классификация и анализ форматов представления мультимедийного контента . . . . .	22
1.2.1 Аналоговые телевизионные стандарты . . . . .	22
1.2.1.1 NTSC . . . . .	22
1.2.1.2 PAL . . . . .	23
1.2.1.3 SECAM . . . . .	24
1.2.2 Цифровые форматы телевизионного и радийного вещания . . . . .	25
1.2.2.1 DVB . . . . .	25
1.2.2.2 ATSC и ISDB . . . . .	26
1.2.2.3 DAB . . . . .	27
1.2.2.4 DRM . . . . .	27
1.2.3 Анализ и выбор формата . . . . .	29
1.3 Анализ прикладного ПО для организации мультимедийного вещания . . . . .	30
1.3.1 Проект VideoLAN . . . . .	31
1.3.2 Решения Microsoft . . . . .	32
1.3.3 Формулирование требований к распределенной системе мультимедийного вещания . . . . .	33
Выводы . . . . .	35
<b>2 ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКОГО АППАРАТА ПРЕДСТАВЛЕНИЯ ВИДЕОДАННЫХ В КОМПАКТНОМ ВИДЕ ДЛЯ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ</b>	<b>36</b>
2.1 Концепция цифрового видео . . . . .	36
2.1.1 Цветовые модели . . . . .	36
2.1.1.1 CMYK . . . . .	36
2.1.1.2 RGB . . . . .	37
2.1.1.3 YCbCr . . . . .	37
2.1.2 Качество изображения . . . . .	38
2.1.2.1 Субъективная оценка качества . . . . .	38
2.1.2.2 Объективная оценка качества . . . . .	39
2.2 Концепция сжатия видео . . . . .	40
2.2.1 Временная модель . . . . .	40
2.2.2 Пространственная модель . . . . .	41
2.2.2.1 Дискретное косинусное преобразование . . . . .	43
2.2.2.2 Дискретное вейвлет-преобразование . . . . .	45
2.2.2.3 Реорганизация данных . . . . .	46
2.2.3 Энтропийное сжатие . . . . .	47
2.2.3.1 Код переменной длины . . . . .	47
2.2.3.2 Арифметическое кодирование . . . . .	49

2.3	Кодек ITU-R H.264 . . . . .	50
2.3.1	Структура . . . . .	51
2.3.2	Интер-предсказание . . . . .	53
2.3.2.1	Субпиксельная интерполяция . . . . .	53
2.3.2.2	Предсказание векторов движения . . . . .	55
2.3.2.3	Взвешенное предсказание . . . . .	55
2.3.3	Интра-предсказание . . . . .	56
2.3.4	Фильтр блочности . . . . .	57
2.3.5	Преобразование и квантование . . . . .	58
2.3.5.1	Преобразование блоков $4 \times 4$ . . . . .	58
2.3.5.2	Квантование . . . . .	60
2.3.6	Реорганизация данных . . . . .	60
2.3.7	Энтропийное кодирование . . . . .	61
2.3.7.1	Экспоненциальное энтропийное кодирование Голомба . . . . .	61
2.3.7.2	Контекстнозависимое кодирование переменной длины . . . . .	61
2.3.7.3	Контекстнозависимое бинарное арифметическое кодирование . . . . .	62
	Выводы . . . . .	63
<b>3</b>	<b>ИССЛЕДОВАНИЕ И РАЗРАБОТКА СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СИСТЕМЕ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ</b>	<b>64</b>
3.1	Многоуровневая модель защиты данных DVB-CSA . . . . .	65
3.2	Гибридная модель защиты данных IP-вещания . . . . .	67
3.2.1	Процесс скрамблирования алгоритмом симметричного шифрования AES . . . . .	71
3.2.1.1	Преобразование SubBytes() . . . . .	74
3.2.1.2	Преобразование ShiftRows() . . . . .	74
3.2.1.3	Преобразование MixColumns() . . . . .	75
3.2.1.4	Преобразование AddRoundKey() . . . . .	75
3.2.1.5	Алгоритм выработки ключей . . . . .	76
3.2.2	Создание защищённой unicast сети между оператором и абонентом . . . . .	76
3.2.2.1	Алгоритм асимметричного шифрования RSA . . . . .	78
3.2.2.2	Безопасная передача данных на основе протокола SSL . . . . .	79
3.2.3	Реализация модели защиты данных IP-вещания с помощью openSSL . . . . .	81
	Выводы . . . . .	83
<b>4</b>	<b>РЕАЛИЗАЦИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ</b>	<b>84</b>
4.1	Подсистема управления и контроля распределенной системы IP-вещания . . . . .	85
4.1.1	Абонентское управление . . . . .	87
4.1.2	Управление вещанием . . . . .	87
4.1.3	Вещательная база данных . . . . .	89
4.2	Подсистема формирования контента распределенной системы IP-вещания . . . . .	93
4.2.1	Базовые блоки подсистемы формирования контента . . . . .	93
4.2.2	Компоненты формирования контента . . . . .	95
4.2.3	Аппаратное обеспечение программно-аппаратный компонентов источников контента . . . . .	98
4.2.3.1	Оцифровка аналогового сигнала (без встроенного кодировщика) . . . . .	98

4.2.3.2	Оцифровка аналогового сигнала (со встроенным кодировщиком) . . . . .	100
4.2.3.3	Прием цифрового эфирного, кабельного и спутникового телевидения . . . . .	101
4.2.4	Исследование реализаций компонентов для мультимедийного вещания	103
4.3	Сетевая подсистема распределенной системы IP-вещания . . . . .	105
4.3.1	Гибридная схема доставки мультимедийных данных . . . . .	106
4.3.2	Протоколы работы сетевой подсистемы мультимедийного вещания . .	107
4.3.2.1	Протокол передачи мультимедийных данных . . . . .	108
4.3.2.2	Протокол установления соединения для доступа абонентов к ресурсам вещания . . . . .	111
4.3.2.3	Протокол запросов мультимедийных данных и получения ключей дескрамблирования . . . . .	112
4.4	Абонентская подсистема распределенной системы IP-вещания . . . . .	113
4.4.1	Подсистема доступа к потоковому вещанию . . . . .	113
4.4.2	Подсистема доступа к Интернет-вещанию . . . . .	117
	Выводы . . . . .	119
<b>5</b>	<b>РАЗРАБОТКА НЕСУЩЕЙ КОНСТРУКЦИИ СЕРВЕРА ВЕЩАНИЯ И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СИСТЕМЫ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ</b>	<b>120</b>
5.1	Несущая конструкция сервера вещания . . . . .	120
5.1.1	Разработка несущей конструкции . . . . .	120
5.1.2	Испытания несущей конструкции . . . . .	121
5.2	Построение экспериментальной системы мультимедийного вещания . . . . .	122
5.3	Методика и порядок испытаний системы мультимедийного вещания . . . . .	124
5.4	Результаты испытаний системы мультимедийного вещания . . . . .	126
5.4.1	Дифференциальные оценки качества ПО . . . . .	126
5.4.2	Интегральные оценка качества ПО . . . . .	126
5.4.2.1	Стабильность аппаратного и программного обеспечения . . . . .	127
5.4.2.2	Использование канала передачи данных . . . . .	127
5.4.2.3	Использования сервера вещания . . . . .	128
	Выводы . . . . .	130
	<b>ЗАКЛЮЧЕНИЕ</b>	<b>131</b>
	<b>СПИСОК ЛИТЕРАТУРЫ</b>	<b>133</b>
	<b>ПРИЛОЖЕНИЕ А Несущая конструкция сервера вещания</b>	<b>135</b>
	<b>ПРИЛОЖЕНИЕ Б Графический материал</b>	<b>139</b>

## ВВЕДЕНИЕ

**Актуальность.** Высокотехнологическое общество требует таких же высокотехнологичных подходов к реализации различного рода услуг. К таковым тенденциям следует отнести и объединение передачи данных и голоса в рамках одного кабеля с использованием сетей передачи данных и технологий IP-телефонии. Кроме того, одним из элементов такого объединения является передача телевизионных каналов по сетям передачи данных, что, кроме стандартных возможностей обычного телевидения, предоставляет контент-провайдерам дополнительные возможности по насыщению информационной потребности клиентов - предложение различных пакетов телепрограмм основанных на потребностях и желаниях потребителей, внедрение услуг виртуальных кинозалов и технология видео-по-запросу (Video-On-Demand, VOD).

Продажа услуг является гораздо более выгодным бизнесом для операторов сетей передач данных, нежели простая продажа Интернет-трафика. По данным Minerva Networks Inc. [1] в США на связь и развлечения абоненты тратят в среднем \$150, в России этот показатель находится на гораздо более низком уровне, но имеется тенденция к росту этого показателя [2].

Самым ярким примером, иллюстрирующим и технологические возможности, и высокую заинтересованность потребителей в услуге, является предлагаемая компанией ЗАО «Комстар-Директ» услуга Стрим-ТВ [19]. Однако применяемая технология ADSL существенно ограничивает и количество потенциальных потребителей (жилые квартиры в Москве, оборудованные телефонной линией), и количество, и качество предоставляемых в рамках услуги продуктов (одновременный просмотр одной телепрограммы, невозможность просмотра HDTV телевидения).

Огромным классом потребителей являются клиенты больших домовых сетей городов России, в которых услуги такого рода практически не развиты. Кроме того, передача видеинформации по сетям передачи данных может использоваться для организации корпоративных систем телевещания, удаленного видеоконтроля объектов, а также организации систем телеобучения.

Построение систем вещания влечет за собой ряд проблем, связанных с тем, что мультимедийное вещание является особым субъектом сети передачи данных, для которого требуется как наличие достаточной пропускной способности самой сети (не менее 4.5 Мбит/с на один канал передачи данных в формате MPEG-2), так и необходимость качественной передачи данных с малыми задержками и потерями - обеспечение приоритизации передаваемого мультимедийного трафика по сети (QoS [3]). Не менее острой проблемой является получение лицензированного мультимедийного контента и защита его от несанкционированного использования.

Внедрение услуг цифрового телевидения в рамках сетей передачи данных не только расширяет спектр предоставляемых услуг (а следовательно и финансовую отдачу), но и позволяет в условиях жесткой конкуренции (в большинстве районов Москвы дома об-

служиваются тремя и более крупными провайдерами) положительно выделяться на фоне других.

Представленные на рынке продукты такие как Cisco IP TV, Minerva Video Concentrator реализуют лишь функцию сбора и подготовки исходного мультимедийного материала, его необходимое сжатие и передачу непосредственно в сеть, канaloобразующее оборудование которого должно обеспечивать полное управление потоками данных и, при необходимости, ограничение доступа пользователей к услуге. Для существующих структур построения большинства домовых сетей такой подход не приемлем, поскольку требует существенных затрат на модернизацию как магистральных участков сети, так и оконечного канaloобразующего оборудования.

**Цель работы.** Работа имеет своей целью разрешить противоречия как между возможностями и желаниями со стороны контент-провайдеров, так и между ожиданиями и предложениями услуг для пользователей системы.

**Решаемые задачи:**

1. Исследование принципов мультимедийного вещания в сетях передачи данных с классификацией технологий доставки информации от сервера до клиента и форматов представления мультимедийного контента.
2. Изучение возможностей стандартизованных технологий представления и передачи мультимедийной информации в сетях передачи данных.
3. Исследование возможностей математического аппарата применяемого в форматах представления мультимедийных данных в цифровом виде.
4. Исследование способов защиты мультимедийной информации в мультикаст-сетях и разработка схемы защиты мультимедийного вещания от несанкционированного доступа.
5. Исследование структуры и прототипов аппаратного обеспечения для получения мультимедийного контента из исходной формы.
6. Разработка серверного и клиентского программного обеспечения системы мультимедийного вещания.
7. Разработка несущей конструкции сервера вещания и построение на её основе опытного образца сервера вещания и внедрение его в эксплуатацию.

**Методы исследования.** Для достижения поставленных целей и задач в работе использован математический аппарат теории цифровой обработки сигналов, теории сжатия изображений и видео, а также приемы и методология формализованного проектирования программного обеспечения RUP.

**Достоверность полученных научных результатов, выводов и рекомендаций диссертационной работы подтверждена:**

1. Результатами внедрения системы мультимедийного вещания в сети студгородка МГТУ им.Н.Э.Баумана, что подтвердило заинтересованность пользователей в подобных услугах, а также целесообразность создания систем мультимедийного вещания в сетях передачи данных.

2. Результатами внедрения разработанных в работе моделей, методов и алгоритмов мультимедийного сжатия, а также программного комплекса мультимедийного вещания в учебный процесс МГТУ им. Н.Э. Баумана, что показало важность мультимедийных данных в образовательном процессе.

**Реализация результатов.** Разработанный в рамках работы аппаратно-программный комплекс мультимедийного вещания по результатам приемо-сдаточных испытаний введен в эксплуатацию в сети Измайловского студгородка МГТУ им.Н.Э.Баумана на базе СНТО «Содействия развитию Измайловской компьютерной сети» (г.Москва).

Кроме того, разработанный комплекс внедрен в учебную и научную работу в рамках лаборатории цифрового телевидения на кафедре «Проектирование и технология производства электронной аппаратуры» (ИУ4) МГТУ им.Н.Э.Баумана.

**Апробация работы.** Результаты работы были представлены на VII молодежной научно-технической конференции «Наукоемкие технологии и интеллектуальные системы» (Россия, Москва, 20-21 апреля 2005), международном научно-техническом симпозиуме «Образование через науку» (Россия, Москва, 17-19 мая 2005).

По результатам Всероссийского конкурса на лучшие научно-технические и инновационные работы студентов по естественным, техническим и гуманитарным наукам (Россия, Москва, декабрь 2003) работа была удостоена диплома 1 степени, награждена дипломом открытого конкурса ОАО «Мосэнерго» на лучшие дипломный и курсовой проекты студентов вузов России (Россия, Москва, 27 мая 2004), дипломом 1 степени во «Всероссийском конкурсе на лучшие научно-технические и инновационные работы студентов по естественным, техническим и гуманитарным наукам» (2005 год), дипломом победителя «Всероссийского конкурса инновационных проектов» (2005 год).

Результаты работы отмечены стипендией Правительства Российской Федерации (2004/2005, 2006/2007 учебные годы), АФК «Система» (2004/2005 учебный год, 2006/2007 учебный год), клуба «Императорского Технического Училища» (2005 год), премией АФК «Система» молодым ученым и специалистам.

**Публикации.** Основные результаты работы опубликованы в 9 печатных работах, докладывались на конкурсах, конференциях и симпозиумах.

# 1 ИССЛЕДОВАНИЕ ПРИНЦИПОВ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

В данном разделе будут рассмотрены принципы мультимедийного вещания в сетях передачи данных, представляющего собой передачу от некоторого центрального узла (иначе — сервера вещания) информационного потока, включающего в себя аудио и визуальные данные с некоторым объёмом служебной информации, и её воспроизведение абонентским приёмным оборудованием (программным обеспечением). Под сетями передачи данных подразумеваются информационные сети различной структуры и топологии, поддерживающие передачу данных протоколу IP (rfc791, rfc793) или IPv6.

## 1.1 Анализ принципов мультимедийного вещания в сетях передачи данных

Постоянное усовершенствование технологий сетей передачи данных с одновременным удешевлением оборудования привело к стремительному росту числа высокоскоростных сетей передачи данных и все большему числу пользователей услуг, предоставляемых этими сетями. Классификация услуг, которые могут предоставляться абонентам, представлена на рис.1.1.

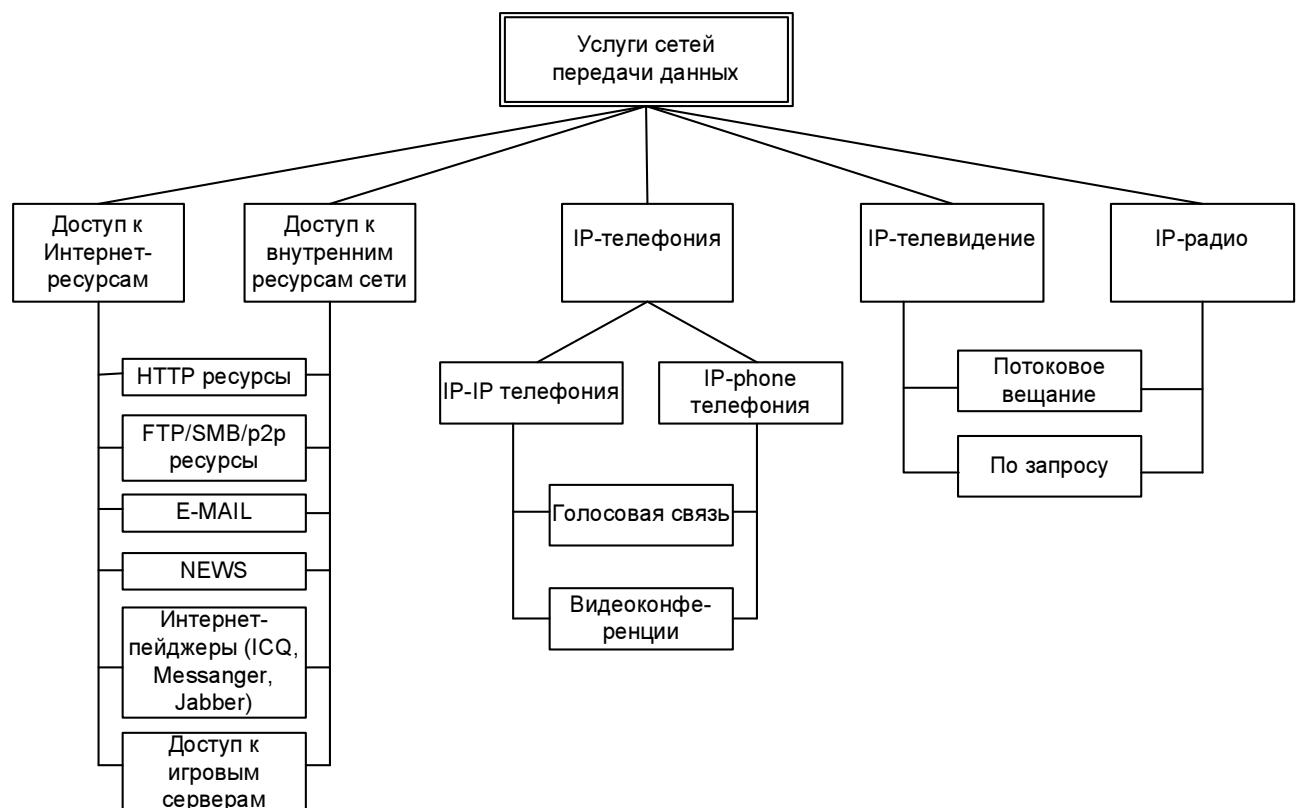


Рисунок 1.1 – Классификация услуг сетей передачи данных

Как видно из классификации, услуги сетей передачи данных можно разделить

на четыре категории: доступ к Интернет ресурсам, доступ к внутренним ресурсам, IP-телефония и IP-телевидение. Различия Интернет-ресурсов и внутренних ресурсов заключается в различных скоростных возможностях, а также затратах на организацию информационного обмена. С точки зрения оператора желательно, чтобы максимальный информационный поток находились внутри сети (игровой трафик, обмен данными и проч.), без задействования дорогого канала доступа к сети Интернет.

Услуга IP-телефонии в последнее время получила бурное развитие. Особенно это заметно с активным приходом на рынок компании Skype. Условно IP-телефонию можно разделить на телефонию только в рамках сетей передачи данных (IP-IP), а также телефонию, связывающую сеть передачи данных с обычной телефонной сетью (IP-phone) (H.323, H.225, H.245, Q931) как в направлении компьютер→телефонная сеть, так и в направлении телефонная сеть→компьютер.

Наиболее перспективными, но пока еще не так сильно распространенными услугами являются IP-телевидение и IP-радио. Предоставление этих услуг возможно только в сетях со скоростью передачи данных 100 и более Мбит/с. Обе услуги могут быть реализованы как в виде потокового вещания -(практически полный аналог существующего телевидения и радио с отличием только в среде и форме передачи сигнала от источника к потребителю), так и в виде телевидения и радио по запросу, когда абоненты запрашивают и просматривают только необходимые им в данный момент времени фильмы, информационные и развлекательные передачи, либо запрашивают отложенный просмотр программ потокового вещания. Радио- и видеоданные возможно объединить единым термином - мультимедиа данные или мультимедийный контент.

В таблице 1.1 представлены сравнительные характеристики требований к мультимедийному вещанию в сетях передачи данных.

Основной задачей для операторов сетей передачи данных, развертывающих системы IP-телевидения и IP-радио (или иначе IP-TV), является задача поиска источников самого мультимедийного контента и выявления критериев сравнения этих источников. На рис.1.2 представлена классификация источников мультимедийного контента.

Как видно из этой классификации, в качестве источников мультимедийного контента могут выступать: файлы с мультимедиа информацией на носителях, эфирное телевидение, эфирное радио, кабельное телевидение, спутниковое телевидение, а также различного вида локальные источники мультимедийной (видео и/или аудио) информации. Дальнейшее разделение каждого источника основывается на различиях оборудования распознавания/приема данного вида контента.

Каждый вид источника обладает своими достоинствами и недостатками, поэтому для получения объективной картины необходимо выделить критерии сравнения, например:

1. Информационная новизна.
2. Стоимость оборудования для получения мультимедийного контента.
3. Сложность преобразования для потокового вещания.

Таблица 1.1 – Сравнительные характеристики требований к мультимедийному вещанию

Наименование сервиса	Протокол	Средняя емкость ресурса, бит/с	Назначение	Аппаратные средства	Примечание
Потоковое вещание видео (multicast)	MPEG2, MPEG4 (UDP, RTP)	4-6М, 2-4М	Потоковое вещание при использовании специализированного каналаоб разующего оборудования	SkyStar3 (PCI плата), SkyStar1	Телевизионное качество (540x768)
Потоковое вещание аудио (multicast)	MPEG1 Layer3 (UDP, RTP)	128k			Стереозвук
Потоковое вещание видео (unicast)	MPEG2, MPEG4 (UDP, RTP)	4-6М, 2-4М			Телевизионное качество (540x768)
Потоковое вещание аудио (unicast)	MPEG1 Layer3 (UDP, RTP)	128k			Стереозвук
IP телефония	H.323	6k-64k	Местная телефонная связь, доступ к международной и международной телефонной сети	IP-Phone, шлюзы IP телефонии	Интерактивный режим
Видео конференцсвязь	H.323	64k-256k	Видеотелефония	микрофон, WEB-камера	Интерактивный режим

4. Сложность преобразования и классификации для услуги видео-по-запросу.

5. Количество доступных различных источников одного типа.

Критерии оценивались на основании мнения студентов МГТУ им.Н.Э.Баумана, живущих в Измайловском студгородке, по 5-ти бальной шкале: 1 - наихудшее, 5 - наилучшее состояние. Результаты сведены в таблицу 1.2.

Как можно увидеть из таблицы, у каждого из источников имеются свои достоинства и недостатки. Поэтому выбор того или иного источника должен определяться как с учетом вышеуказанных критериев, так и с учётом различного рода ограничений (возможностей приобретенного или разработанного программного обеспечения, финансовых, организационных) и мнения потенциальных абонентов данной услуги.

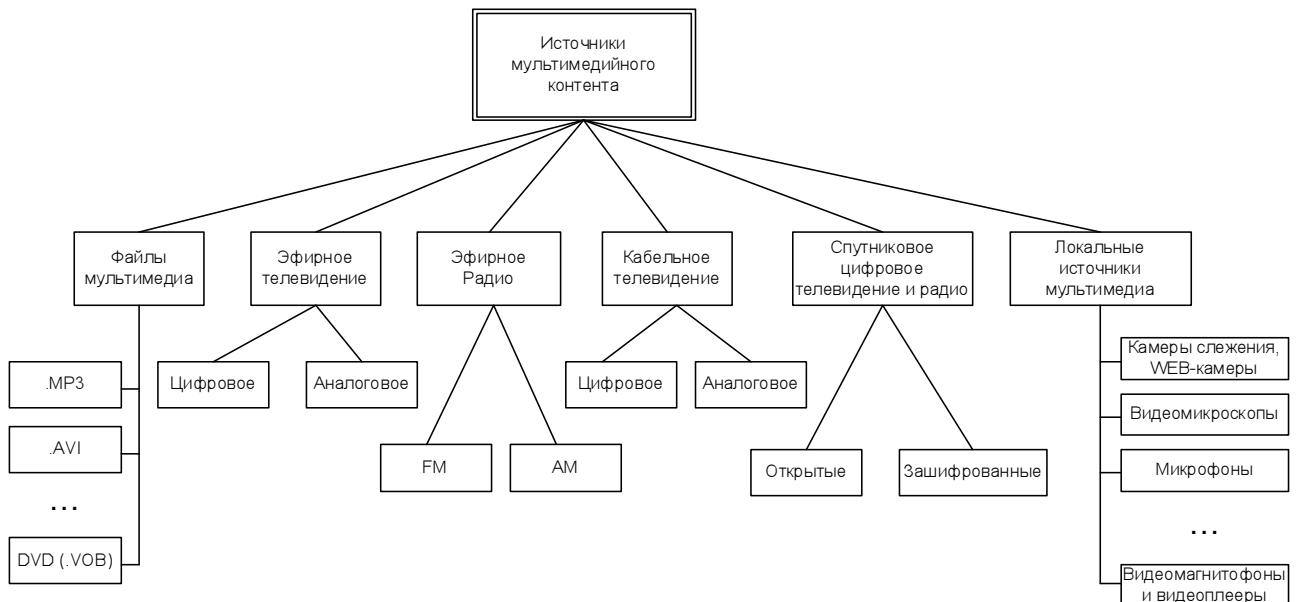


Рисунок 1.2 – Классификация источников мультимедийного контента

Таблица 1.2 – Оценка источников мультимедийного контента

Источник	Критерий				
	1	2	3	4	5
Файлы мультимедиа	1	1	3	1	5
Цифровое эфирное телевидение	4	4	1	5	1
Аналоговое эфирное телевидение	4	2	5	5	4
Эфирное радио (FM,AM)	4	2	4	5	4
Цифровое кабельное телевидение	4	4	1	5	2
Аналоговое кабельное телевидение	4	2	5	5	2
Открытое спутниковое цифровое телевидение и радио	4	3	1	5	4
Зашифрованное спутниковое цифровое телевидение и радио	5	5	3	5	5
Локальные источники мультимедиа	2	3	3	5	3

### 1.1.1 Классификация технологий доставки информации от сервера до клиента

Под технологией доставки информации от сервера до клиента следует понимать многообразие протоколов передачи данных, с помощью которых осуществляется общение сервера вещания и клиента в рамках сети передачи данных. Существует две основные схемы доставки цифровых потоков по IP сетям, обладающих своими достоинствами и недостатками: технология точка-точка (unicast), технология точка-многоточка (multicast) (рис.1.3а и 1.3б соответственно).

В случае использования unicast технологии возможно использование протоколов передачи данных без гарантии доставки: UDP, RTP (Real-Time Transport Protocol - Протокол передачи реального времени, RFC-2205, -2209, -2210, -1990, -1889, -3989, -3952; «RTP: A Transport Protocol for Real-Time Applications» H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson). Последний базируется на идеях, предложенных Кларком и Тенненхаузом [5], и предназначен для доставки данных в реальном масштабе времени. При этом определяется

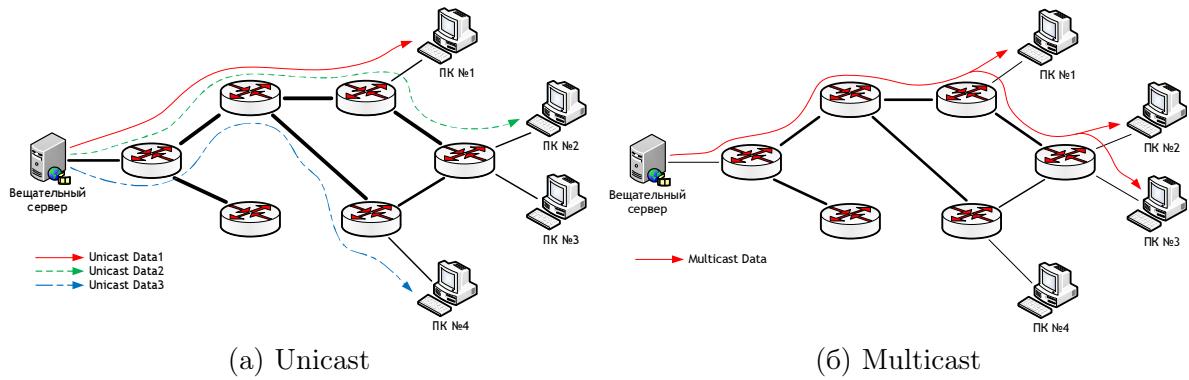


Рисунок 1.3 – Схемы доставки цифрового потока от сервера до клиента

тип поля данных, производится нумерация посылок, присвоение временных меток и мониторинг доставки. Приложения обычно используют RTP поверх протокола UDP для того, чтобы использовать его возможности мультиплексирования и контрольного суммирования. Но RTP может использоваться и поверх любой другой сетевой транспортной среды. Однако сам по себе RTP не обеспечивает своевременной доставки и не предоставляет каких-либо гарантий уровня сервиса. Этот протокол не может гарантировать также корректного порядка доставки данных. Правильный порядок выкладки информации может быть обеспечен принимающей стороной с помощью порядковых номеров пакетов. Такая возможность крайне важна практически всегда, но особое внимание этому уделяется при восстановлении передаваемого изображения.

Кроме того, при использовании unicast возможно применение и протоколов с гарантированной передачей данных: TCP, HTTP. В этом случае будет несколько увеличен информационный поток, но зато будет гарантировано качество принимаемого мультимедийного контента в условиях ненадежного канала передачи данных. Под ненадежностью канала в данном случае должны пониматься кратковременные отказы передачи (различного рода коллизии в сети), сбои в передаче (неправильный порядок IP пакетов принятых клиентским ПО из-за различного времени доставки) и прочее. Информационная ёмкость самого канала должна быть достаточна как для передачи мультимедийного контента, так и для передачи служебной информации и повторных частей мультимедийного контента.

При использовании multicast технологии возможно применение следующих протоколов без гарантии доставки: UDP, RTP. Как уже отмечалось выше RTP обеспечивает некоторый контроль за информационным потоком, но не может полностью гарантировать доставку данных до клиента. Использование multicast технологии с UDP или RTP протоколом совместно с интеллектуальным каналообразующим оборудованием, поддерживающим IGMP маршрутизацию (RFC-1112, RFC-2236), позволяет достичь максимальной эффективности сервера мультимедийного вещания - аппаратные и программные затраты сервера вещания идут только на получение мультимедийного контента и передачу его в сеть, а доставку до конкретного абонента и гарантию этой доставки будет обеспечивать каналообразующее оборудование.

Кроме того, существует возможность передачи multicast трафика по unicast сети с помощью так называемой технологии MBONE [4]. MBONE — это виртуальная сеть, базирующаяся на multicast-протоколах, которые были одобрены IETF (The Internet Engineering Task Force) летом 1992 года. В основу легли разработки, выполненные в компании Ксерокс. Данный режим работы поддерживается не всеми маршрутизаторами. Сеть представляет собой систему Ethernet-сетей, объединенных друг с другом соединениями точка-точка, которые называются «туннелями» (DVMRP Tunnel).

Конечными точками таких туннелей обычно являются машины класса рабочих станций, снабженные соответствующим программным обеспечением (Multicast router). Впервые multicast-туннель был реализован в Стэнфордском университете в 1988 году. IP-multicast-пакеты инкапсулируются при передаче через туннели так, что они выглядят как обычные IP-unicast-пакеты. Таким образом, возможно объединение нескольких multicast сетей с помощью высокоскоростных каналов передачи данных, не поддерживающих технологию multicast. Сравнительная оценка параметров технологий доставке представлена в таблице 1.3.

Таблица 1.3 – Оценка параметров unicast и multicast

<b>Особенности</b>	
Непосредственная передача данных от сервера клиенту с установлением или без установления соединения. Причем в отправляемых IP пакетах явно указывается IP адрес сервера и IP адрес клиента.	Опосредованная передача данных от сервера клиенту, осуществляемая с помощью входа сервера и клиентов в т.н. multicast группы [6]. В IP пакетах, отправляемых сервером содержится IP адрес самого сервера и адрес multicast группы, для которой предназначен пакет. Каналообразующее оборудование (маршрутизаторы, коммутаторы) производят отслеживание подключения и отключения клиентов к/из multicast групп и соответственно направляют или не направляют соответствующий IP пакет в сегмент клиента
<b>Используемые протоколы</b>	
передачи: TCP, UDP, RTP, HTTP маршрутизации: RIP, BGP, OSPF	UDP, RTP IGMP
<b>Каналообразующее оборудование, поддерживающее передачу по схемам</b>	
Все оборудование, поддерживающее передачу данных по протоколу IP	Маршрутизаторы, поддерживающие протокол маршрутизации IGMP Коммутаторы с поддержкой IGMP Snooping Прочие коммутаторы и концентраторы с передачей multicast пакетов в широковещательном режиме

При решении вопроса относительно схемы предоставления мультимедийных услуг необходимо учитывать существующую инфраструктуру IP сети (существующее оборудование, возможности по его модернизации), количество пользователей сети, количество

потенциальных абонентов услуги.

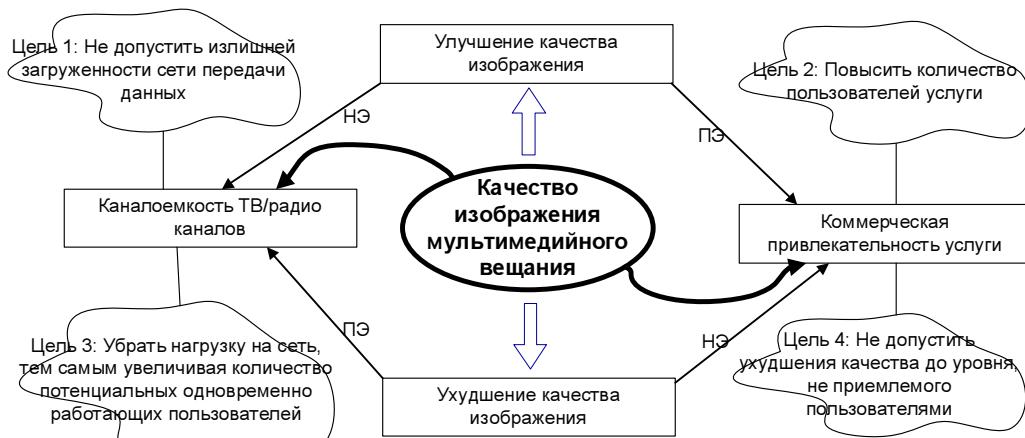
Принципиально может сложиться две ситуации - мультимедийные услуги должны быть приложением и простым расширением функциональности базовой IP сети (сети предприятий, офисов) и мультимедийные услуги как отдельный вид предоставляемых услуг внутри сети (за определенную плату). Основное различие этих ситуаций - отсутствие и наличие необходимости организации системы разграничения доступа к мультимедиа услугам.

В случае unicast технологии организация разделения доступа реализуется достаточно просто стандартными методами. В частности может быть организован доступ к серверу мультимедиа контента с использованием паролей доступа. В случае применения multicast технологии, организация защиты от несанкционированного доступа достаточно сложна. Это должно быть либо чисто аппаратное решение, когда каналообразующему оборудованию указываются абоненты, которым разрешен доступ к услуге, либо это должно быть шифрование мультимедийного потока на стороне сервера и его дешифрация с помощью санкционировано раздаваемых ключей на стороне клиента.

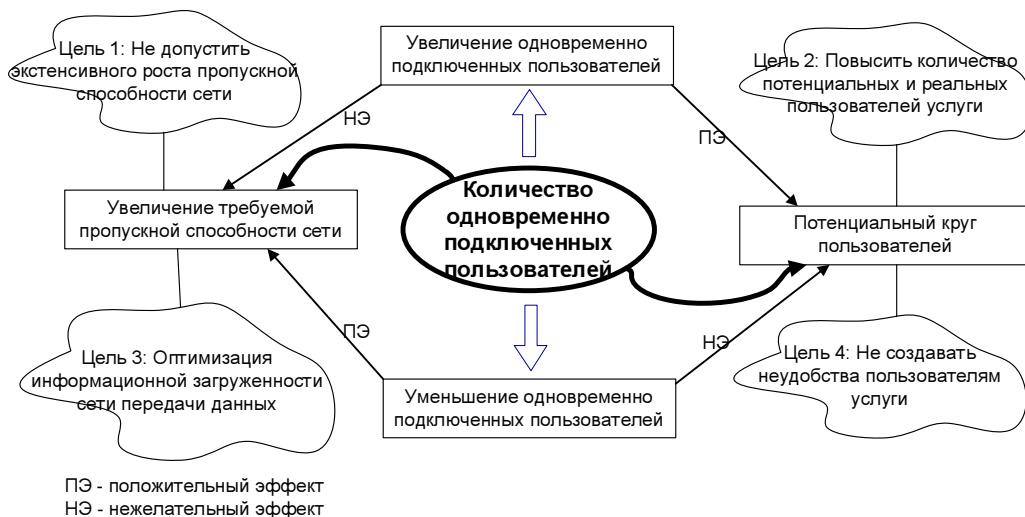
Решение вопроса об использовании той или иной технологии мультимедийной доставки информации в рамках сетей передачи данных не может быть осуществлено без анализа причин возникновения этих технологий и противоречий, возникающих при выборе той или иной технологии.

### **1.1.2 Антагонизмы в реализации вещания мультимедийного контента**

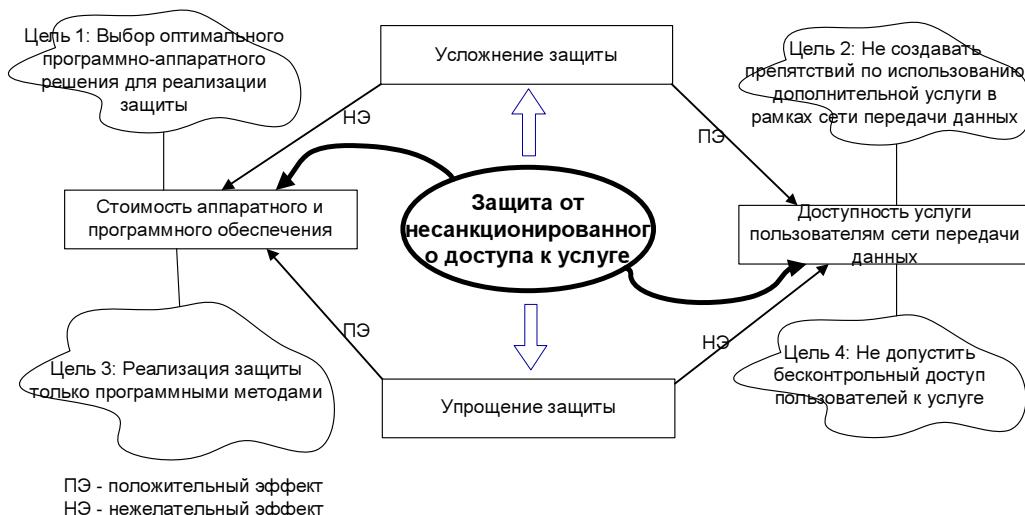
В реализации вещания мультимедийного контента можно выделить ряд противоречий, связанных с качеством изображения, используемого в мультимедийном вещании, с количеством пользователей, использующих услуги мультимедийного вещания (одновременно подключенных пользователей к серверу вещания), а также связанных со способом и уровнем защиты системы мультимедийного вещания от несанкционированного доступа к мультимедийным услугам (рис.1.4а, 1.4б и 1.4в соответственно).



(а) Качество изображения



(б) Количество абонентов



(в) Защита от несанкционированного доступа

Рисунок 1.4 – Противоречия в реализации системы IP-вещания

Из анализа противоречий можно выделить основные нестыковки между различного рода желаниями и целями:

1	<u>Желание уменьшить каналоемкость ТВ/радио канала</u>	<u>Желание увеличить качество изображения/звука</u>
2	Увеличить количество одновременно подключенных абонентов	Не увеличивать пропускную способность сети (не менять структуру сети)
3	Увеличить количество различного доступного для просмотра мультимедийного контента	Не увеличивать пропускную способность сети (не менять структуру сети); Не расширять аппаратную часть комплекса вещания
4	Организация полноценной системы защиты от несанкционированного доступа	Минимальные затраты (на аппаратное и программное обеспечение) для организации этой системы

Рассмотрим каждую из этих несостыковок и пути ее преодоления:

1. Уменьшение требуемой одним ТВ или радио каналом полосы пропускания сети передачи данных эффективно достигается путем увеличения уровня сжатия исходных мультимедиа данных. Решается это либо за счет использования более эффективных алгоритмов сжатия видео потока, либо за счет увеличения потерь качества. Второй подход реализуется гораздо проще, но не дает существенного уменьшения требуемой полосы пропускания при сохранении должного уровня качества.
2. Количество одновременно подключенных абонентов и различных вещаемых мультимедийных каналах является одним из ключевых моментов при построении комплекса мультимедийного вещания. Как уже отмечалось в п.1.1.1 существует unicast и multicast технологии доставки информации от сервера до абонента. Технология multicast хотя теоретически и может быть организована в рамках неуправляемых Ethernet сетей (без поддержки технологий IGMP маршрутизации), но эффективность такой реализации сводится к нулю, т.е. весь multicast трафик распространяется по всей сети независимо от того, есть ли подключенные пользователи multicast сервисов или нет. В таких сетях приобретает смысл реализации мультимедийного вещания посредством гарантированной unicast (например по протоколу TCP) передачи данных. В unicast реализации встает вопрос использования ресурсов вещательных серверов (один сервер может обслужить порядка 100-200 одновременно подключенных абонентов) и сегментации сети (блок вещательных серверов необходимо выделять в отдельную высокоскоростную сеть, должна существовать магистральная сеть оператора, раздельные абонентские сегменты сети).
3. Увеличение количества различного мультимедийного контента связано с одной стороны с возможностями сети передачи данных, с другой стороны — с возможностями оборудования, что обуславливает в конечном счете стоимость инсталляции системы IP-TV вещания. В случае использования в качестве источника мультимедийного контента открытых цифровых спутниковых каналов, то с

помощью одного экземпляра оборудования (DVB-модем) возможен прием для дальнейшей обработки целого ряда мультимедийных программ (ТВ и/или радио). В случае с эфирными телевизионными каналами - доступное на рынке оборудование обеспечивает получение только одного мультимедийного потока.

4. Как уже отмечалось, в случае unicast технологии организация разделения доступа реализуется достаточно просто чисто программными методами, но существуют ограничения на количество одновременно подключенных клиентов (в пересчете на сервер вещания и/или сегмент сети). Multicast снимает ограничения на количество одновременно подключенных абонентов, но организация защиты от несанкционированного доступа требует дополнительных программных или аппаратно-программных решений.

При построении системы IP-TV вещания для конкретной сети, после анализа исходных данных, а именно: а) количества и состава источников мультимедийного вещания, б) формы представления мультимедийного контента, в) метода распространения этого мультимедийного контента в рамках сети передачи данных, г) решения вопроса о том как должна быть реализована безопасности системы и защита от несанкционированного доступа, - принимается решение о закупке того или иного оборудования и раз-(до-)рабатывается программное обеспечение согласно требованиям оператора.

Чтобы выбрать конкретный тип источника мультимедийного вещания, необходимо проанализировать не только интересность и доступность различных типов источников, но и оценить необходимые затраты на преобразование контента из исходного формата в необходимый цифровой.

## **1.2 Классификация и анализ форматов представления мультимедийного контента**

Научно-техническая революция, а также экономические и политические интересы обусловили появление широкого спектра форматов представления мультимедийных данных. На смену разработанным в аналоговую эру различным стандартам телевизионного вещания NTSC, PAL, SECAM приходят цифровые форматы DVB, ATSC, ISDB. Классификация форматов представления передачи мультимедийного контента представлена на рис.1.5.

### **1.2.1 Аналоговые телевизионные стандарты**

#### **1.2.1.1 NTSC**

Система цветного телевидения NTSC была разработана в 1953 году в США Национальным комитетом по телевизионным стандартам (National Television Standards Committee). NTSC принята в качестве стандартной системы цветного телевидения также в Канаде, Японии и ряде стран американского континента. В качестве сигналов для передачи цветовой информации в системе NTSC приняты цветоразностные сигналы. Передача этих



Рисунок 1.5 – Классификация форматов представления мультимедиа данных

сигналов осуществляется в спектре сигнала яркости на одной цветовой поднесущей.

Кроме эксплуатационных недостатков, связанных со сложным принципом передачи и разделения сигналов цветности - квадратурной модуляцией и синхронным детектированием, необходимо указать на большую подверженность системы NTSC искажениям типа «дифференциальная фаза» и «дифференциальное усиление». Первое приводит к искажениям цветового тона, который изменяется в зависимости от мгновенного значения сигнала яркости. Второе из-за нелинейности амплитудных характеристик приводит к искажениям насыщенности.

Помимо так называемого «базового» NTSC M (525 строк/30 кадр./сек./частота поднесущей цвета 3,58 МГц), существуют еще три варианта этой системы. Первый называется NTSC 4,43 и используется в мультистандартных VHS-видеомагнитофонах. Временные параметры видеосигнала такие же, как в базовом NTSC M. Разница в том, что цветовое кодирование и декодирование производится в «PAL-формате», т.е. частота цветовой поднесущей такая же, как в PAL (4,43 МГц). Второй вариант NTSC-J используется в Японии (Japan). Отличается от базового NTSC M отсутствием подпорки гасящих интервалов в активной части строки. Соответственно амплитуда его составляет 0,714 В вместо принятого в NTSC 1 В (впрочем как в PAL и SECAM). Третий вариант имеет название «noninterlaced NTSC».

Достоинства и недостатки стандарта NTSC по сравнению с другими представлены в таблице 1.4.

### 1.2.1.2 PAL

Эта система (Phase Alternation Line - строка с переменной фазой), разработанная в ФРГ, в своей основе содержит все идеи американской NTSC. Особенность PAL заключа-

Таблица 1.4 – Достоинства и недостатки NTSC

Преимущества	Недостатки
Более высокая (по сравнению с PAL и SECAM) частота кадров - использование частоты кадров 30 Гц (в действительности 29,97 Гц) приводит к уменьшению заметности мерцания изображения.	Более выраженные муар, точечная интерференция и перекрестные искажения - это происходит из-за большей вероятности взаимодействия с монохромным сигналом изображения на более низкой частоте поднесущей.
Высокая точность редактирования цвета - возможно редактировать любые 4 поля без оказания влияния на цвет.	Изменение оттенка - вариации фазы цветовой поднесущей вызывают сдвиги в отображении цветов, заставляя оснащать приемники регулировкой оттенка (Tint). Многие NTSC-телевизоры имеют цепи автоматической регулировки оттенка.
Менее заметные шумы на изображении, достижение лучшего соотношения сигнал/-шум, чем в PAL/625.	
Меньшее число строк развертки - сниженная вертикальная четкость, более заметна строчная структура на экранах с большой диагональю.	Более низкая по отношению к PAL контрастность - значение гамма-коррекции составляет 2,2, в то время как в PAL/625 оно равно 2,8.

ется в оригинальном способе устранения фазовых искажений, присущих системе NTSC.

В системе PAL фаза поднесущей одного цветоразностного сигнала от строки к строке меняется на 180 градусов. Кроме того, в приемнике используется линия задержки на время одной строки (64 мкс). Т.е. имеются два сигнала цветности с относительной задержкой на одну строку. Изменение фазы от строки к строке на 180° приводит к тому, что фазовые ошибки, одинаковые по величине, имеют разные знаки. Сложение напряжения на входе линии задержки с перевернутым напряжением на ее выходе устраниет ошибку (сбой) фазы.

При очевидных достоинствах главным недостатком системы PAL является существенное усложнение ТВ-приемника за счет введения в его схему дополнительных узлов для задержки сигнала цветности на время одной строки и периодического изменения фазы цветоразностного сигнала. Следует также отметить, что искажения типа «дифференциальное усиление» в PAL не компенсируются. Достоинства и недостатки стандарта PAL по сравнению с другими представлены в таблице 1.5.

### 1.2.1.3 SECAM

В 1958 г. французский инженер Анри де Франс изобрел новую систему, названную SECAM (SEquential Couleur Avec Memoire), в которой отсутствовал основной недостаток NTSC - искажения цветового тона, вызываемые нелинейностью частотных, фазовых и амплитудных характеристик узлов телевизионного тракта. В SECAM информация о цветовом тоне не определяется фазовыми соотношениями сигналов цветности. В первых вариантах (система «Анри де Франс») информация о цветовом тоне передавалась амплитудной модуляцией поднесущей. В более усовершенствованной системе SECAM цветовая информация передается с помощью частотной модуляции поднесущей цвета.

Цветоразностные сигналы в SECAM передаются поочередно: в течение одной стро-

Таблица 1.5 – Достоинства и недостатки PAL

Преимущества	Недостатки
<p>Более детальная картинка - большее число строк развертки, а также более широкая полоса сигнала яркости.</p> <p>Устойчивость оттенков - благодаря инверсии фазы поднесущей на каждой последующей строке, любое фазовое искажение будет подавлено. Более высокий уровень контраста - значение гамма-коррекции 2,8 против 2,2 в NTSC/525.</p>	<p>Более заметное мерцание по сравнению с NTSC - более низкая частота кадров (25 кадров/сек.).</p> <p>Более заметны шумы - требование более высокой частоты поднесущей приводит к ухудшению отношения сигнал/шум в PAL/625 по сравнению с NTSC/525. Потеря точности редактирования цвета - из-за чередования фазы цветового сигнала редактирование может быть осуществлено с точностью <math>\pm 4</math> кадра (8 полей). Снижение цветовой насыщенности при неизменном оттенке - точность цветов достигается посредством потери информации о разности фаз сигналов оттенка и насыщенности.</p>

ки - сигнал R-Y, в течение следующей - B-Y и т. д. Цветовая информация как для R-Y, так и для B-Y «снимается» через строку. При этом предполагается, что в пропущенных строках цветовая информация идентична соседним. Иными словами, для сигналов цветности полный кадр содержит вдвое меньшее количество строк, что приводит к соответствующему увеличению размеров окрашенных мелких деталей по вертикали. Визуальная четкость по вертикали при этом не снизится, т.к. более мелкие детали передаются сигналом яркости Y с полным числом строк развертки. Таким образом, при поочередной (через строку) передаче сигналов цветности в приемнике в результате использования элемента памяти (линии задержки) образуются три исходных сигнала цветности. Поэтому рассматриваемую систему часто называют последовательно-одновременной (или по-французски Sequential a memoire - последовательная с памятью).

Одной из причин принятия на «вооружение» SECAM во Франции была защита внутреннего рынка от «вторжения» чуждой NTSC. Хотя новизна решений и явные преимущества при создании системы также были учтены. И в СССР эта система была принята не в последнюю очередь по политическим соображениям - лишь бы не американская NTSC и немецкий PAL. Естественно, и страны Варшавского договора «добровольно» приняли SECAM (пожалуй, только ГДР удалось отстоять «свой» стандарт звука - 5,5 МГц вместо советских 6,5).

Достоинства и недостатки стандарта SECAM по сравнению с другими представлены в таблице 1.6.

## 1.2.2 Цифровые форматы телевизионного и радийного вещания

### 1.2.2.1 DVB

DVB (Digital Video Broadcasting Project, DVB-C, DVB-DSNG, DVB-H, DVB-MC, DVB-MS, DVB-MT, DVB-P, DVB-S, DVB-S2, DVB-SFN, DVB-SMATV, DVB-T, DVB-MHP,

Таблица 1.6 – Достоинства и недостатки SECAM

Преимущества	Недостатки
Устойчивость оттенка и постоянство насыщенности. Большее вертикальное разрешение - в SECAM используется более высокое число строк развертки, чем в NTSC/525	<p>Более заметно мерцание по сравнению с NTSC. Невозможно смешивание двух синхронных сигналов цвета SECAM - большинство ТВ-студий в SECAM-странах работают в PAL и переводят передачи в SECAM лишь для вещания. Кроме того, продвинутое домашнее оборудование S-VHS, Hi8 записывает в PAL и только при проигрывании транскодирует в SECAM. Регулярные шумовые структуры на изображении (сеточка и др.) - частотная модуляция приводит к появлению регулярных шумовых структур даже на нецветных объектах.</p> <p>Сниженное качество монохромного сигнала - т.к. одна из цветовых поднесущих имеет частоту 4,25 МГц, полоса меньшей ширины может быть использована для монохромного сигнала.</p> <p>Несовместимость между различными версиями SECAM - некоторые из вариантов SECAM (эфир и видео) несовместимы друг с другом. Например, между оригинальной французской версией SECAM и так называемым Middle East SECAM.</p>

DVB-M) - организация, которая разрабатывает технологии для цифрового телевидения [20]. В Европе наиболее широко используются следующие протоколы передачи, разработанные DVB: DVB-C (для кабельных сетей EN 300 429), DVB-S (для спутникового вещания EN 300 421, TR 101 198), DVB-T (для наземного эфирного вещания EN 300 744, TR 101 190). DVB разрабатывает не только протоколы передачи, но и стандарты для интерактивных приложений, таких как приставки цифрового телевидения (set-top boxes) и т.п. Другие DVB протоколы включают MHP (multimedia home platform, сокращенно DVB-MHP: TS 101 812, TS 102 812, TS 102 819), DVB-M (стандарт измерений сигналов DVB-S/T/C; TR 101 290, TR 101 291), DVB-H («обновление» стандарта DVB-T, которое позволяет доставлять цифровой поток в мобильные устройства по наземным эфирным сетям, EN 302 304).

### 1.2.2.2 ATSC и ISDB

ATSC (The Advanced Television Systems Committee, ATSC Standard A/53C with Amendment No. 1 and Corrigendum No. 1) - организация, разрабатывающая и утверждающая стандарты для передовых телевизионных систем, в том числе и HDTV. Наиболее широко стандарты ATSC распространены в США и Канаде [7].

ISDB (Integrated Services Digital Broadcasting, ISDB-T) - стандарт цифрового телевидения, разработанный в Японии. Он интегрирует в себя различные виды цифрового

контента. Это может быть HDTV, STDV, звук, графика, текст и т.д.

#### **1.2.2.3 DAB**

Европейские фирмы в 1987 году основали консорциум Eureka-147 с целью разработки принципиально новой системы цифрового радиовещания DAB (Digital Audio Broadcasting) [8]. Участниками этого проекта являются около 50 фирм и организаций из Великобритании, Германии, Франции, Голландии, Италии, Швеции, Швейцарии, Норвегии, Финляндии, Японии, Канады, США и ряда других стран. В участники проекта от России, по представлению институтов - лидеров проекта - IRT (Германия) и ССЕТТ (Франция), был в 1995 г. принят ИРПА им. А.С.Попова.

В 1992 году на основе всемирного соглашения для DAB были выделены L- и S-диапазоны. Первые приемники, в основном для измерительных целей, были созданы в 1988 году. С 1990 года ряд членов проекта Эврика-147 приняли участие в проекте JESSI, в рамках которого была разработана первая интегральная микросхема для коммерческих DAB-приемников. Первый DAB-приемник потребительского типа был представлен на выставке в 1995 году в Берлине. Миниатюризация приемников продолжается, в настоящее время их серийным выпуском занимаются фирмы Grundig, Philips и др. В европейских странах эксплуатируется уже несколько десятков тысяч приемников.

Для решения проблемы вещания необходимо решение множества организационных проблем, в первую очередь - выделение отдельного диапазона частот. Европейский опыт показал, что использование диапазона 88-108 мГц совместно с существующими ЧМ-станциями нецелесообразно. В конце 1999 г. коллегия Минсвязи РФ наметила трехэтапную стратегию перехода на цифровое радиовещание, рассчитанную на 10-15 лет:

- 2001-2002 гг. Опытное вещание в Москве и Петербурге 6 государственных станций: «Радио России», «Маяк», «Маяк-FM», «Юность», «Орфей» и одной местной. Возможна передача пейджинговой или мультимедийной информации.
- 2002-2003 гг. Расширение опытного вещания на Московскую и Ленинградскую области, появление 6 коммерческих станций.
- 2003-2010 гг. Полный охват территории РФ, в дальнейшем - сокращение количества аналоговых УКВ станций

В качестве формата представления мультимедиа данных используется MPEG-1 или MPEG-2.

#### **1.2.2.4 DRM**

DRM (Digital Radio Mondiale) в отличие от стандарта DAB, использующего MPEG-2, в DRM применяется более современный вариант компрессии MPEG-4 [9]. Он включает адаптивный механизм компрессии аудиосигнала AAC (Advanced Audio Coding) в моно и стереовариантах, а также CELP (Code-exited Linear Prediction) для высококачественного кодирования речи и шумоподобных сигналов. В MPEG-4 долговременное предсказание проводится не во временной, а в спектральной плоскости. Кодер делает предсказание, а затем кодирует либо разницу между реальным и предсказанным сигналом, либо сам входной сигнал, если его значение можно закодировать более компактно, чем разницу. Кроме то-

го, кодер поддерживает несколько новых механизмов, связанных со способностью потока адаптироваться к изменениям параметров канала. Любой из вариантов может дополняться техникой SBR (Spectral Band Replicatoin), предназначеннной для повышения качества передачи верхних частот. При передаче на частотах ниже 30 МГц все форматы, кроме стереофонического, используют полосу 9/10 МГц. Использование техники SBR требует более широкой полосы.

Помимо аудиосигналов, в цифровом потоке могут передаваться данные. Мультиплексированный поток аудио- и данных формируют основной сервисный канал Main Service Channel (MSC). В MSC передается до 4 потоков, каждый из которых переносит или аудио или данные. Информация канала MSC разбивается на логические кадры по 400 мс каждый. Дополнительно к MSC формируются еще два дополнительных канала. Основной и сервисные каналы определенным образом мультиплексируются, в результате чего образуются транспортные суперкадры длительностью 1200 мс. Первый дополнительный канал, Fast Access Channel - FAC (канал скоростного доступа), переносит данные о параметрах радиочастотного сигнала и информацию, позволяющую выделять отдельные услуги. К параметрам сигнала относятся идентификатор потока, ширина занимаемой полосы, тип модуляции, тип кодирования, индекс глубины перемежения, количество передаваемых услуг. Эти параметры передаются в каждом FAC кадре. К параметрам, характеризующим услуги, относится указание типа сервиса (аудио/данные), флаг условного доступа, указатель языка и некоторые другие. Они передаются последовательно - в одном кадре параметры, относящиеся к одному сервису.

Второй дополнительный канал, Service Description Channel - SDC (канал описания услуг), содержит информацию, относящуюся к условному доступу, программу передач, информацию об авторских правах, вспомогательную информацию для некоторых приложений, а также ссылки на альтернативные частоты, на которых передается тот же канал. Информация SDC размещается в начале каждого суперкадра и начинается с ссылок на альтернативные частоты. Это позволяет автоматически выбрать канал, принимаемый в данный момент наилучшим образом. В DRM, как и в DAB, применяется система модуляции COFDM. Эта система весьма эффективна для передачи сигналов по радиоканалу с многолучевым распространением радиоволн и селективным замиранием сигнала, характерным для коротких волн. Для компенсации помех многолучевого распространения используется защитный интервал. Он не должен превышать 20% от общей длительности символа, чтобы не снизить пропускную способность канала. Количество несущих, размещаемых в полосе частот канала, ограничивается Доплеровским смещением частоты сигнала, возникающим в режиме мобильного приема. С учетом этих факторов в полосе 9/10 кГц используется около 200 несущих. Их точное количество, равно как и длительность символа и защитного интервала, зависит от характера распространения радиоволн (поверхностные или пространственные), предположительной дальности передачи и требуемой достоверности.

### 1.2.3 Анализ и выбор формата

С одной стороны более подходящей формой мультимедийного контента является формат MPEG-2, поскольку является де факто стандартом передачи цифрового телевидения (DVB, ATSC, ISDB) и радиовещания (DAB), для его распространения по цифровым сетям нет необходимости в создании каких либо программных или аппаратных средств по кодированию мультимедийных данных в цифровое представление (исключение – необходимость оборудования декодирования зашифрованных каналов). С другой стороны, формат MPEG-2 для передачи телевизионных передач является достаточно каналоёмким – вещание одного канала требует от 4 до 10 мегабит/с пропускной способности канала, что ограничивает применение MPEG-2 в IP сетях и требует использования дополнительных средств по перекодированию в более эффективный формат сжатия, например H.264. В случае вещания радиопрограмм с требованиями к каналу 128-192 кбит/с подходит и MPEG-2, и MPEG-1 (Layer 3).

Таким образом к свойствам представления мультимедийного контента в виде MPEG-2 можно отнести:

- + простоту и низкую стоимость оборудования получения мультимедийного контента;
- + наличие источников мультимедийного контента, использующих формат MPEG-2 для распространения контента от студии до зрителей;
- + высокое качество (практически студийное) видеоизображения и звука;
- высокая каналоемкость (4-10 мегабит/с).

Устранение недостатка MPEG-2 может быть достигнуто за счет транскодирования (декодирования и последующего кодирования) в другой формат представления. В частности может быть использован или другой профиль MPEG-2 (для уменьшения каналоемкости при снижении качества исходного видеоизображения), или более эффективный формат H.264, позволяющий при том же качестве изображения и звука получать менее каналоемкие цифровые потоки. Учитывая допускаемый уровень искажения изображения при просмотре мультимедийного контента абонентами (просмотр телевизионный каналов параллельно основной работе, в небольшом окне, редкие включения полноэкранного режима), возможно получить цифровые потоки около 1-2 Мбита/с на канал или на абонента в зависимости от применяемой технологии доставки данных. Это влечет существенные изменения требований к аппаратной или программно-аппаратной части в плане необходимости организации декодирования исходного MPEG-2 потока и кодирования его с заданными параметрами в H.264 (MPEG-4) в реальном масштабе времени. В этом смысле более простым в реализации является использование аналогового вещания, поскольку не требует процесса декодирования исходного MPEG-2 потока. Т.е. осуществляется кодирование в H.264 (MPEG4) не цифрового потока MPEG-2, а аналогового сигнала получаемого или от внешних источников (спутниковые ресиверы, видеомагнитофоны и проч.), или из внутренних источников (ТВ тюнеры, видеокамеры) и оцифровываемого в формат BT.601 с помощью специального оборудования [10].

Основным достоинством H.264 (MPEG4) является низкая каналоемкость (1-2 Мбит/с), а недостатком - высокие требования к программно-аппаратной части (дорогое оборудование, сложный комплекс программного обеспечения). В таблице 1.7 представлен анализ сравнительных характеристик вещательных форматов вещания.

Таблица 1.7 – Сравнительные характеристики форматов представления мультимедийного контента

	ТВ						Радио	
	NTSC	PAL	SECAM	DVB	ATSC	ISDB	DAB	DRM
Тип	аналог.	аналог.	аналог.	цифр.	цифр.	цифр.	цифр.	цифр.
Формат	-	-	-	MPEG2	MPEG2	MPEG2	MPEG2	MPEG4
Частота кадров	30	25	25	-	-	-	-	-
Разреш.	525 строк	625 строк	625 строк	768x576 и другое	1920x1080 и другое	1920x1080 и другое	-	-
Исп. в России	нет	да	да	да (DVB-S)	нет	нет	эксперим.	нет

Исходя из вышеперечисленного можно сделать вывод о том, что однозначного вывода о том, какой формат представления более предпочтительный нельзя. Необходимо дополнительно произвести исследования возможностей сети передачи данных, требований потенциальных абонентов.

Немаловажным шагом в реализации IP-TV вещания является исследование существующих разработок в этой области. Это позволит реализовать сервис, включающий в себя последние технологические достижения.

### 1.3 Анализ прикладного ПО для организации мультимедийного вещания

Существует ряд программных решений по организации мультимедийного вещания в рамках высокоскоростной сети передачи данных, каждое из которых обладает некоторыми положительными и отрицательными моментами.

Часть решений является комплексными - производителем аппаратного обеспечения разработан комплекс программного обеспечения как для организации вещания, так и для просмотра этого вещания (проект Cisco IP-TV). Такой комплекс не обладает гибкостью, поскольку поддерживает строго ограниченные виды источников мультимедийного контента, ограничивает методы организации защиты от несанкционированного доступа, форматы представления мультимедийного контента и прочее.

Другим решением является проект программного обеспечения VideoLAN, свободно распространяемый по лицензии GNU. Обладая заложенной в него гибкостью, он поддерживает огромное число разнообразного оборудования, при этом являясь проектом с открытым кодом, что дает возможность его доработки для различных специализированных применений.

Также заслуживает рассмотрения решения компании Microsoft для реализации мультимедийного вещания в рамках высокоскоростной сети передачи данных.

В таблице 1.8 приведены сравнительные характеристики организации мультимедийного вещания с использованием различных решений

Таблица 1.8 – Сравнительные характеристики организации мультимедийного вещания

Решение	Особенности	Стоимость реализации
Cisco IP-TV	Закрытый коммерческий продукт на базе аппаратных решений Cisco. Получение мультимедийного контента осуществляется только с использованием оборудования Cisco, а прием на стороне клиента с помощью разработанного компанией Cisco программного обеспечения.	Cisco IP/TV 3425 Broadcast Server 10000\$
Microsoft Media Encoder	Закрытый коммерческий программный продукт организации мультимедийного вещания на базе Windows платформы. Получение мультимедийного контента осуществляется только с помощью специализированного или стандартного оборудования, поддерживающего стандартные интерфейсные функции	Сервер вещания - бесплатный при условии покупки ОС Windows XP/2003 server Оборудование приема - от 100\$ на канал
VideoLAN	Открытый программный продукт организации мультимедийного вещания платформах Linux, Windows, MacOS X, Unix и других. Поддержка оборудования приема мультимедийного контента со стандартными интерфейсными функциями и ряда специфического оборудования с собственным API	ПО - бесплатное (лицензия GNU). Оборудование приема - от 100\$ на канал

Произведем более детальное рассмотрение программных решений.

### 1.3.1 Проект VideoLAN

Проект был начат французскими студентами École Centrale Paris, в дальнейшем к нему подключились заинтересованные лица со всего земного шара [11]. Проект нацелен на создание программного обеспечения для потокового вещания в рамках высокоскоростных сетей передачи данных в стандартах MPEG-1, MPEG-2, MPEG-4, вещания спутниковых телевизионных каналов, эфирных и кабельных аналоговых телевизионных каналов, работающего под различными операционными системами. В данный момент программное обеспечение портировано на все популярные операционные системы.

Изначально проект VideoLAN был разделен на две взаимодополняющие друг друга части - VLS (VideoLAN Server - сервер) и VLC (VideoLAN Client - клиент), однако впоследствии клиент VLC приобрел всю функциональность серверной части и даже больше. Таким образом на данный момент можно считать что существует клиентская часть с возможностями сервера вещания, а некоторые специализированные задачи (такие как транс-

ляция спутниковых ТВ каналов) могут осуществляться с помощью сервера VLS.

Общая структура использования программного обеспечения проекта VideoLAN показана на рис.1.6.

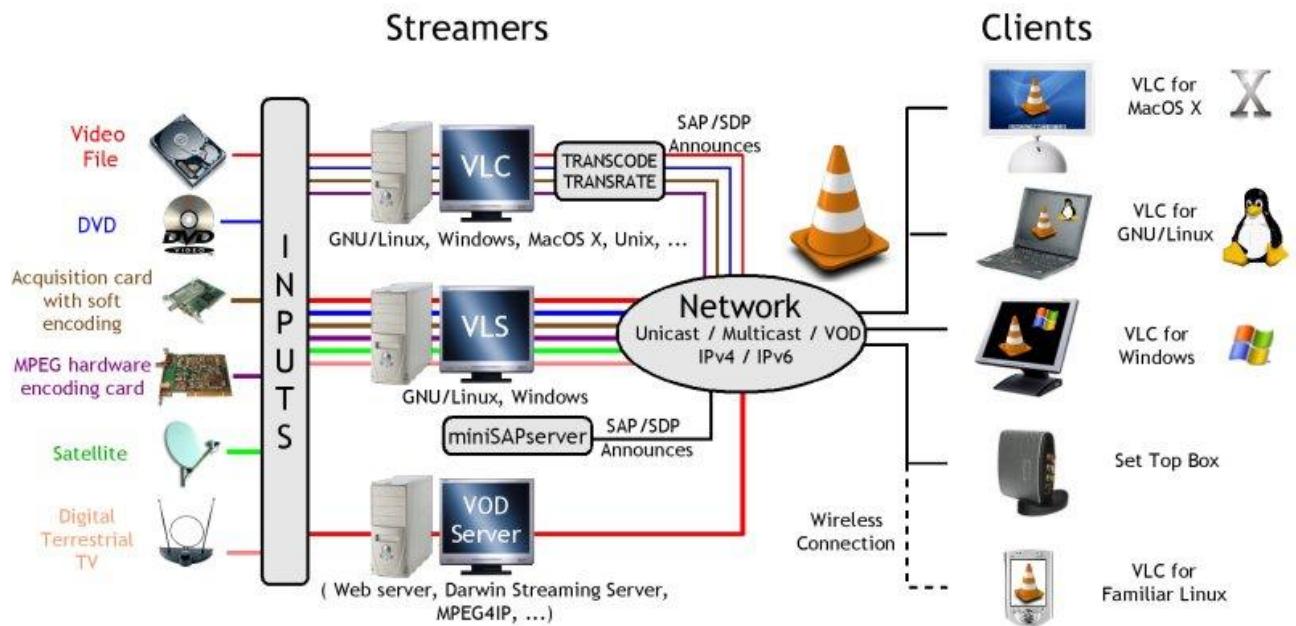


Рисунок 1.6 – Структура мультимедийного вещания с помощью проекта VideoLAN

Представленная структура полностью соответствует концепции построения комплекса мультимедийного вещания.

Однако нельзя не отметить существенные недостатки самого проекта VideoLAN. К таким необходимо отнести некоторую разнородность серверных частей. Для построения единого комплекса программно-аппаратного обеспечения с помощью проекта VideoLAN необходима дополнительная доработка программного обеспечения, разработка различных систем мониторинга и управления внутренними объектами системы.

### 1.3.2 Решения Microsoft

В качестве решения от компании Microsoft можно привести продукт Microsoft Media Encoder 9 Series. Структура мультимедийного вещания с использованием продуктов Microsoft представлена на рис.1.7.

Достоинством данного программного обеспечения является то, что оно разработано компанией Microsoft, поэтому автоматически отпадают вопросы совместимости с собственно операционной системой Windows, а также плеером Windows Media Player для отображения получаемых трансляций. Другим немаловажным является тот факт, что реализованы все необходимые методы доставки контента от сервера до клиента: multicast режим, режим unicast по протоколу UDP, а также режим unicast по протоколу TCP/HTTP.

Главным недостатком является малая гибкость, сложность реализации удаленного управления системой, возможность работы только со стандартным оборудованием, невоз-



Рисунок 1.7 – Структура мультимедийного вещания с помощью продуктов Microsoft

можность внесения внутренних изменений в код программы, что практически препятствует применению данного решения для реализации комплекса мультимедийного вещания.

В качестве итога, можно отметить, что ни одно из рассмотренных решений не реализует защиту от несанкционированного доступа к мультимедийным услугам на чисто программном уровне, а значит преодоление соответствующего противоречия между доступностью услуги для легальных пользователей, недоступностью для остальных и стоимостью аппаратного обеспечения для реализации защиты будет достаточно однобоким.

Качество изображения мультимедийного вещания в продукте компании Microsoft задается оператором, что дает пути решения соответствующего противоречия, в то время как в проекте VideoLAN качество изображения определяется либо приемным оборудованием (аппаратное MPEG-2 кодирование), либо самим контент провайдером (цифровые спутниковые каналы).

Таким образом встает необходимость в создании программного продукта, с помощью которого возможно оптимальное решение поставленных в п.1.1.2 противоречий: оптимальное качество изображения мультимедийного вещания, оптимальное количество подключенных пользователей и оптимальный уровень защиты от несанкционированного доступа к мультимедийным услугам.

### 1.3.3 Формулирование требований к распределенной системе мультимедийного вещания

Разрабатываемая система должна быть гибкой для возможности подключения различного оборудования, обслуживающего разные типы источников мультимедийного контента, включать возможности использования различных схем распространения данных от сервера к абонентам (в т.ч. смешанных). Для удовлетворения этих требований

структура системы должна представлять собой комплекс взаимодействующих подсистем (контроля, управления, формирования контента, сетевая и абонентская подсистемы), которые в свою очередь разбиваются на компоненты и модули.

В качестве ограничительных элементов разработки системы мультимедийного вещания выступали:

- ограничения, накладываемые возможностями локальных вычислительных сетей (пропускная способность 100 или 1000 Мбит/с, с и без поддержки IGMP протоколов);
- ограничения, связанные с источниками мультимедийного контента;
- необходимость защиты от доступа к системе с рабочих станций не авторизованных в локальной вычислительной сети (в том числе подключенных через прокси или NAT);
- финансовые ограничения.

## Выводы

В разделе классифицированы услуги, которые потенциально могут предоставляться в сетях передачи данных: доступ к Интернет-ресурсам, доступ к внутренним ресурсам сети, IP-телефония, IP-телевидение и IP-радио. Выделен один из экономически перспективных и активно развивающихся видов услуг - мультимедийное вещание (IP-телевидение + IP-радио). Определены и классифицированы возможные источники мультимедийного контента: файлы мультимедиа, эфирное телевидение, эфирное радио, кабельное телевидение, спутниковое цифровое телевидение и радио, а также различного рода локальные источники мультимедийных данных. Данна сравнительная оценка источников по различным критериям, которая показала, что не существует какого либо приоритетного источника контента и к вопросу выбора надо подходить комплексно, учитывая и потребности потенциальных абонентов и возможности оператора сети передачи данных.

Также рассмотрены технологии доставки информации, в частности мультимедийной информации, от сервера до абонента: unicast, multicast, сети MBONE. Классифицированы и проанализированы различные решения для представления и передачи мультимедийных данных (аналоговых и цифровых), определены слабые и сильные стороны этих решений. Перспективной формой представления мультимедийных данных оказалася MPEG-2, на котором базируются стандарты цифрового телевидения и радио (DVB, ATSC, ISDB, DAB), однако же высокие требования к пропускной способности сети передачи данных (4-10 Мегабит/с на один ТВ канал) серьезно ограничивает применение этого формата в рамках мультимедийного вещания. Решение проблем, связанных с требованиями к пропускной способности, лежит в применении H.264 (MPEG-4), однако затраты на аппаратные и программные ресурсы могут вынудить отказаться от него и вернуться либо к исходному MPEG-2, либо перекодированному с увеличенной степенью сжатия MPEG-2.

Выделены противоречия между различными желаниями, возможностями и требованиями при реализации мультимедийного вещания в рамках сетей передачи данных: уменьшение каналоемкости канала и улучшения его качества; увеличение количества одновременно подключенных абонентов и не изменение структуры сети; организация надежной системы защиты от несанкционированного доступа при минимальных затратах на аппаратное и программное обеспечение.

Решение о применении той или иной технологии должно приниматься только после анализа существующей сети, возможностей модернизации, а также на основе количества и требований потенциального круга абонентов.

Проанализирован ряд программных решений, которые хотя и являются достаточно универсальными, но не поддерживают весь спектр потенциально используемого оборудования, а также не содержащее средств по защите от несанкционированного использования.

## **2 ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКОГО АППАРАТА ПРЕДСТАВЛЕНИЯ ВИДЕОДАННЫХ В КОМПАКТНОМ ВИДЕ ДЛЯ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ**

В данном разделе осуществляется анализ общих концепций представления видео последовательностей в цифровом виде. Поскольку оцифрованные видео последовательности представляют собой большие объемы данных, непригодные для хранения и передачи (порядка 200 Мибит на 1 секунду видео стандартного телевизионного качества), то необходимы способы существенного сжатия (соотношение более 1:50) видео данных. В рамках подраздела концепции сжатия видео осуществляются исследования способов реализации такого существенного сжатия, используя механизмы, учитывающие свойства высокой коррелированности как последовательных кадров, так и коррелированность внутри одного кадра видео. Лидером в области сжатия естественного видео в настоящее время является стандарт H.264, внутренняя архитектура которого также является частью исследований в рамках данного раздела.

### **2.1 Концепция цифрового видео**

Цифровое видео есть представление некоторой визуальной сцены, дискретизированной по времени и в пространстве. В каждый конкретный момент времени происходит формирование кадра или поля (в случае раздельной оцифровки нечётный и чётных строк). Формирование кадра осуществляется через константные интервалы времени (обычно через каждые  $1/25$  или  $1/30$  секунды), формируя тем самым видеопоследовательность. Для представления цветных изображений используется три набора отсчётов (компонентов). Известные форматы представления видеосигнала в цифровом виде включают ITU-R BT.601 [13] и ряд т.н. «промежуточных форматов».

#### **2.1.1 Цветовые модели**

Как уже было отмечено, для представления цветных изображений необходимо использовать три компонента цветности. Эти компоненты цветности являются базисными и их линейная комбинация представляет все возможные цвета заданной глубины. Разработан ряд цветовых моделей, использующих различные компоненты цветности: RGB, CMYK, YCbCr и другие. При совпадении глубины цвета (битовой ёмкости на каждую компоненту цветности), возможна конвертация из одной цветовой модели и обратно без потери точности воспроизведения цвета.

##### **2.1.1.1 CMYK**

CMYK представляет собой субтрактивную схему формирования цвета, используемую прежде всего в полиграфии для стандартной триадной печати. Схема CMYK, как правило, обладает сравнительно небольшим цветовым охватом. Каждое из чисел в цветовой модели CMYK представляет собой процент краски голубого, пурпурного, жёлтого и

чёрного цвета, составляющей цветовую комбинацию, а точнее, размер точки растра, выводимом на фотонаборном аппарате на плёнке данного цвета. Например, для получения тёмно-оранжевого цвета следует смешать 30% голубой краски, 45% пурпурной краски, 80% жёлтой краски и 5% чёрной краски. Это можно обозначить следующим образом: (30,45,80,5). Иногда пользуются таким обозначением: C30M45Y80K5.

### 2.1.1.2 RGB

Компонентами цветности в RGB являются три основных цвета - красный, зелёный и синий. RGB является аддитивной цветовой моделью, описывающей способ синтеза цвета, путём добавления к чёрному, т.е. компоненты цветности отражают интенсивность соответствующего компонента цвета. Цвет (0,0,0) соответствует цвету с нулевой интенсивностью всех компонент - чёрному, цвет (255,255,255), при 8-битных компонентах, - белому.

### 2.1.1.3 YCbCk

Во времена создания цветного телевидения, для обратной совместимости с чёрно-белым приёмным оборудованием, была разработана цветовая модель YCbCk, первая компонента которой соответствует яркости точки, а две другие - цветоразностные составляющие этой же точки. Кроме того, человеческое восприятие гораздо более чувствительно к яркости, нежели к цветостным составляющим, что позволило на основе YCbCk модели создать эффективные представления цветных изображений, в которых каждым четырём точкам изображения соответствует четыре точки яркостной компоненты и, от 1 до 4 точек (в зависимости от выбранного представления) каждой цветоразностной компоненты. Такие представления имеют обозначения 4:2:0, 4:2:2 и 4:4:4. На рис.2.1 показано распределение компонент цветности в этих представлениях.

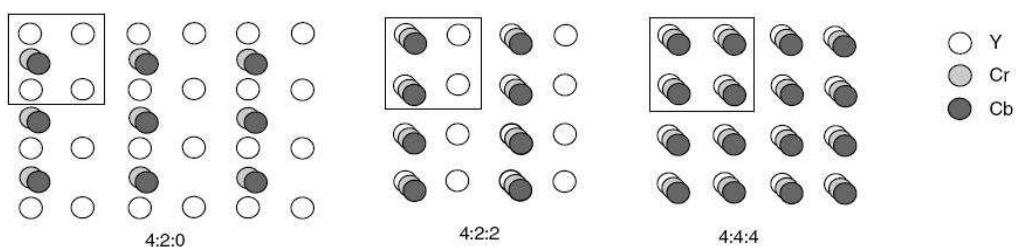


Рисунок 2.1 – Распределение компонент цветности в 4:2:0, 4:2:2 и 4:4:4 представлении YCbCk

Для конвертации между RGB и YCbCk цветовой моделью применяются следующие формулы:

$$Y = k_r R + (1 - k_b - k_r)G + k_b B$$

$$Cb = \frac{0.5}{1 - k_b} (B - Y)$$

$$Cr = \frac{0.5}{1 - k_r} (R - Y)$$

$$R = Y + \frac{1 - k_r}{0.5} Cr$$

$$G = Y - \frac{2k_b(1 - k_b)}{1 - k_b - k_r} Cb - \frac{2k_r(1 - k_r)}{1 - k_b - k_r} Cr$$

$$B = Y + \frac{1 - k_b}{0.5} Cb$$

По рекомендации ITU-R BT.601 [13] определены значения  $k_b = 0.114$  и  $k_r = 0.299$ . При подстановке этих значений получаются следующие формулы преобразования:

$$Y = 0.299R + 0.587G + 0.114B$$

$$Cb = 0.564(B - Y)$$

$$Cr = 0.713(R - Y)$$

$$R = Y + 1.402Cr$$

$$G = Y - 0.344Cb - 0.714Cr$$

$$B = Y + 1.772Cb$$

### 2.1.2 Качество изображения

Одним из важнейших элементов для оценки качества видеокодеков является оценка качества изображения [12]. Процесс этот является достаточно сложным, поскольку существует ряд особенностей восприятия изображения человеком. *Субъективная* оценка качества изображения складывается из различных факторов, затрудняющих получение точной оценки качества изображения (например имеется большая разница восприятия при пассивном просмотре фильма и распознавании образов на записи с камеры видеонаблюдения). С другой стороны *объективная* оценка даёт точные, повторяющиеся результаты, однако пока не разработано объективной системы оценок, которая полностью отражает субъективное восприятие изображения человеком.

#### 2.1.2.1 Субъективная оценка качества

Восприятие человеком визуальной сцены является результатом взаимодействия таких компонентов как «визуальная система человека», глаза и мозг. Восприятие качества складывается из пространственной и временной чёткости. Кроме того, на восприятие оказывает влияние обстановка, в которой осуществляется просмотр визуальной сцены, состояние наблюдателя, отношение наблюдателя к просматриваемой видеопоследовательности и другие факторы.

Существует ряд процедур для субъективной оценки качества, определённых в рекомендации ITU-R BT.500-11 [14]. Одной из часто используемых процедур является метод непрерывной шкалы качества с двойным стимулом (Double Stimulus Continuous Quality Scale, DSCQS), в рамках которой наблюдателю предлагается два изображения или короткие видеопоследовательности А и Б и просят дать оценку качества А и Б, путём пометки

на линии с пятью интервалами от «Отлично» до «Плохо». Обычно в ходе процедуры оценки наблюдателю предлагается набор различных последовательностей для индивидуальной оценки каждой из них. Одна из последовательностей, представленных для оценки, является исходной, другая - обработанной, причём в ходе процедуры оценки исходная и обработанная последовательности случайным образом меняются, чтобы исключить возможность предубеждённой оценки обработанной последовательности по сравнению с оригиналом.

### 2.1.2.2 Объективная оценка качества

Сложность и высокая стоимость субъективной оценки приводят к необходимости создания оценки с использованием некоторого алгоритма. Самой распространённой системой объективной оценки качества видеоизображений является расчет отношения сигнал-шум (Peak Signal to Noise Ratio, PSNR) [12]. Она не является идеальной оценкой качества, что послужило поводом создания гораздо более сложных мер оценки качества, дающих результаты приближенные к субъективным оценкам.

Отношение сигнал-шум (2.1) рассчитывается по логарифмической шкале и зависит от средней квадратической ошибки (MSE) между оригинальным и обработанным изображением относительно  $(2^n - 1)^2$  (квадрат максимально возможного значения сигнала на изображении,  $n$  - число бит на каждый отсчёт изображения). Чем больше PSNR, тем качественнее считается изображение.

$$PSNR_{dB} = 10 \log_{10} \frac{(2^n - 1)^2}{MSE} \quad (2.1)$$

Широкое распространение PSNR получило благодаря лёгкому вычислению. Однако в некоторых случаях этот метод оценки может давать результаты противоречащие субъективной оценке. На рис.2.2 представлены 3 изображения: оригинал (а), ухудшенная версия с PSNR, равным 30.6 dB (б), ухудшенная версия с PSNR, равным 28.3 dB. А на рис.2.3 представлен кадр с меньшим значением PSNR, однако по субъективной оценке этот кадр заметно выигрывает у кадров б) и в) рис.2.2.



Рисунок 2.2 – Примеры расчета PSNR: а) исходный кадр, б)  $PSNR = 30.6 \text{ dB}$ , в)  $PSNR = 28.3 \text{ dB}$

Таким образом, полностью полагаться только на PSNR при оценке качества видеопоследовательностей (в частности качества видеокодеков) нельзя.



Рисунок 2.3 – Кадр с  $PSNR = 27.7 \text{ dB}$  (размыт фон)

## 2.2 Концепция сжатия видео

Сжатие данных является процессом представления данных меньшим числом бит. Несжатый поток видеоданных предъявляет очень высокие требования к пропускной способности каналов и оборудования, а также к месту для хранения, поскольку одна секунда несжатого видео телевизионного качества занимает около 216 Мибит. По этой причине, сжатие видеопотока является необходимым элементом для хранения и передачи видео.

Сжатие включает в себя две комплиментарные системы: компрессор (кодировщик) и декомпрессор (декодер). Пару кодировщика и декодера называют *КОДЕКОМ*.

Компрессия данных достигается за счёт избавления от избыточности. Ряд типов данных включает *статистическую* избыточность и эффективно сжимается с помощью *сжатия без потерь*. Для видео такой тип сжатия даёт довольно скромный коэффициент сжатия – около 3-4. Поэтому применяется *сжатие с потерями*, в котором декодированное видео не совпадает с исходным в смысле байт-кода, но идентично или приемлемо в смысле человеческого восприятия. Такой подход позволяет достичь серьёзных коэффициентов сжатия.

Подход сжатия с потерями можно применить для избавления от пространственной и временной избыточности видео. В группе последовательных кадров (временном домене) обычно присутствует высокая корреляция между соседними кадрами. В пространственном домене высокая присутствует высокая корреляция между соседними отсчётами кадра.

В наиболее эффективных современных стандартах сжатия видео таких как ITU-R H.264 (MPEG-4/Part 10 AVC) и MPEG-4/Part 2 Video [12] применяется гибридная модель кодека, в которой происходит избавление как от временной, так и от пространственной и энтропийной избыточности. Структурная схема кодировщика видео с гибридной пространственно-временной моделью избавления от избыточности показана на рис.2.4.

### 2.2.1 Временная модель

Одним из примеров временной модели избавления от избыточности является механизм компенсации движения, в котором передаче или сохранению подвергается только

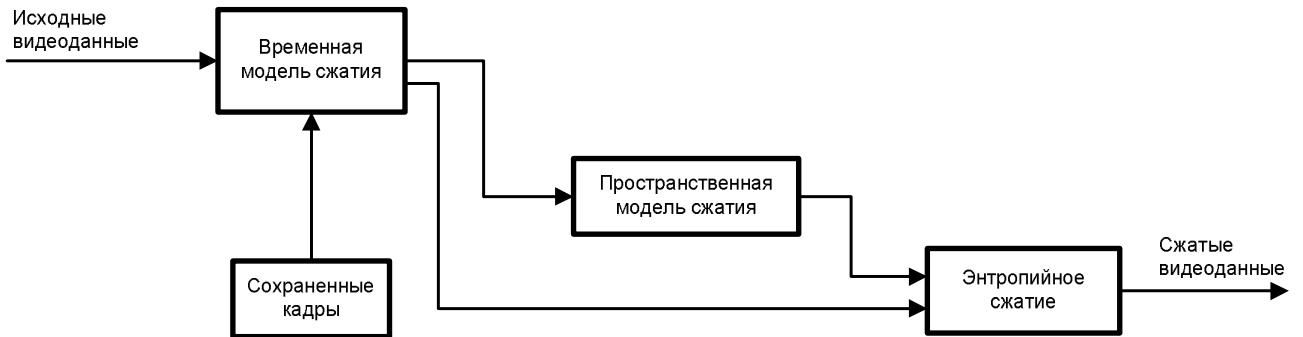


Рисунок 2.4 – Структурная схема кодировщика видео

ко изменившаяся часть изображения. Этот процесс разбивается на этапы поиска схожих компонентов на предыдущих кадрах и вычитание из текущего наиболее подходящего компонента. В этом случае энергия кадра-разности является меньшей, что позволяет закодировать его меньшим числом бит по сравнению с исходным кадром.

В стандарте сжатия ITU-R H.264 [16] применяется компенсация движения прямоугольных областей (от 4x4 до 16x16 пикселей). Поскольку на двух соседних кадрах изменения если и были, то в небольших пределах, поэтому эффективный поиск заключается в сканировании для каждого прямоугольного блока кадра соседних областей на предыдущих кадрах. Кроме того, изменение могло быть не кратным числу отсчётов, поэтому используется так называемое подпиксельное сканирование (1/2-пикельное, 1/4-пикельное, 1/8-пикельное), для чего может осуществляться интерполяция сканируемой области.

### 2.2.2 Пространственная модель

Одной из компонент пространственной модели является предсказательное кодирование изображения. Данный процесс практически полностью аналогичен компенсации движения, за исключением того, что в качестве области сканирования выступают не предыдущие или последующие кадры, а закодированные (или декодированные, если рассматривать процесс декодирования) компоненты самого изображения. Кроме того, практически не имеет смысла подпиксельное сканирование, поскольку движения никакого не присутствует, мы лишь пытаемся уменьшить энергию очередной компоненты изображения. Пространственное предсказание (предсказательное кодирование) изображения часто описывают как «Differential Pulse Code Modulation» (DPCM) [12]. На рис.2.5 показана схема работы DPCM. Выделенные компоненты изображения являются кандидатами для использования в качестве основы предсказания.

Другим немаловажным компонентом пространственной модели является кодирование преобразованием, т.е. преобразовании изображения или нескомпенсированной компоненты изображения в другую область (например, частотную). Выбор типа преобразования зависит от ряда критериев [12]:

- Данные в другой области должны быть декоррелированы и компактными, т.е. практически вся энергия должна быть сконцентрирована в небольшом количе-

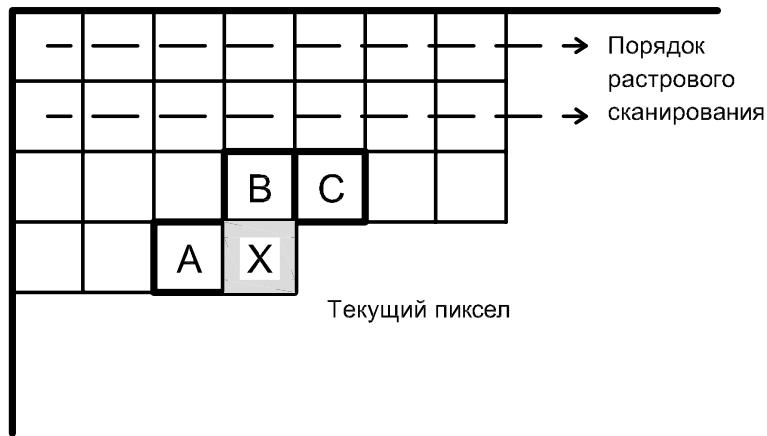


Рисунок 2.5 – Порядок работы DPCM

стве значений.

- Преобразование должно быть обратимым (ортогональным).
- Преобразование должно быть эффективно вычислимым (малое использование памяти, реализация в числах с фиксированной точкой, малое количество арифметических операций и проч.).

Существует большое количество преобразований для сжатия изображений и видео и наиболее популярные разделяются на две категории: блочные и кадровые. К первым относят преобразование Кархуэна-Лоэву (Karhunen-Loeve Transform, KLT), Singular Value Decomposition (SVD) и дискретное косинусное преобразование (Discrete Cosine Transform, DCT) [12]. Эти преобразования осуществляются над блоками размера  $N \times N$ , поэтому не требуют большого объёма оперативной памяти и подходят для сжатия остатка от скомпенсированных по движению блоков изображения. С другой стороны, преобразования на уровне блоков приводят к появлению артефактов на границах блоков — эффекта блочности. Кадровые преобразования работают с изображением в целом. Самым известным кадровым преобразованием является дискретное вейвлет-преобразование (Discrete Wavelet Transform, DWT [15]).

Из требований обратимости к преобразованию вытекает, что сжатие с использованием только преобразований является сжатием без потерь, а следовательно нельзя ожидать высокого коэффициента компрессии. Поскольку в результате преобразования большая часть энергии сконцентрирована в небольшом числе отсчётов, то применяется техника квантования, а полученный результат подвергается энтропийному сжатию (например алгоритмом Хаффмана, см.п.2.2.3.1). Выбором таблиц квантования определяется степень потерь и во многом влияет на коэффициент компрессии.

На рис.2.6 и рис.2.7 представлены соответственно 2D функция автокорреляции исходного изображения и коэффициентов ДКП этого изображения. Легко заметить, что основная энергия приходится на очень ограниченное число отсчётов.

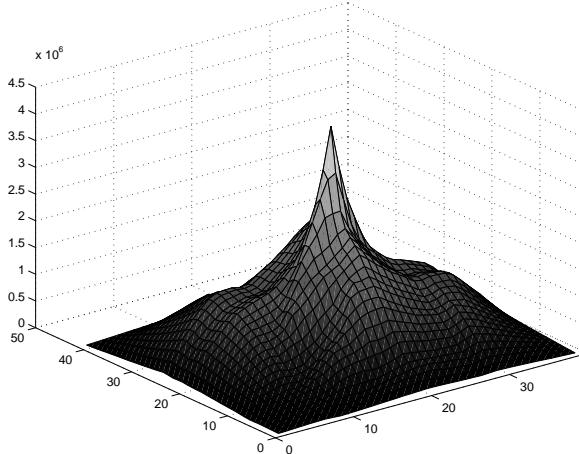


Рисунок 2.6 – Функция 2D  
автокорреляции для исходного  
изображения в пространственной области

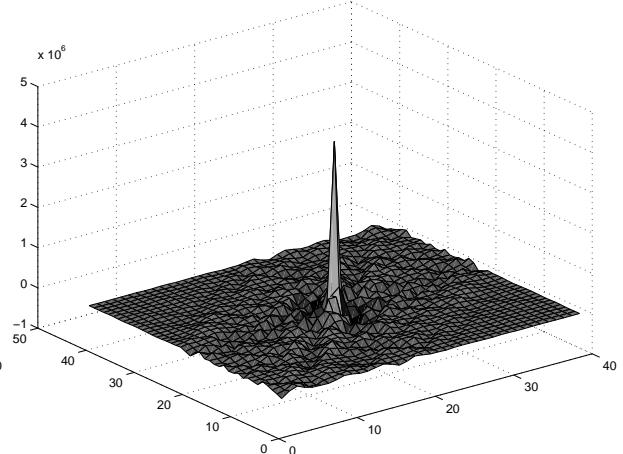


Рисунок 2.7 – Функция 2D  
автокорреляции для исходного  
изображения в частотной области

### 2.2.2.1 Дискретное косинусное преобразование

Дискретное косинусное преобразование (ДКП) осуществляется над матрицей  $\mathbf{X}$  размерности  $N \times N$  (обычно или значения отсчётов исходного изображения, или значения остатков после компенсации движения). Действие ДКП (и его обратной формы ИДКП) может быть описано в терминах матрицы преобразования  $\mathbf{A}$ . Прямое ДКП над матрицей  $\mathbf{X}$  записывается следующим образом [12]:

$$\mathbf{Y} = \mathbf{AXA}^T \quad (2.2)$$

ИДКП можно записать:

$$\mathbf{X} = \mathbf{A}^T \mathbf{YA} \quad (2.3)$$

где  $\mathbf{X}$  – исходная матрица отсчётов;

$\mathbf{Y}$  – матрица коэффициентов;

$\mathbf{A}$  – матрица преобразования размерности  $N \times N$ , элементами которой являются:

$$A_{ij} = C_i \cos \frac{(2j+1)i\pi}{2N} \quad (2.4)$$

$$\text{где } C_i = \begin{cases} \sqrt{\frac{1}{N}} & \text{если } i = 0 \\ \sqrt{\frac{2}{N}} & \text{если } i > 0 \end{cases}$$

Формулы (2.2) и (2.3) можно записать в суммарной форме:

$$Y_{xy} = C_x C_y \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} X_{ij} \cos \frac{(2j+1)y\pi}{2N} \cos \frac{(2i+1)x\pi}{2N} \quad (2.5)$$

$$X_{ij} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C_x C_y Y_{xy} \cos \frac{(2j+1)y\pi}{2N} \cos \frac{(2i+1)x\pi}{2N} \quad (2.6)$$

Результатом прямого дискретного косинусного преобразования является матрица размерности  $N \times N$  коэффициентов в области ДКП и эти коэффициенты могут рассматриваться как веса набора *базисных шаблонов*. На рис.2.8 представлены базисные шаблоны для матрицы  $4 \times 4$ .

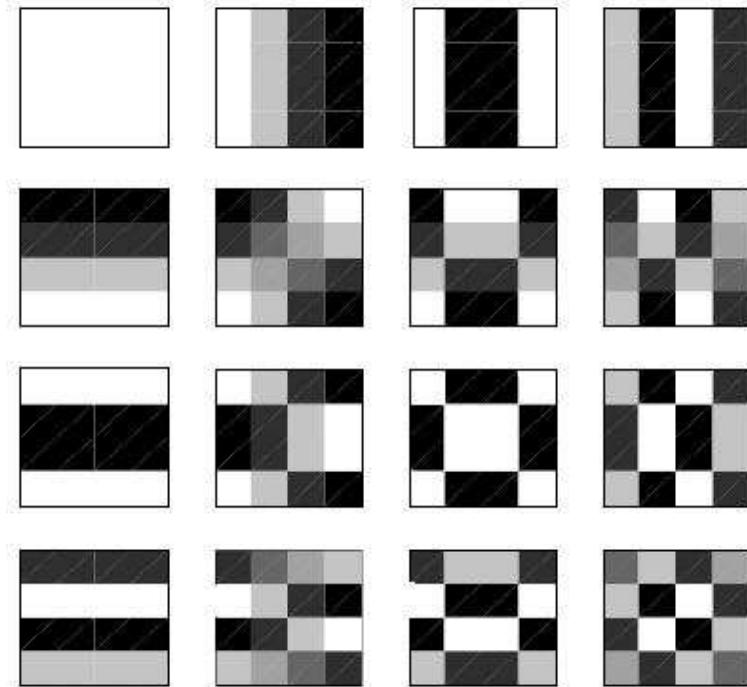


Рисунок 2.8 – Базисные шаблоны ДКП размерности  $4 \times 4$

Для блока  $4 \times 4$  исходного изображения (рис.2.9) исходные коэффициенты яркостной составляющей и коэффициенты ДКП преобразования представляют собой соответственно матрицы

$$\begin{pmatrix} 58 & 64 & 84 & 92 \\ 74 & 84 & 87 & 83 \\ 96 & 103 & 94 & 85 \\ 103 & 114 & 106 & 90 \end{pmatrix}$$

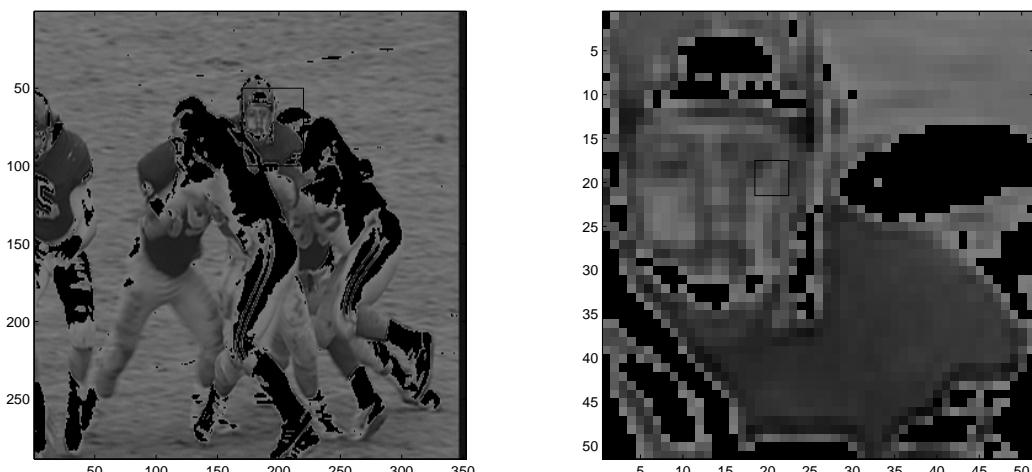
$$\text{и } \begin{pmatrix} 354.2500 & -7.0180 & -13.7500 & -0.6108 \\ -44.3286 & -29.4225 & 9.7432 & 4.2981 \\ 1.2500 & -9.9481 & 1.2500 & 2.7677 \\ 0.7726 & 0.2981 & 3.2704 & -0.0775 \end{pmatrix}$$


Рисунок 2.9 – Блок  $4 \times 4$  яркостной составляющей изображения

Если оставить в матрице коэффициентов  $1, 2, \dots, 7$  значений, то в результате инверсного ДКП получаем матрицы, представленные на рис. 2.10. Как можно легко заметить, всего 5 коэффициентами матрицы ДКП можно без заметных для глаза искажений закодировать исходный блок изображения.

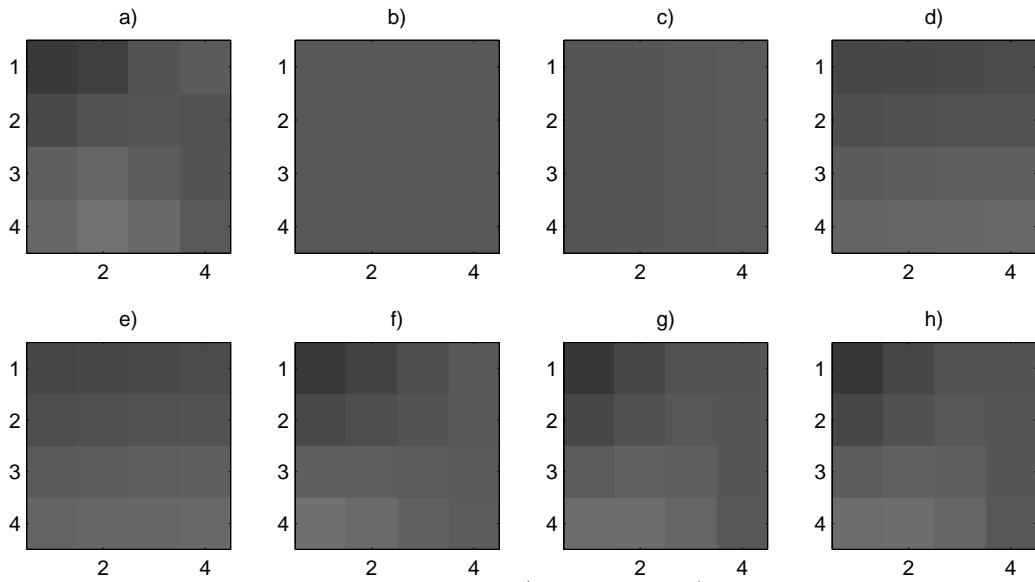


Рисунок 2.10 – Результат инверсного ДКП: а) полного; б) 1 коэффициент матрицы ДКП; в) 2 коэффициента матрицы ДКП; г) 3 коэффициента матрицы ДКП; д) 4 коэффициента матрицы ДКП; е) 5 коэффициентов матрицы ДКП; ж) 6 коэффициентов матрицы ДКП; з) 7 коэффициентов матрицы ДКП

### 2.2.2.2 Дискретное вейвлет-преобразование

Дискретное вейвлет-преобразование основано на наборе фильтров с коэффициентами, эквивалентными дискретным вейвлет-функциям [15]. В общем виде, вейвлет-преобразование сигнала из  $N$  отсчётов представляет собой разделение исходного сигнала на высокочастотную (H) и низкочастотную (L) части с помощью пары фильтров, после чего каждая часть прореживается в 2 раза. При соответствующем подборе фильтров, такая операция является обратимой.

Точно такой же подход может быть применён для двухмерного сигнала (например яркостной составляющей изображения). Каждая строка 2D изображения  $N \times N$  пикселей подвергается низкочастотной и высокочастотной фильтрации и прореживанию, формируя тем самым две матрицы  $N/2 \times N$ , которые можно обозначить L и H соответственно. Затем все столбцы матриц L и H опять подвергаются низкочастотной и высокочастотной фильтрации с прореживанием, в результате получая четыре матрицы размерности  $N/2 \times N/2$ : LL, LH, HL и HH. Эти четыре матрицы хранят в себе необходимое количество данных для полного восстановления исходного изображения.

Программное обеспечение сжатия изображения и видео последовательно несколько раз осуществляет разделение LL матрицы на подматрицы. Результат моделирования в среде Matlab двустадийного процесса вейвлет-преобразования показан на рис. 2.11. Сжатие изображение происходит за счёт того, что коэффициенты в высокочастотной области

близки к нулю (на рисунке - чёрный цвет) и после квантования могут быть отброшены.

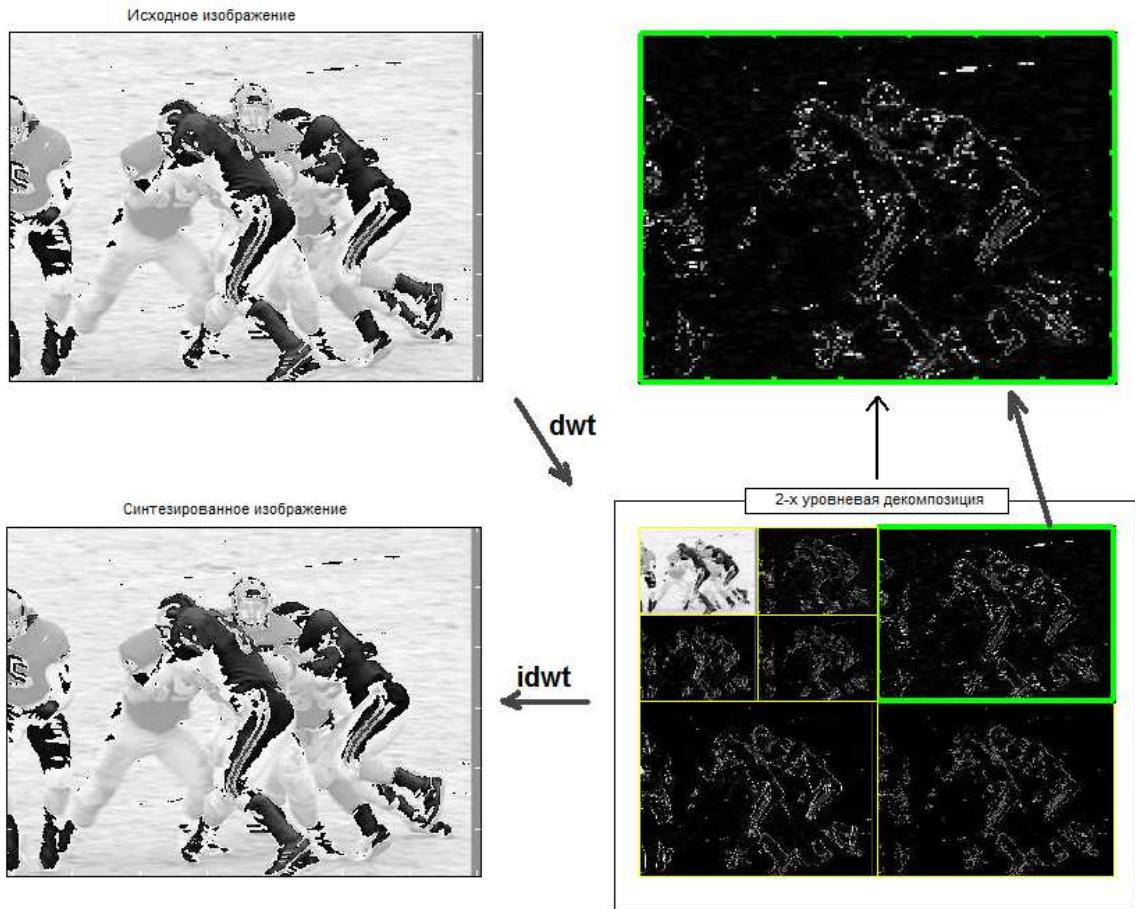


Рисунок 2.11 – Пример двумерного вейвлет-преобразования

### 2.2.2.3 Реорганизация данных

Одним из важных этапов сжатия изображений и видео является преобразование двумерного изображения (или коэффициентов трансформации) в одномерный массив данных. Здесь же, необходимо сгруппировать значащие элементы вначале массива, а нулевые - в конце. В зависимости от типа преобразования существуют эффективные методики такого преобразования.

При использовании ДКП преобразования вероятность ненулевых коэффициентов в матрице  $4 \times 4$  представлена на рис.2.12, из которого следует, что коэффициент  $(0,0)$  должен находиться в начале массива, затем следовать ближайшие к нему коэффициенты, а последним - коэффициент  $(7,7)$ . Именно такая логика заложена в зиг-заг преобразование, показанное на рис.2.13.

Для вейвлет-преобразования распределение коэффициентов показано на рис.2.14. Таким образом, первыми следуют коэффициенты низкочастотной области, затем соответствующие коэффициенты высокочастотной части, и далее вниз по «дереву».

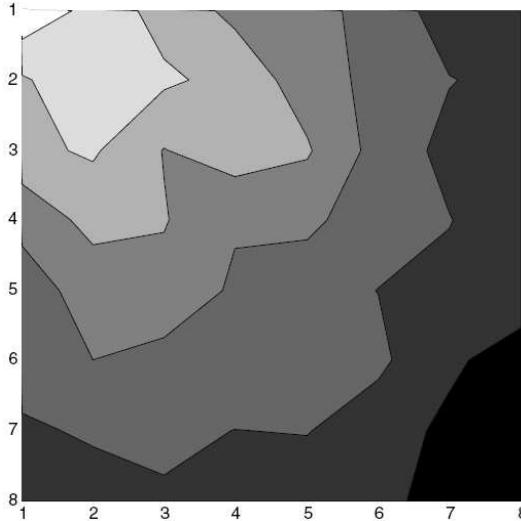


Рисунок 2.12 – Типовое распределение вероятности нахождения ненулевых коэффициентов в квантованной матрице ДКП преобразования

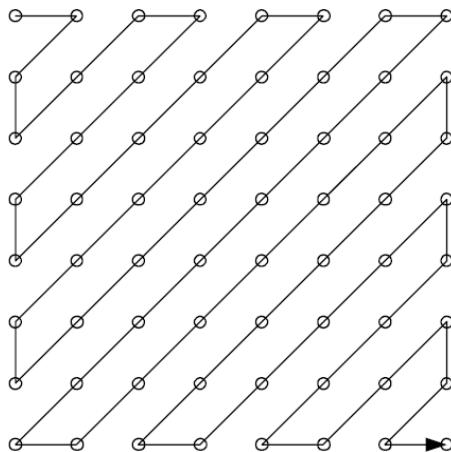


Рисунок 2.13 – Схема работы зиг-заг преобразования

### 2.2.3 Энтропийное сжатие

В процессе энтропийного сжатия происходит преобразование набора данных, представляющих собой элемент видеопоследовательности, в сжатый поток байт, пригодный для передачи или хранения. В качестве входных элементов могут выступать квантованные коэффициенты преобразований (после зиг-заг или древовидного преобразования), векторы движения, маркеры, заголовки и другая вспомогательная информация.

#### 2.2.3.1 Код переменной длины

Кодирование с помощью кода переменной длины заключается в назначении входным символам кодовых слов (кодов переменной длины). Чаще встречающиеся входные символы связываются с короткими кодовыми словами, а менее встречающиеся - с более длинными.

Самым известным кодом переменной длины является метод Хаффмана, в котором назначение длин кодовым словам основаны на вероятности появления символов в исходных данных. В случае, если вероятность была правильно просчитана, то метод Хаффмана

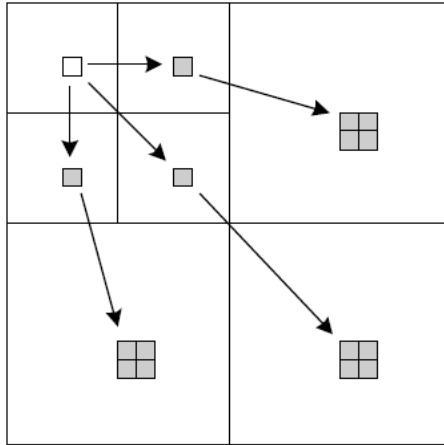


Рисунок 2.14 – Коэффициент вейвлет-преобразования и его «дети»

позволяет достаточно компактно представить исходные данные. Однако, для каждого различных исходных данных, необходимо передавать таблицу вероятности, что снижает эффективность сжатия. Кроме того, эффективность сжатия снижается из-за необходимости назначения целочисленных длин кодовых слов.

Порядок работы оригинального алгоритма Хаффмана состоит из следующих этапов:

1. Символы первичного алфавита  $m_1$  выписывают в порядке убывания вероятностей.
2. Последние  $n_0$  символов объединяют в новый символ, вероятность которого равна сумме этих символов, удаляют эти символы и вставляют новый символ в список остальных на соответствующее место (по вероятности).  $n_0$  вычисляется из системы:

$$\begin{cases} 2 \leq n_0 \leq m_2 \\ n_0 = m_1 - a(m_2 - 1) \end{cases}$$

где  $a$  — целое число;

$m_1$  и  $m_2$  — мощность первичного и вторичного алфавита соответственно.

3. Последние  $m_2$  символов снова объединяют в один и вставляют его в соответствующей позиции, предварительно удалив символы, вошедшие в объединение.
4. Предыдущий шаг повторяют до тех пор, пока сумма всех  $m_2$  символов не станет равной 1.

Этот процесс можно представить как построение дерева, корень которого — символ с вероятностью 1, получившийся при объединении символов из последнего шага, его  $m_2$  потомков — символы из предыдущего шага и т.д.

Каждые  $m_2$  элементов, стоящих на одном уровне, нумеруются от 0 до  $m_2 - 1$ . Коды получаются из путей (от первого потомка корня и до листка). При декодировании можно использовать то же самое дерево, которое считывается по одной цифре и делается шаг по дереву, пока не достигается лист — тогда выводится символ, стоящий в листе и производится возврат в корень.

Для преодоления неэффективности из-за передачи дополнительных таблиц вероятности, в MPEG применяют кодирование на основе заранее просчитанных на основании «типовых» видеопоследовательностей и опубликованных в стандарте таблиц кодовых слов.

### 2.2.3.2 Арифметическое кодирование

Арифметическое кодирование позволяет отойти от необходимости назначения кодовым словам целочисленных длин используя другой подход кодирования - представление исходного потока в виде одного действительного числа.

Принцип действия арифметического кодирования можно описать следующим образом. Пусть имеется некоторый алфавит, входные данные из символов этого алфавита и данные о вероятности появления каждого символа алфавита во входных данных.

Последовательно для каждого символа входных данных выполняются операции:

- Разметка рабочего интервала координатной прямой (в начальный момент рабочий интервал равен  $[0, 1]$ ) на интервалы таким образом, что каждый интервал соответствует одному символу входного алфавита, а длины пропорциональны вероятности появления соответствующего символа во входных данных.
- Нахождение интервала, соответствующего рассматриваемому входному символу, и назначение его рабочим.

Последним шагом является выбор любого числа из результирующего рабочего интервала, которое и будет представлять исходные данные в кодированном виде.

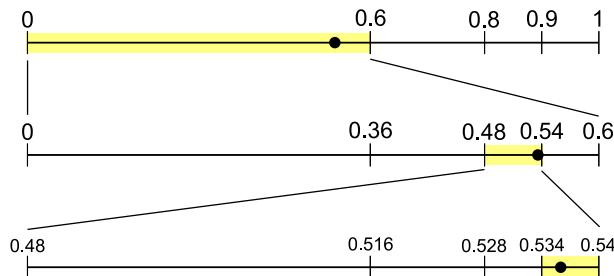


Рисунок 2.15 – Процесс декодирования данных, закодированных с помощью арифметического кодирования

Работа декодирования проиллюстрирована на рис.2.15. Входными данными декодирования является некоторый алфавит и вероятность появления каждого символа алфавита в данных, а также действительное число (на рисунке это число 0.538 на рисунке 2.15). Первые два элемента - общие для кодирования и декодирования, третий элемент - выходные данные кодирования. Порядок работы практически аналогичен процессу кодирования, за исключением того, что на каждом этапе идёт поиск нужного интервала на основе полученного действительного числа. Для окончания процесса декодирования необходимо заранее знать количество символов в закодированных данных, либо ввести в алфавит специальный символ окончания данных.

## 2.3 Кодек ITU-R H.264

Самым эффективным с точки зрения отношения качества видео к требуемому потоку данных является кодек H.264, известный также как ISO/IEC 14496 (MPEG-4) Part 10 [12]. Кодек разработан для широкого применения в различных областях:

- цифровое вещание в кабельных сетях, со спутника, в DSL сетях, эфирное цифровое вещание;
- хранение мультимедийных данных на оптических и других носителях;
- мультимедийные сервисы по запросу /

В кодеке H.264 применены следующие новые технологии:

- переменный размер блока для компенсации движения;
- точность компенсации движения до  $1/4$  пикселя;
- векторы движения за границы изображения;
- множественная ссылочность компенсации движения;
- независимость ссылочности от порядка воспроизведения;
- взвешенное предсказание;
- пространственное предсказание в интра-кодировании;
- встроенный фильтр блочности;
- контекстно-зависимое арифметическое энтропийное кодирование и контекстно-зависимый код переменной длины.

Кодек H.264, в отличие от MPEG-4 Visual, предназначен для кодирования естественных видеопоследовательностей и не включает в себя возможность многопланового кодирования. Кроме того, на данный момент отсутствует возможность масштабируемости, т.е. возможности разделения закодированного потока на базовый (минимальное качество изображения и требования к потоку данных) и дополнительных (повышение требований к потоку данных и качеству изображения).

Стандарт H.264/AVC [16] определяет следующие понятия:

Поле (часть интерлейсного видео) или фрейм кодируется с целью получения *закодированной картинки*. Закодированный фрейм обладает *номером фрейма*, который не обязательно связан с порядком декодирования, а каждое закодированное поле прогрессивного или интерлейсного видео имеет *счётчик порядка изображения*, который и определяет порядок декодирования полей. Ранее закодированные изображения (*ссылочные изображения*) могут использоваться в интер-предсказаниях других закодированных изображений. Ссылочные изображения организованы в виде одного или двух списков и называются соответственно *список 0* и *список 1*.

Закодированное изображение состоит из набора *макроблоков*, состоящих из  $16 \times 16$  отсчётов яркостной составляющей изображения и соответствующего количества отсчётов цветоразностных составляющих (по  $8 \times 8$  отсчётов в случае использования 4:2:0 YCbCr цветовой модели). В рамках изображения макроблоки организованы в *слайсы*, представляющих собой набор макроблоков в порядке растрового сканирования (не обязательно

последовательных). Слайс типа I (интра) может содержать только макроблоки типа I, слайс типа P (предсказательный) может содержать макроблоки типов I и P, слайс типа B (двунаправленное предсказание) - макроблоки типов I и B. Кроме того, стандартом определены слайсы типов SI и SP, но в рамках профиля, соответствующего вещательным применениям кодека (профиль Main) они не используются.

Макроблоки типа I предсказываются с использованием интра-предсказаний на основе ранее декодированных отсчётов в текущем слайсе. Предсказание осуществляется либо для макроблока в целом, либо для каждого  $4 \times 4$  блока яркостной и соответствующих цветоразностных составляющих.

Макроблоки типа P предсказываются, используя интер-предсказания на основе ссылочных изображений. Интер-кодированный макроблок может быть разделен на части, т.е. блоки яркостной составляющей размерностью  $16 \times 16$ ,  $16 \times 8$ ,  $8 \times 16$  или  $8 \times 8$  и соответственные блоки цветоразностных составляющих. Если выбран блок  $8 \times 8$ , то он может быть дальше разделен на части размерностью  $8 \times 8$ ,  $8 \times 4$ ,  $4 \times 8$  или  $4 \times 4$ . Каждый макроблок может быть предсказан на основе ровно одного изображения из списка 0. Если макроблок был разделен на части, то каждая часть предсказывается на основе одного и того же ссылочного изображения из списка 0.

Макроблоки типа B предсказываются с помощью интер-предсказания на основе одного ссылочного изображения из списка 0 и/или изображения из списка 1. Если макроблок был разделен на части, то каждая часть предсказывается на основе одних и тех же ссылочных изображений.

### 2.3.1 Структура

Стандарт H.264 [16] не включает явные инструкции по реализации кодировщика и декодера, а только описывает синтаксис закодированного потока и методы для его декодирования. Создание эффективного для мультимедийного вещания в сетях передачи кодека и является одной из целей настоящей работы.

Структурная схема кодировщика и декодера представлена на рис.2.16 и рис.2.17 соответственно. Улучшения по сравнению с предыдущими стандартами присутствуют внутри каждого блока.

Кодировщик включает в себя два пути движения данных: прямой (слева направо) и обратный, или поток реконструируемых данных (справа налево).

В процессе кодирования каждый входной фрейм  $F_n$  обрабатывается в единицах макроблоков. Каждый макроблок кодируется в режиме интра- или интер-, формируя для каждого блока в макроблоке данные предсказания PRED (P на схеме). В режиме интра-, данные PRED формируются на основе ранее закодированных, декодированных и реконструированных отсчётов текущего слайса ( $uF'_n$  на схемах). В режиме интер-, данные PRED формируются с помощью предсказания на основе компенсации движения одной или нескольких ссылочных изображений, выбранных из списка 0 и/или 1. На схемах, ссылочные изображения обозначены  $F'_{n-1}$ , но ссылочное изображение для каждого макроблока

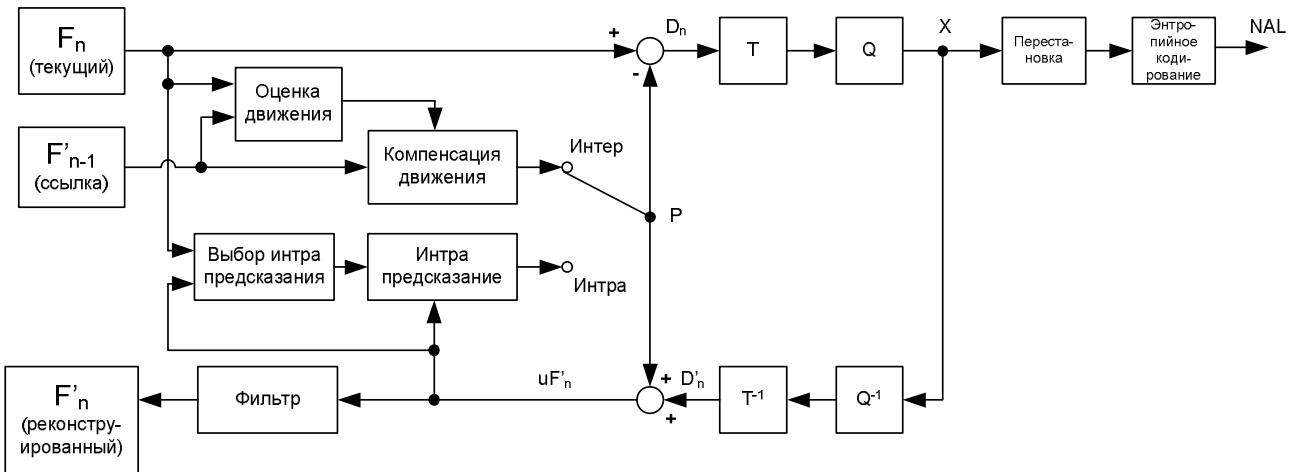


Рисунок 2.16 – Структурная схема кодировщика H.264

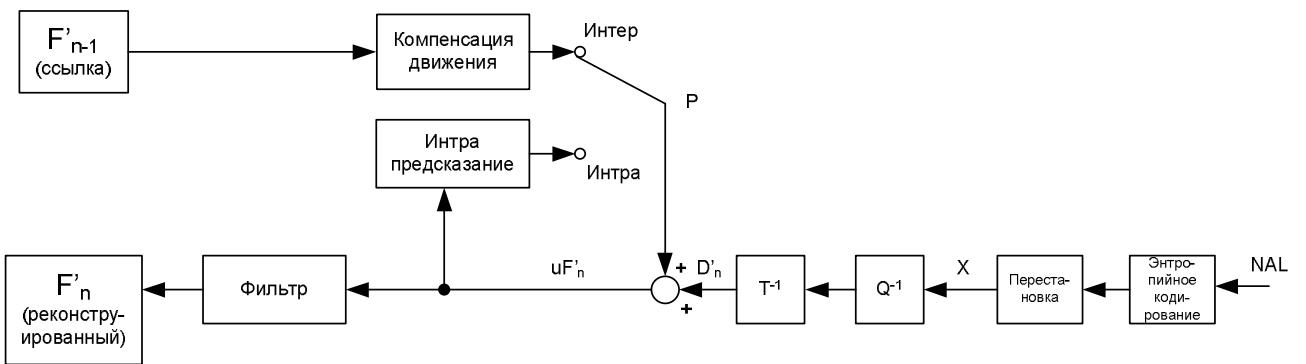


Рисунок 2.17 – Структурная схема декодера H.264

изображения может быть выбрано независимо.

Результат предсказания PRED вычитается из текущего блока, формируя остаток  $D_n$ , который затем блоками  $T$ ,  $Q$  подвергается соответственно трансформации и квантованию, формируя  $X$ . После чего  $X$  подвергается операции реорганизации данных и энтропийному кодированию. Эта и дополнительная информация, служащая для декодирования каждого блока в рамках макроблока (режим предсказания, параметры квантования, вектора движения и проч.) формирует собой сжатый поток данных в форме Network Abstraction Layer (NAL), который используется для хранения и/или передачи мультимедийных данных.

Для исключения эффекта накапливания ошибки компенсации движения из-за несовпадения исходного изображения и декодированного изображения, в кодировщик введена ветвь реконструкции изображения на основе данных  $X$ , т.е. эти данные подвергаются обратному квантованию (блок  $Q^{-1}$ ) и обратной трансформации (блок  $T^{-1}$ ), складываются с данными предсказания PRED. Для удаления эффекта блочности в ссылочных изображениях ( $F'_n$ ) используется блок фильтрации.

Декодер практически идентичен ветви реконструкции кодировщика. Исключение составляет то, что входом являются данные NAL, которые подвергаются энтропийному декодированию и обратной перестановке.

Стандарт H.264 определяет несколько профилей, поддерживающих наборы функций кодирования и определяющих необходимые элементы кодировщика и декодера: Baseline, Main, Extended, High, High 10, High 4:2:2, High 4:4:4. Профиль *Baseline* поддерживает интра- и интер-кодирование, энтропийное кодирование с помощью адаптивного к контексту кода переменной длины. Профиль *Main* включает поддержку интерлейсного видео, интер-кодирование с использованием двунаправленного предсказания (тип B), взвешенное интер-предсказание, адаптивное к контексту арифметическое кодирование. Профиль *Extended* не поддерживает интерлейсное видео и адаптивное к контексту арифметическое кодирование, но позволяет эффективное переключение между потоками данных (слайсы типов SP и SI) и имеет повышенную стойкость к ошибкам. Остальные профили предназначены для телевидения особо высокой чёткости и студийного видео. Для мультимедийного вещания, в т.ч. в сетях передачи данных предназначен профиль *Main*.

### 2.3.2 Интер-предсказание

Интер-предсказание работает на основе ранее закодированных фреймов, формируя вектора движения и остаточное изображение, которое затем подвергается трансформации и квантованию. Интер-предсказание ведётся на уровне макроблоков, которые в свою очередь могут быть поделены на субблоки. Возможные комбинации деления на субблоки  $16 \times 16$ ,  $16 \times 8$ ,  $8 \times 16$ ,  $8 \times 8$ , каждый субблок  $8 \times 8$  может быть в свою очередь разделен на субблоки  $8 \times 8$ ,  $8 \times 4$ ,  $4 \times 8$  и  $4 \times 4$  (рис.2.18). Цель такого деления - максимально эффективно использовать механизм предсказаний. В монотонных участках изображения в операции предсказания будет использоваться целый макроблок, а в участках с повышенной детализацией - минимально возможные субблоки (рис.2.19).

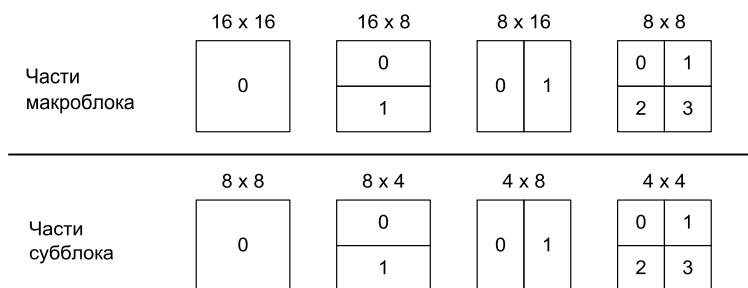


Рисунок 2.18 – Возможные комбинации разделения макроблока на субблоки

#### 2.3.2.1 Субпиксельная интерполяция

Поскольку каждый субблок в интер-кодированном макроблоке предсказывается на основании области ссылочного изображения такого же размера, то встаёт вопрос о нахождении наиболее подходящего участка. Для компенсации незначительного движения H.264 предусматривает компенсацию движения с точностью до  $1/4$  пикселя для яркостной составляющей и  $1/8$  для цветностных. Для реализации такой точности, используется техника интерполяции отсчётов в блоках ссылочного изображения.

Для яркостной составляющей вначале идёт определение полуピксельных значений с помощью фильтра с конечной импульсной характеристикой 6-го порядка с коэф-

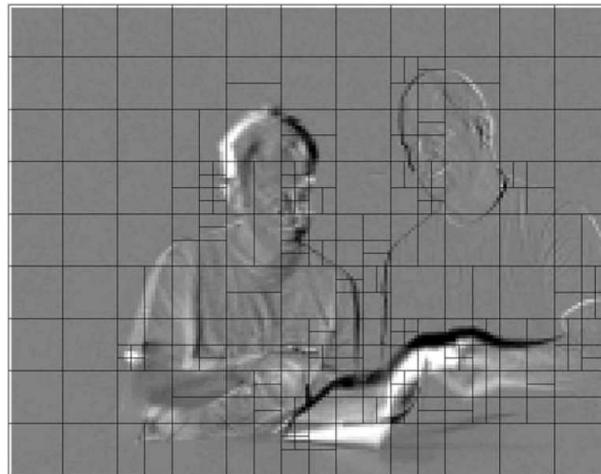


Рисунок 2.19 – Выбор размера блоков для операции предсказания движения

фициентами  $(1, -5, 5, 5, -5, 1)$  [16]. Таким образом, отсчёт  $\mathbf{b}$  (рис.2.20) будет вычислен по формуле:

$$b_1 = E - 5 * F + 20 * G + 20 * H - 5 * I + J$$

$$\mathbf{b} = \text{round}(b_1 >> 5)$$

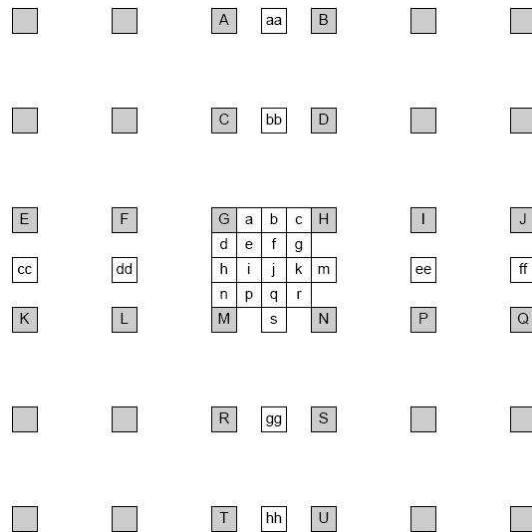


Рисунок 2.20 – Схема интерполяции яркостной составляющей макроблока

Значение  $j$  вычисляется с помощью фильтра, используя вычисленные промежуточные значения:

$$j_1 = cc - 5 * dd + 20 * h_1 + 20 * m_1 - 5 * ee + ff, \text{ либо}$$

$$j_1 = aa - 5 * bb + 20 * b_1 + 20 * s_1 - 5 * gg + hh$$

$$j = \text{round}(j_1 >> 10)$$

Отсчёты в четвертных позициях ( $a, c, d, n, f, i, k, q$ ) вычисляются нахождением среднего значения ближайших отсчётов. Например, отсчёт  $a$  вычисляется по формуле:

$$a = (G + b + 1) \gg 1$$

Для получения 1/8 пиксельной точности для цветностных составляющих (при использовании 4:2:0 цветовой модели) используется линейная интерполяция. Каждое позиционное значение  $\mathbf{a}$  (рис.2.21) вычисляется по формуле [16]:

$$\mathbf{a} = \text{round}([(8 - d_x) \cdot (8 - d_y) \cdot A + d_x \cdot (8 - d_y)B + (8 - d_x) \cdot d_yC + d_x \cdot d_yD] \gg 6)$$

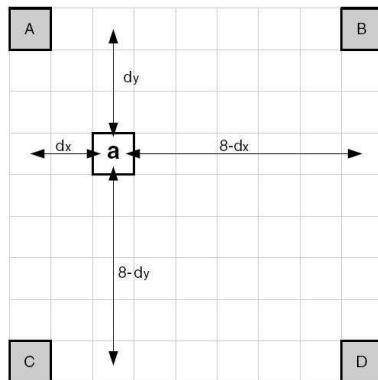


Рисунок 2.21 – Схема интерполяции цветностных составляющих макроблока

### 2.3.2.2 Предсказание векторов движения

При достаточно мелком разбиении на субблоки, может возникнуть ситуация избыточности информации в векторах движения, поскольку движение является процессом макроскопическим по отношению к блокам и субблокам. Для преодоления этого противоречия используется предсказание векторов движения на основе ранее закодированных векторов и кодирование только разницы.

### 2.3.2.3 Взвешенное предсказание

Взвешенное предсказание - это метод модификации (масштабирования) отсчётов при компенсации движения в слайсах типов Р и В. Существует три типа взвешенного предсказания, определённого в стандарте:

1. макроблок типа Р, явное взвешенное предсказание;
2. макроблок типа В, явное взвешенное предсказание;
3. макроблок типа В, неявное взвешенное предсказание.

Каждый предсказываемый отсчёт маштабируется коэффициентом  $w$  непосредственно перед операцией компенсации движения. В явных типах предсказаний, коэффициент  $w$  определяется кодировщиком и передаётся в заголовке слайса, в неявном типе предсказания коэффициенты  $w_0$  и  $w_1$  вычисляются на основе относительных позиций ссылочных изображений в списке 0 и списке 1. Чем ближе по временной шкале ссылочное изображение к кодируемому, тем больший коэффициент масштабирования используется.

### 2.3.3 Интра-предсказание

В режиме интра-предсказания данные  $P$  (см.рис.2.16) формируются на основе ранее закодированных и реконструированных блоков и вычитается из текущего блока до его трансформации и кодирования. Для яркостных отсчётов,  $P$  формируется для каждого  $4 \times 4$  блока или для  $16 \times 16$  макроблока в целом. Всего имеется девять возможных режимов предсказания  $4 \times 4$  блоков (рис.2.22) и 4 варианта для макроблоков  $16 \times 16$ . Кодировщик должен выбрать подходящий вариант кодирования по критерию минимизации разницы между  $P$  и текущим кодируемым блоком.

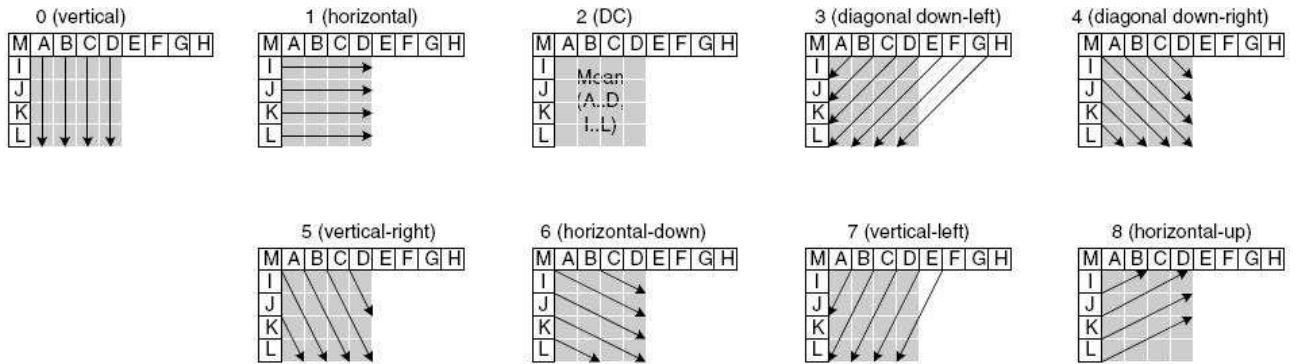


Рисунок 2.22 – Варианты интра-предсказания для блоков  $4 \times 4$

В таблицах 2.1 и 2.2 приведены описания всех режимов предсказания блоков размерности  $4 \times 4$  и  $16 \times 16$  соответственно.

Таблица 2.1 – Режимы интра-предсказаний  $4 \times 4$  блоков

Режим	Примечание
Mode 0 (Vertical)	Верхние отсчёты A, B, C, D экстраполируются вертикально
Mode 1 (Horizontal)	Левые отсчёты I, J, K, L экстраполируются горизонтально
Mode 2 (DC)	Все отсчёты экстраполируются средним значением A...D и I...L
Mode 3 (Diagonal Down-Left)	Отсчёты экстраполируются по диагонали вниз справа налево
Mode 4 (Diagonal right. Down-Right)	Отсчёты экстраполируются по диагонали вниз слева направо
Mode 5 (Vertical-Right)	Экстраполирование под углом около $26.6^\circ$ вниз слева направо
Mode 6 (Horizontal-Down)	Экстраполирование под углом около $26.6^\circ$ вниз слева направо
Mode 7 (Vertical-Left)	Экстраполирование под углом около $26.6^\circ$ вниз слева направо
Mode 8 (Horizontal-Up)	Экстраполирование под углом около $26.6^\circ$ вверх слева направо

Таблица 2.2 – Режимы интра-предсказаний  $16 \times 16$  блоков

Режим	Примечание
Mode 0 (vertical)	Экстраполяция верхних отсчётов
Mode 1 (horizontal)	Экстраполяция левых отсчётов
Mode 2 (DC)	Экстраполяция средним значением верхних и левых отсчётов
Mode 4 (Plane)	Линейная двухмерная функция экстраполяции по верхним и левым отсчётам

### 2.3.4 Фильтр блочности

Фильтрации подвергается каждый макроблок для уменьшения эффекта блочности изображения. Фильтрация осуществляется после инверсной трансформации в кодировщике (перед реконструкцией и сохранением макроблока для будущих предсказаний) и в декодере (перед реконструкцией и отображением макроблока).

Фильтрации подвергаются блоки  $4 \times 4$  на вертикальных и горизонтальных краях макроблоков (исключение - края слайсов) в следующем порядке:

1. Фильтрация 4 вертикальных границ яркостной компоненты.
2. Фильтрация 4 горизонтальных границ яркостной компоненты.
3. Фильтрация 2 вертикальных границ каждой цветоразностной компоненты.
4. Фильтрация 2 горизонтальных границ каждой цветоразностной компоненты.

Каждая операция фильтрации может изменить до трёх отсчётов на каждой стороне границы. На рис.2.23 показаны по четыре отсчёта на каждой стороне вертикальной и горизонтальной границы. Мощность фильтра (количество необходимой фильтрации) определяется текущими значениями квантования, режимов кодирования соседних блоков, а также градиентом отсчётов на границе.

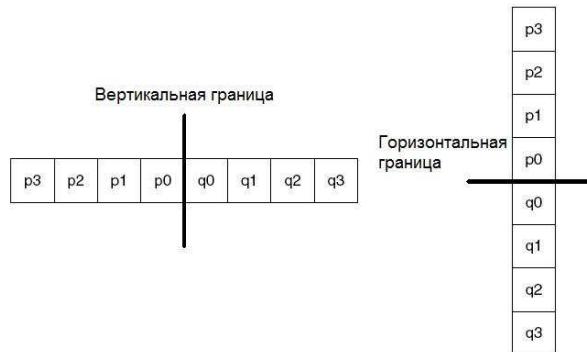


Рисунок 2.23 – Границы макроблоков, подвергающиеся фильтрации

Группа отсчётов из набора  $(p_2, p_1, p_0, q_0, q_1, q_2)$  будет отфильтрована только в случае выполнения условий:

- (a)  $BS > 0$
- (b)  $|p_0 - q_0| < \alpha$  и  $|p_1 - p_0| < \beta$  и  $|q_1 - q_0| < \beta$ .

где  $\alpha$  и  $\beta$  — значения, определённые в стандарте; они увеличиваются при увеличении среднего значения квантования блоков  $p$  и  $q$ .

### 2.3.5 Преобразование и квантование

В стандарте H.264 определены три типа преобразований: преобразование Адамара (Hadamard) для массива  $4 \times 4$  постоянных коэффициентов яркостной компоненты в интра блоках, преобразование Адамара для массива  $2 \times 2$  постоянных коэффициентов цветоразностных составляющих и основанное на ДКП преобразование всех прочих блоков данных  $4 \times 4$ . На рис.2.24 показана последовательность передачи (в сеть или на диск) блоков внутри макроблока. Если макроблок кодируется в режиме  $16 \times 16$  интра, то блок, обозначенный '-1', содержащий преобразованные DC коэффициенты каждого субблока  $4 \times 4$  яркостной составляющей, будет передан в первую очередь. Затем передаются блоки 0-15 (DC коэффициенты не передаются, если были ранее переданы в виде блока '-1'), затем передаются блоки 16 и 17 (DC коэффициенты цветоразностных составляющих), после чего блоки 18-25 (без DC коэффициентов).

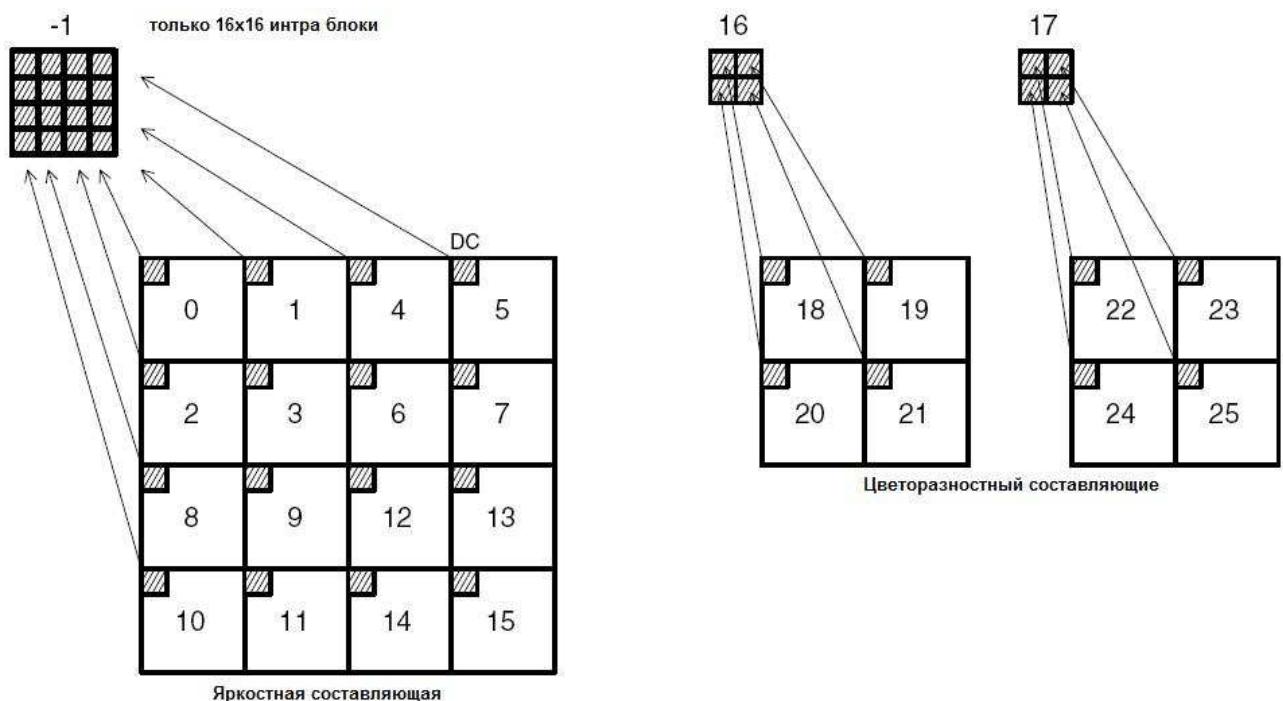


Рисунок 2.24 – Последовательность сканирования блоков внутри макроблока

#### 2.3.5.1 Преобразование блоков $4 \times 4$

Данное преобразование осуществляется над блоками 0-15 и 18-25 на рис.2.24 после интра или интер предсказаний. Преобразование H.264 [17] основано на ДКП, но имеет ряд особенностей:

1. Преобразование является целочисленным (все операции могут быть осуществлены в рамках целочисленной арифметики без потери точности).
2. Возможность обеспечить точное совпадение  $X \equiv T^{-1}(T(X))$  (за счёт целочисленной арифметики).

3. Основная часть преобразования может быть реализована с использованием только сложений и сдвигов.
4. Операция умножения в масштабировании (часть преобразования) интегрирована в квантование, уменьшая тем самым общее число умножений.

Инверсное квантование (масштабирование) и операции обратного преобразования могут быть реализованы в рамках 16-битной целочисленной арифметики с одним умножением на коэффициент без потерь точности.

Уравнение (2.2) может быть преобразовано [17] в эквивалентную форму:

$$\mathbf{Y} = (CXC^T) \otimes \mathbf{E} = \left( \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & d & -d & -1 \\ 1 & -1 & -1 & 1 \\ d & -1 & 1 & -d \end{bmatrix} \begin{bmatrix} \mathbf{X} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & d \\ 1 & d & -1 & -1 \\ 1 & -d & -1 & 1 \\ 1 & -1 & 1 & -d \end{bmatrix} \right) \otimes \begin{bmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \end{bmatrix} \quad (2.7)$$

Преобразование  $CXC^T$  является ядром 2D преобразования. Матрица  $\mathbf{E}$  коэффициентов масштабирования и символ  $\otimes$  означает, что каждый элемент  $(CXC^T)$  умножается на коэффициент масштабирования в соответствующей позиции матрицы  $\mathbf{E}$ . Коэффициенты  $a$  и  $b$  определяются формулами:

$$a = \frac{1}{2}, \quad b = \sqrt{\frac{1}{2}} \cos\left(\frac{\pi}{8}\right), \quad c = \sqrt{\frac{1}{2}} \cos\left(\frac{3\pi}{8}\right), \quad d = \frac{c}{b} \approx 0.414$$

Для упрощения реализации преобразования, принимают  $d$  равным 0.5. Для того, чтобы преобразование осталось ортогональным, коэффициент  $b$  также модифицируется, таким образом:

$$a = \frac{1}{2}, \quad b = \sqrt{\frac{2}{5}}, \quad d = \frac{1}{2}$$

2-я и 4-я строка матрицы  $C$  и 2-я и 4-я колонка матрицы  $C^T$  домножаются на 2, а матрица  $E$  модифицируется соответствующим образом для компенсации изменений. В окончательном виде прямое преобразование имеет вид:

$$\mathbf{Y} = C_f \mathbf{X} C_f^T \otimes \mathbf{E}_f = \left( \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{bmatrix} \begin{bmatrix} \mathbf{X} \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 & 1 \\ 1 & 1 & -1 & -2 \\ 1 & -1 & -1 & 2 \\ 1 & -2 & 1 & -1 \end{bmatrix} \right) \otimes \begin{bmatrix} a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \\ a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \end{bmatrix} \quad (2.8)$$

Преобразование (2.8) является приближением  $4 \times 4$  ДКП, но из-за изменения коэффициентов  $d$  и  $b$  результат преобразования не идентичен ДКП.

Обратное преобразование представляет собой [17]:

$$\mathbf{X} = C_i^T (\mathbf{Y} \otimes \mathbf{E}_i) C_i = \begin{bmatrix} 1 & 1 & 1 & \frac{1}{2} \\ 1 & \frac{1}{2} & -1 & -1 \\ 1 & -\frac{1}{2} & -1 & 1 \\ 1 & -1 & 1 & -\frac{1}{2} \end{bmatrix} \left( \begin{bmatrix} \mathbf{Y} \end{bmatrix} \otimes \begin{bmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \end{bmatrix} \right) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \frac{1}{2} & -\frac{1}{2} & -1 \\ 1 & -1 & -1 & 1 \\ \frac{1}{2} & -1 & 1 & -\frac{1}{2} \end{bmatrix} \quad (2.9)$$

В преобразовании (2.9)  $\mathbf{Y}$  заранее домножается на соответствующий коэффициент из матрицы  $\mathbf{E}_i$ . Деления на  $\pm 1/2$  в матрицах  $C$  и  $C^T$  могут быть реализованы в целочисленной арифметике операциями сдвига без существенной потери точности, поскольку коэффициенты  $\mathbf{Y}$  были заранее масштабированы.

### 2.3.5.2 Квантование

Стандарт H.264 предполагает скалярное квантование, позволяющее избежать деление и работы с арифметикой с плавающей точкой, а также включает пост- и пре-масштабирование с помощью матриц  $\mathbf{E}_f$  и  $\mathbf{E}_i$ .

Операция прямого квантования описывается уравнением [17]:

$$Z_{ij} = \text{round}(Y_{ij}/Q_{step})$$

где  $Y_{ij}$  - коэффициент трансформации,

$Q_{step}$  - шаг квантования,

$Z_{ij}$  - квантованный коэффициент.

Пост-масштабирование коэффициентами  $a^2$ ,  $ab/2$  и  $b^2/4$  встраивается в прямое квантование. Для этого блок  $\mathbf{X}$  преобразовывается в блок  $\mathbf{W}$  с немасштабированными коэффициентами ( $\mathbf{W} = C \mathbf{X} C^T$ ), после чего каждый коэффициент  $W_{ij}$  подвергается квантованию и масштабированию в единой операции:

$$Z_{ij} = \text{round} \left( W_{ij} \cdot \frac{PF}{Q_{step}} \right) \quad (2.10)$$

$PF$  – в зависимости от позиции  $(i, j)$   $a^2$ ,  $ab/2$  или  $b^2/4$ .

Обратное квантование описывается уравнением:

$$Y'_{ij} = Z_{ij} Q_{step} \quad (2.11)$$

С учетом пре-масштабирования матрицей  $\mathbf{E}_i$  уравнение (2.11) примет вид:

$$W'_{ij} = Z_{ij} Q_{step} \cdot PF \cdot 64 \quad (2.12)$$

### 2.3.6 Реорганизация данных

В кодировщике, коэффициенты преобразования каждого  $4 \times 4$  блока преобразуются в 16-ти элементный массив в порядке зиг-заг сканирования (рис.2.13). В макроблоке

закодированном в режиме интра  $16 \times 16$ , DC коэффициенты каждого  $4 \times 4$  субблока сканируются в первую очередь, формируя массив размерности  $4 \times 4$ , который преобразуется в 16-ти элементный массив зиг-заг сканированием. Оставшиеся 15 коэффициентов сканируются аналогичным образом начиная со второго элемента.

### 2.3.7 Энтропийное кодирование

В H.264 стандарте определено несколько вариантов энтропийного кодирования, определяемых режимами кодирования. В случае нулевого режима (значение `entropy_coding_mode` равно 0), данные преобразования кодируются с помощью контекстнозависимого кода переменной длины (CAVLC), а прочие данные, закодированные кодом переменной длины, кодируются с помощью экспоненциальных кодов Голомба (Exp-Golomb). В других режимах (в случае использования профиля Main) может быть использовано контекстнозависимое бинарное арифметическое кодирование (CABAC) [12].

#### 2.3.7.1 Экспоненциальное энтропийное кодирование Голомба

Экспоненциальные коды Голомба представляют собой код переменной длины, построенный следующим образом:

$$[M \text{ нулей}][1][INFO]$$

где *INFO* - информационное поле размерности  $M$ -бит.

Первое кодовое слово не имеет лидирующих нулей и поля *INFO*, кодовые слова 1 и 2 имеют однобитные *INFO*-поля, кодовые слова 3-6 – двухбитные и так далее. Длина каждого экспоненциального кода Голомба составляет  $(2M + 1)$  бит и каждое кодовое слово может быть определено из номера кода *code\_num* следующим образом:

$$\begin{aligned} M &= \text{floor}(\log_2[code\_num + 1]) \\ INFO &= code\_num + 1 - 2^M \end{aligned}$$

Декодируется кодовое слово следующим образом:

1. Считывается число  $M$  лидирующих нулей, за которыми следует 1.
2. Считывание  $M$ -битного поля *INFO*.
3. Вычисление  $code\_num = 2^M + INFO - 1$ .

#### 2.3.7.2 Контекстнозависимое кодирование переменной длины

Работа контекстнозависимого кодирования переменной длины (CAVLC) осуществляется следующим образом [12]:

1. Кодирование числа коэффициентов (TotalCoeffs) и замыкающих единиц (TrailingOne).
2. Кодируется знак каждого TrailingOne коэффициента.
3. Кодирование уровня (знак и значение) оставшихся ненулевых коэффициентов.
4. Кодирование общего числа нулей за последним коэффициентом.
5. Кодирование каждой последовательности нулей.

### 2.3.7.3 Контекстнозависимое бинарное арифметическое кодирование

Контекстнозависимое бинарное арифметическое кодирование (САВАС) достигает хорошей степени сжатия за счёт (а) выбора вероятностных моделей для каждого синтаксического элемента в соответствии с контекстом элемента, (б) адаптивных оценок вероятности на основе локальной статистики и (с) за счёт использования арифметического кодирования, а не кода переменной длины. Кодирование данных включает в себя следующие шаги:

1. Бинаризация: САВАС работает только с бинарными данными (0 или 1), поэтому небинарные данные (коэффициенты трансформации, вектора движение и проч.) должны быть приведены в бинарный вид. Этот процесс аналогичен процессу преобразования символа в код переменной длины, но этот код в дальнейшем будет арифметически закодирован.
2. Выбор модели контекста. «Модель контекста» представляет собой вероятностную модель одного или более битов бинаризированного символа. Выбор осуществляется из набора моделей на основании статистики полученной при кодировании предыдущих символов. Контекстная модель сохраняет вероятности каждого бита быть в значении '1' или '0'.
3. Арифметическое кодирование. Каждый бит кодируется с помощью соответствующей вероятностной модели (см.п.2.2.3.2), причём каждый раз имеется только два подинтервала для каждого бита (соответственно для '0' и для '1').
4. Обновление вероятности. Выбранная модель контекста обновляется на основании фактически закодированного значения (т.е. если было закодировано значение '1', то частота появления '1' увеличивается на единицу).

## Выводы

Цифровое представление видео представляет собой дискретизированный по времени и в пространстве сигнал. Дискретизация осуществляется через константные интервалы времени (обычно через каждые 1/25 или 1/30 секунды). Для представления цветных изображений используется три набора отсчётов (компонентов), тип и значения которых зависят от выбранной цветовой модели (CMYK модель - процент краски голубого, пурпурного, жёлтого цветов, RGB модель - интенсивность красного, зеленого и синего цветов, YCbCr - значения яркостной и двух цветоразностных составляющих).

Сжатие данных является процессом представления данных меньшим числом бит. Несжатый поток видеоданных предъявляет очень высокие требования к пропускной способности каналов и оборудования, а также к месту для хранения, поскольку одна секунда несжатого видео телевизионного качества занимает около 216 Мбит. Компрессия данных достигается за счёт избавления от избыточности. Ряд типов данных включает *статистическую* избыточность и эффективно сжимается с помощью *сжатия без потерь*. Для видео такой тип сжатия даёт довольно скромный коэффициент сжатия – около 3-4. Поэтому применяется *сжатие с потерями*, в котором декодированное видео не совпадает с исходным в смысле байт-кода, но идентично или приемлемо в смысле человеческого восприятия. Такой подход позволяет достичь серьёзных коэффициентов сжатия.

В современных стандартах сжатия видео применяется гибридная модель кодека, в которой происходит избавление как от временной (компенсация движения), так и от пространственной (предсказательное кодирование, дискретное косинусное преобразование, дискретное вейвлет-преобразование, квантование) и энтропийной избыточности (код переменной длины, арифметическое кодирование).

Самым эффективным с точки зрения отношения качества видео к требуемому потоку данных является кодек H.264, использующим технологии переменного размер блока для компенсации движения, повышенную точность компенсации движения (до 1/4 пикселя), реализации векторов движения за границы изображения, множественной ссылочности компенсации движения, независимости ссылочности от порядка воспроизведения, взвешенного предсказания, пространственного предсказания в интра-кодировании, встроенного фильтра блочности, контекстнозависимого арифметическое энтропийного кодирования и контекстнозависимого кода переменной длины.

Эффективность сжатия (примерно в два-три раза большая чем для MPEG-2) и возможность аппаратной и программной реализации обуславливает выбор H.264 стандарта в качестве основного варианта представления данных в рамках IP-TV вещания.

### **3 ИССЛЕДОВАНИЕ И РАЗРАБОТКА СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СИСТЕМЕ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ**

В данном разделе осуществляется исследование существующих технологий защиты данных от несанкционированного доступа в рамках мультикаст сетей и разработка новой гибридной системы защиты для использования в смешанных мультикаст-юникаст сетях, каковыми являются сети передачи данных (например Ethernet).

Зашита от несанкционированного доступа (ЗНД) к вещанию является одним из важнейших элементов любой вещательной деятельности, в том числе, важнейшим элементом мультимедийного вещания в сетях передачи данных. Цели ЗНД могут быть различными: защита авторских и смежных прав (ограничение зоны вещания), продажа услуг пользователям (т.е. защита от нелегальных пользователей). При использовании различных типов вещания, существенно различаются способы реализации ЗНД.

В случае эфирного телевидения ограничение зоны вещания осуществляется естественным образом (ограниченная зона приёма эфирного сигнала) и не требует дополнительных средств. Спутниковое телевещание, которое предназначено для максимального охвата территорий, требует уже дополнительных мер, чтобы ограничить зону просмотра той или иной телепрограммы. Эти меры включают как минимум реализации системы защиты без идентификации конкретного абонента. По такому принципу реализована система спутникового вещания пакета российских телеканалов «Триколор ТВ» [18]. Любой житель РФ может приобрести оборудование со встроенной системой защиты и без оплаты какой либо абонентской платы осуществлять просмотр телепрограмм практически в любой точке страны. Однако за пределами РФ легальный просмотр невозможен, поскольку приёмное оборудование с соответствующей системой защиты там приобрести невозможно.

Любое коммерческое вещание (эфирное, кабельное, спутниковое, в сетях передачи данных) само по себе подразумевает наличие систем защиты от неоплаченного использования услуг. На рис.3.1 представлена классификация применяемых способов защиты телевещания. Аналоговые способы защиты в настоящее время находят применение в кабельных телевизионных сетях. В спутниковом и IP-вещание используются только цифровые способы. В любом случае, для взимания платы за услугу, необходима дифференциация каждого абонента.

Существенное отличие спутникового и IP-вещания составляет в среде и типе передачи данных. Если в спутниковом вещании единственным потоком данных является односторонняя передача данных от вещателя к абоненту (за исключением систем с обратным спутниковым или модемным каналом), то в IP-вещании имеется, но пока не активно используется, высокоскоростной двунаправленный канал передачи данных. Неиспользование свойства двунаправленности ограничивает варианты использования систем вещания. На рис.3.2 показаны способы предоставления доступа абонентов к контенту и методы идентификации пользователей. Как уже отмечалось, защита несанкционирован-



Рисунок 3.1 – Классификация способов защиты телевещания от несанкционированного доступа

ного доступа может либо отсутствовать вовсе, либо основываться на группах абонентов, либо индивидуализировать каждого подключенного абонента. В случае одностороннего распространения мультимедийных данных индивидуализация абонентов (либо групп абонентов) возможна только с помощью применения специальных смарт-карт, которые представляют собой низкоскоростное вычислительное устройство, принимающее решение на стороне абонента на основе получаемых данных о возможности предоставления абоненту услуги (выдача ключа для дешифрации данных) или нет. При двунаправленной связи «Оператор-Абонент» появляются дополнительные возможности, такие как опознавание пользователей на основе логинов и паролей, индивидуальной информации специфичной для пользователя (IP, MAC адреса) и другие.

Для примера можно отметить услугу IP-вещания, предоставляемую под маркой Стим-ТВ [19], в которой используется односторонняя система защиты от несанкционированного доступа, основанная на смарт-картах. Существенным минусом такой системы является принципиальная невозможность использования услуги непосредственно с использованием ПК (необходимо приобретать специальную приставку к телевизору), что достаточно странно, учитывая факт, что услуга IP-TV является в основном дополнением к услуге доступа в Интернет.

### 3.1 Многоуровневая модель защиты данных DVB-CSA

Используемая модель разграничения доступа к вещанию в стандарте DVB (DVB-CSA, DVB-CAM, DVB-CI [20]) представлена на рис.3.3. Модель является многоуровневой моделью защиты информации: мультиплексированный транспортный поток (TS) под-

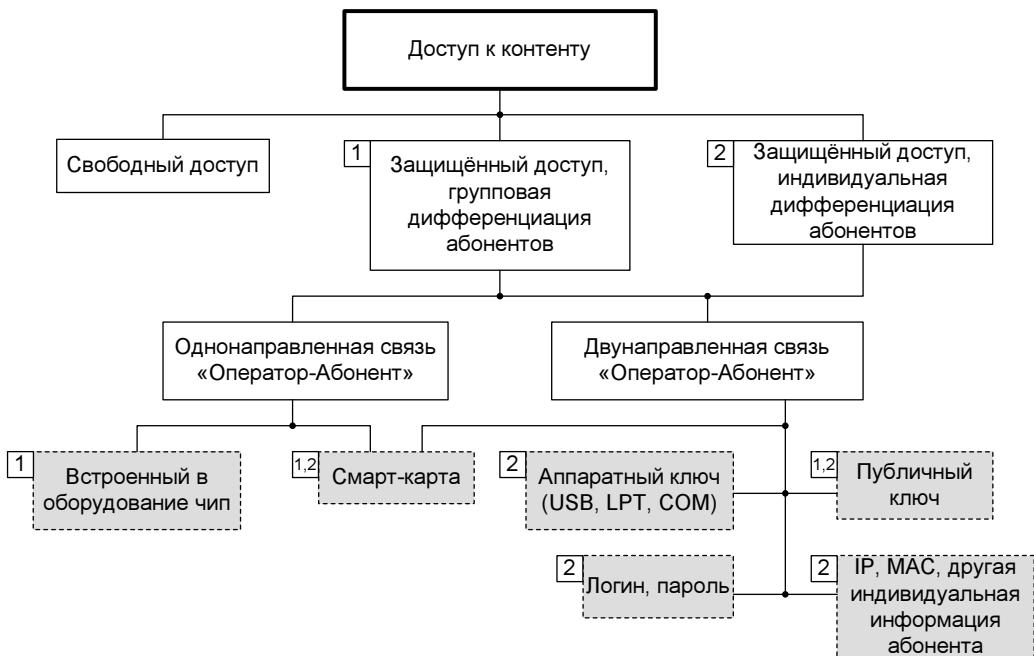


Рисунок 3.2 – Классификация методов идентификации абонентов

вергается скрамблению, т.е. симметричному шифрованию с помощью определяемого стандартом алгоритма (DVB-CSA) с помощью генерируемого кодового слова (CW). Само кодовое слово также подвергается шифрованию в рамках системы управления абонентами. Внутренняя организация и способ шифрации кодового слова полностью определяется разработчиками системы управления абонентами. В настоящее время существует множество таких систем: Viaccess, Conax, BISS, Mediaguard и многие другие. Необходимая информация для дешифрации кодового слова, а соответственно и транспортного потока в целом, передается на мультиплексор в виде сообщений ECM (Entitlement Control Message) и EMM (Entitlement Management Message). Первое сообщение содержит в себе информацию необходимую для дешифрации кодового слова, а второе информацию о правах того или иного абонента. На основании EMM сообщения смарт-карте может сообщаться информация о том, должна ли она дешифровывать кодовые слова. Скрамблированный транспортный поток (TS') доставляется соответствующим образом до абонентского оборудования, в котором происходит обратный процесс. Транспортный поток пропускается через дескрамблер, который при наличии правильного кодового слова декодирует нужные части транспортного потока, далее TS поступает на демультиплексор, из которого декодированное аудио и видео поступает на воспроизведение, а служебные сообщения ECM и EMM поступают в систему условного доступа, которая, при наличии соответствующей подписки у абонента, дешифрует кодовое слово.

Генерация новых кодовых слов осуществляется как правило с интервалом 10 секунд. Для возможности бесшлейфного воспроизведения данных, вводится понятие четных и нечетных кодовых слов. Т.е. в период действия, например, четного ключа, система управления пользователями генерирует соответствующие ECM сообщения для нечетного ключа (возможно уникальные для каждого абонента) и доставляет их. Период действия 10 се-

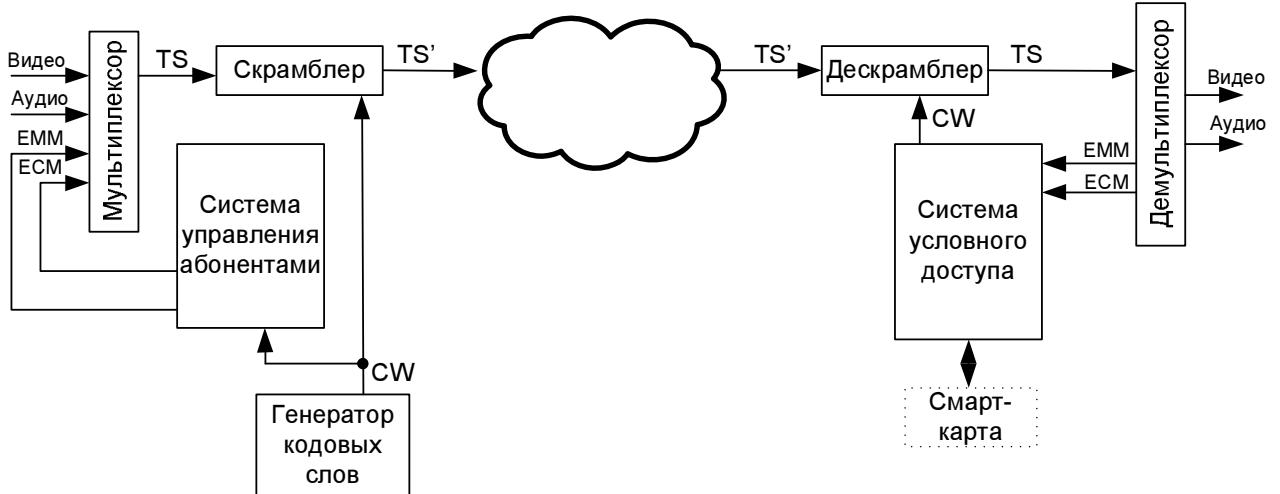


Рисунок 3.3 – Многоуровневая модель разграничения доступа стандарта DVB-CSA

кунд с запасом перекрывает необходимое время генерации и доставки сообщений. Таким образом, каждый раз при смене ключа, абонентское оборудование имеет уже подготовленный к работе новый ключ.

Огромным достоинством такой многоуровневой модели является возможность параллельной работы нескольких систем управления абонентами, либо различных версий одной и той же системы. Это не только позволяет разработчикам систем управления абонентами легко конкурировать между собой, но и относительно безболезненно для абонентов производить обновление системы (введение в эксплуатацию обновленной системы и плавная замена абонентского оборудования).

Полное перенесение технологии DVB-CSA в рамки IP сетей возможен, но сталкивается с рядом трудностей:

1. Проблема лицензирования разработки и использования скрамблера и дескрамблеров DVB-CSA [21], что зачастую является неприемлемым для малых и средних сетей.
2. Алгоритм DVB-CSA заточен на простую реализацию в аппаратной форме, но имеет затратную реализацию в программной форме (большое число битовых перестановок).
3. Трансформированное понятие транспортного потока. Если в сетях DVB (эфирные, кабельные, спутниковые) транспортный поток представляет собой мультиплексированный поток данных нескольких каналов + служебная информация, то в сетях IP существует необходимость демультиплексированной передачи данных на уровне одного канала.

### 3.2 Гибридная модель защиты данных IP-вещания

Для эффективной работы системы в условиях полноценной двунаправленной IP сети, необходима модификация структурной схемы работы системы. Модифицированная

структурная схема представлена на рис.3.4. Для преодоления трудностей использования дорогих (в смысле лицензирования) алгоритмов скрамблирования DVB-CSA, в рамках IP-вещания целесообразно воспользоваться не так давно принятым Национальным институтом стандартов (НИСТ) США алгоритмом AES (Advanced Encryption Standard) симметричного блочного шифрования [23], а для передачи ключей использовать безопасное двунаправленное соединение абонентского терминала с системой управления пользователями оператора с непосредственной аутентификацией и авторизацией абонента. То есть блоки скрамблирования и дескрамблирования (схема на рис.3.3) в предлагаемой реализации занимает симметричное шифрование на основе алгоритма AES, а вместо системы условного доступа, работающей на основе ECM/EMM сообщений, система аутентификации и авторизации пользователей на основе асимметричного алгоритма шифрования RSA [26].

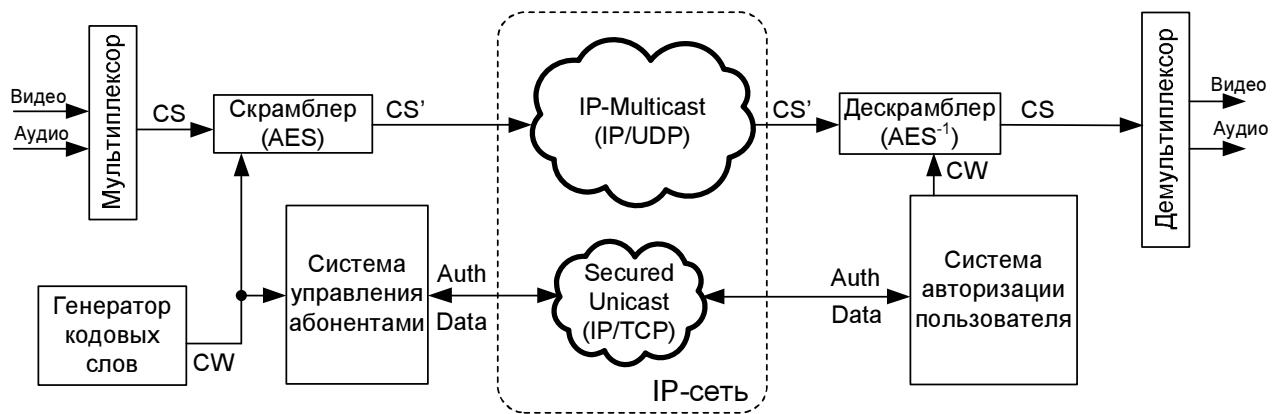


Рисунок 3.4 – Структурная схема работы защиты контента в IP-вещания

Таким образом, отличие от схемы работы DVB-CSA заключается в том, что транспортный поток мультиплексированных данных всех каналов и служебной информации (TS) заменен транспортным потоком мультиплексированных данных одного канала (канальный поток, CS), причем в этот транспортный поток не включены данные для системы условного доступа (ECM и EMM). Канальный поток (CS) после скрамблирования (CS') доставляется до абонентов по мультикаст сети, а необходимые данные для дескрамблирования передаются индивидуально каждому абоненту по защищенной юникаст сети (Secured Unicast), что может быть реализовано на основе SSL (Secured Socket Layer [27]) технологии (см. п.3.2.2.2). Поток данных в рамках Secured Unicast по сравнению с канальным потоком (CS') - незначительный (установление соединения абонентом, аутентификация, авторизация, передача необходимых ключей для дескрамблирования данных), поэтому применение unicast технологии не будет являться каким либо ограничением работы системы.

Для различных типов разграничения доступа к мультимедийному вещанию и требований к уровню безопасности, блок авторизации может быть чисто программным, либо использовать уникальные для пользователя аппаратные элементы.

В случае программной реализации блока авторизации, уникальность пользователя будет обеспечена с помощью логина и пароля и/или подписанных системой управления

ния пользователями публичного ключа. При необходимости ограничения использования IP-TV услуг с логином и паролем в рамках одного компьютера, можно воспользоваться дополнительной авторизацией на основе IP адреса.

В случае необходимости более глубокой системы защиты, возможно реализация аутентификации и авторизации на базе аппаратных ключей (USB, COM, LPT). Максимальная, но и самая дорогостоящая, защита может быть при реализации блоков системы авторизации и дескрамблирования в рамках одного USB устройства. В таком случае весь процесс раскодирования данных канала происходит вне персонального компьютера, а следовательно невозможным становится программное отслеживание ключей декодирования.

Схему работы защищённой от несанкционированного доступа системы IP-вещания можно проиллюстрировать диаграммой вариантов использования (UML Use Case Diagram), представленной на рис.3.5. В таблице 3.1 даны расшифровки и пояснения к блокам диаграммы. Из схемы видно, что внешними по отношению к системе являются три компонента: непосредственно оператор системы, принимающий решение о вещаемых каналах и доступа к вещанию пользователей («Управление пользователями» на схеме), абоненты и собственно распространяемый контент. Система может предусматривать перед непосредственной передачей контента в сеть модификацию контента в плане его перекодирования (например из MPEG-2 формата MPEG-4 AVC/H.264 формат), а также скрамблирования. Процесс скрамблирования включает элемент генерации кодовых слов (CW), которые в свою очередь через систему управления пользователями (путем авторизации и аутентификации абонентского терминала) доставляются легальным абонентам. Более подробно работа распределенной системы вещания описана в разделе 4.

Таблица 3.1 – Спецификация диаграммы вариантов использования защищенной системы IP-вещания

Наименование	Примечание
<b>Актеры</b>	
Контент	Собственно мультимедийные данные, получаемые из какого-либо источника
Оператор	Оператор системы IP-вещания
Абонент	Конкретный абонент системы IP-вещания
<b>Варианты использования</b>	
Передача в сеть	Процесс подготовки и передачи в сеть мультимедийного контента. В процесс подготовки входит сжатие и/или перекодирование исходного материала, а также скрамблирование с целью защиты от несанкционированного доступа
Сжатие/Перекодирование	Процесс преобразования исходных мультимедийных данных в необходимый формат (H.264) с требуемыми характеристиками (качество, битрейт)

Продолжение таблицы 3.1

Наименование	Примечание
Скрамблирование	Процесс скрамблирования мультимедийных данных для защиты от несанкционированного доступа к услугам IP-вещания. Ключи процесса скрамблирования (симметричное шифрование AES) формируются с помощью процесса генерации ключей
Генерация ключей скрамблирования	Процесс генерации ключей симметричного шифрования. Может быть реализован либо чисто программно с использованием генератора псевдослучайных чисел, либо, при необходимости повышенной степени безопасности, с помощью энтропийного генератора случайных чисел
Управление пользователями	Подсистема управления пользователями, в т.ч. процесс биллинга. Интегрирует процессы установки прав абонента на контент (сроки подписки, доступные каналы) и непосредственно авторизацию пользователей и передачу по защищенному каналу необходимых ключей для дескрамблирования
Установка прав абонент-контент	Подпроцесс управления пользователями, реализующий биллинговую систему
Авторизация пользователей	Подпроцесс управления пользователями непосредственно осуществляющий взаимодействие с абонентскими терминалами (STB, ПК), обеспечивающий авторизацию и передачу необходимой информации для дескрамблирования данных
Получение данных из сети	Подключение к необходимым мультикаст группам и доставка данных на абонентский терминал с серверов оператора
Просмотр вещания	Процесс выбора интересующего канала из списка доступных и его отображение на абонентском терминале. Включает процесс дескрамблирования и процесс получения списка разрешенных каналов
Дескрамблирование	Процесс дескрамблирования получаемых с серверов оператора мультимедийных данных, включает

Продолжение таблицы 3.1

Наименование	Примечание
Аутентификация и авторизация	Процесс аутентификации и авторизации абонентского терминала в системе управления пользователями оператора, интегрирует в себя процессы получения списка разрешенных каналов и ключей для дескрамблирования мультимедийного потока с серверов оператора
Получение списка разрешенных каналов	Запрос и актуализация списка доступных абоненту каналов в рамках IP-вещания
Получение ключей дескрамблирования	Процесс постоянного получения по защищенному каналу ключей для дескрамблирования мультимедийных данных, получаемых с серверов оператора

### 3.2.1 Процесс скрамблирования алгоритмом симметричного шифрования AES

Выбор алгоритма AES в качестве основы процесса скрамблирования и дескрамблирования был сделан на основании ряда критериев: алгоритм AES может быть эффективно реализован в аппаратной и программной форме, стандарт AES имеет высокую стойкость к взлому, а также минимальная (или нулевая) стоимость использования алгоритма.

Формальное начало процессу разработки нового криптостандарта было положено 2 января 1997 года, когда национальный институт стандартов США объявил о своем решении разрабатывать AES по причине моральной устаревшести DES и недостаточной эффективности заменившего его алгоритма «Triple DES» (по сути дела, тот же самый шифр, применяемый три раза). Затем, 12 сентября того же года был опубликован официальный призыв ко всем заинтересованным кругам о выдвижении своих алгоритмов в качестве возможных кандидатов [22]. Тогда же были оговорены следующие первичные требования, которым должен удовлетворять AES: это должен быть незасекреченный, открыто опубликованный алгоритм шифрования, бесплатно доступный по всему миру. Спустя некоторое время было уточнено, что AES будет блочным шифром, реализующим криптографию с симметричным ключом, причем алгоритм (как минимум) должен поддерживать 128-битную длину шифруемого блока текста и длины ключей размером 128, 192 и 256 бит. Если же формулировать цель процесса AES совсем кратко, то ее можно свести к таким словам: «новый блочный шифр должен быть более стойким и более эффективным, чем Triple DES».

Критерии оценки алгоритмов-кандидатов были разработаны на основе первичных требований НИСТ и последовавшего затем публичного обсуждения на проведенном в Ин-

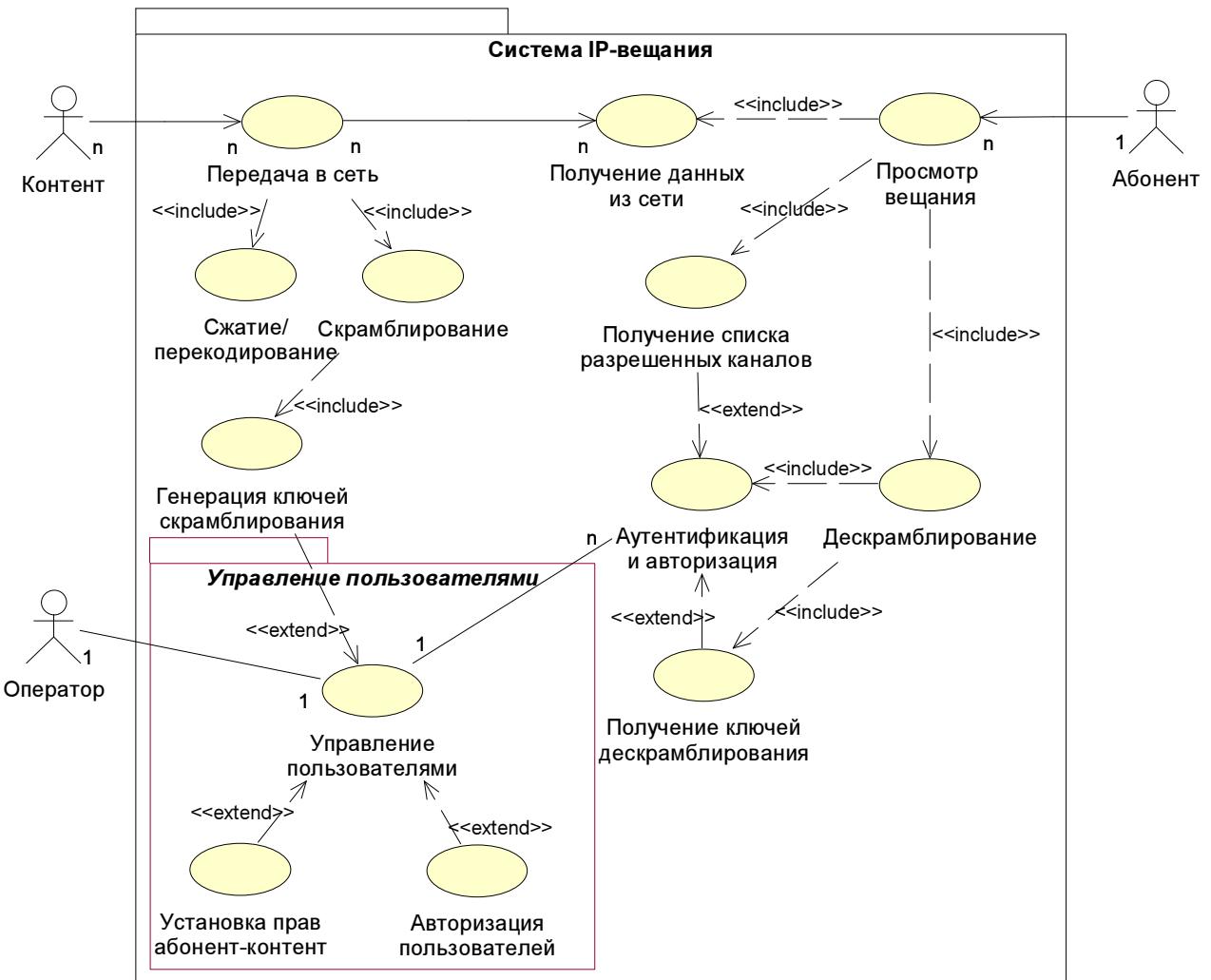


Рисунок 3.5 – Диаграмма вариантов использования защищенной системы IP-вещания

ституте стандартов открытом семинаре 15 апреля 1997 года. Все оценочные критерии были разбиты на три основные категории: стойкость, стоимость, характеристики алгоритма:

- *Стойкость* расценивается как самый важный фактор при оценке кандидатов. Под стойкостью понимаются такие свойства шифра как неподдаваемость алгоритма криptoаналитическому вскрытию, прочность его математического фундамента, равновероятность выхода алгоритма и, наконец, относительная стойкость алгоритма в сравнении с остальными кандидатами.
- *Стоимость* - это вторая важная область оценки, куда включаются и вопросы (аннулирования необходимости) лицензирования, вычислительная эффективность (скорость) на разнообразных платформах и требования к памяти.
- *Характеристики алгоритма* и его реализации, такие как гибкость, простота, программная и аппаратная «укладываемость» - это третья важная область оценки кандидатов. Под гибкостью понимается способность алгоритма работать с различными длинами ключей и блоков текста, возможность реализации алгоритма в качестве поточного шифра, алгоритма хеширования, генератора случайных чисел и т.д.

Победителем конкурса и новым стандартом стал алгоритм Rijndael, разработанный двумя специалистами по криптографии из Бельгии. Алгоритм представляет каждый блок кодируемых данных в виде двумерного массива байт размером 4x4, 4x6 или 4x8 в зависимости от установленной длины блока [24]. Далее на соответствующих этапах преобразования производятся либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами в таблице.

Так как алгоритм может быть сформулирован в терминах всего лишь двух операций, - побитового суммирования по модулю 2 и индексированного извлечения из памяти, выполняемых над байтами [24], - он может быть эффективно реализован на любых компьютерных платформах от младших микроконтроллеров до суперпроцессоров. В силу тех же причин, а также потому что архитектура алгоритма допускает высокую степень параллелизма, он может быть также очень эффективно реализован в аппаратуре. В конечном итоге именно приведенные выше факторы вкупе с высокой стойкостью алгоритма определили его победу в конкурсе на место нового стандарта.

Прямое и обратное преобразования в шифре имеют одинаковую алгоритмическую структуру и различаются константами сдвига, ключевыми элементами, узлами замен и константами умножения. При аппаратной реализации они могут быть совмещены на 60%, при программной оптимальное быстродействие может быть достигнуто лишь при полностью раздельных реализациях обеих функций.

Все преобразования в шифре имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-битных так и на 32-битных процессорах. В структуре алгоритма заложена возможность параллельного выполнения некоторых операций, что на многопроцессорных рабочих станциях может еще поднять скорость шифрования в 4 раза.

Принятый стандарт AES на основе алгоритма Rijndael [25] определяет ряд комбинаций длин ключа, размера шифруемого блока и количество раундов (один шаг преобразования) шифрования, представленных в таблице 3.2. Результат каждого раунда представляет собой состояние или промежуточный результат.

Таблица 3.2 – Комбинации длин ключа, шифруемого блока и числа раундов AES

	<b>Длина ключа (<math>N_k</math> слов)</b>	<b>Размер блока (<math>N_b</math> слов)</b>	<b>Число раундов (<math>N_r</math>)</b>
<b>AES-128</b>	4	4	10
<b>AES-192</b>	6	4	12
<b>AES-256</b>	8	4	14

Работу алгоритма определяется псевдокодом, представленным в листинге 3.1.

Как можно увидеть из листинга алгоритмом определены лишь четыре операции преобразования: AddRoundKey, SubBytes, ShiftRows и MixColumns.

```

Cipher( byte in[4*Nb] , byte out[4*Nb] , word w[Nb*(Nr+1)])
begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state , w[0 , Nb-1])      // См.н.3.2.1.4

    for round = 1 step 1 to -Nr1
    begin
        SubBytes(state)                  // См.н.3.2.1.1
        ShiftRows(state)                // См.н.3.2.1.2
        MixColumns(state)               // См.н.3.2.1.3
        AddRoundKey(state , w[round*Nb , (round+1)*Nb-1])
    end

    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state , w[Nr*Nb , (Nr+1)*Nb-1])
    out = state
end

```

Листинг 3.1 – Псевдокод алгоритма AES

### 3.2.1.1 Преобразование SubBytes()

Преобразование `SubBytes()` является нелинейной заменой байт, которая производится независимо над каждым байтом *состояния* с использованием таблиц замены (S-box). Эти таблицы, из которых могут быть получены обратные, сформированы с помощью двух преобразований [25]:

1. Получение обратного элемента относительно умножения в поле  $GF(2^8)$ . Элемент  $\{00\}$  переходит сам в себя.
2. Осуществление афинного (3.1) преобразования над  $GF(2)$ .

$$b'_i = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i \quad \text{для } 0 \leq i < 8 \quad (3.1)$$

где  $b_i$  —  $i$ -й бит байта;

$c_i$  —  $i$ -й бит байта со значением  $\{63\}_{10} \equiv \{01100011\}_2$ .

Используемая в преобразовании `SubBytes()` таблица замены (S-box) представлена на рис.3.6.

### 3.2.1.2 Преобразование ShiftRows()

В преобразовании `ShiftRows()` последние 3 строки состояния циклически сдвигаются на различное число байт, первая строка не сдвигается.

Определяется `ShiftRows()` формулой (3.2) [25].

$$s'_{r,c} = s_{r,(c+shift(r,Nb))mod Nb} \quad \text{для } 0 < r < 4 \quad \text{и} \quad 0 \leq c < Nb \quad (3.2)$$

		γ															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Рисунок 3.6 – S-box - таблица замены для байта  $xy$  (в шестнадцатеричном формате)

где значение  $shift(r, Nb)$  зависит от номера строки  $r$  (длина блока  $Nb = 4$ , см.табл.3.2):

$$shift(1, 4) = 1; \quad shift(2, 4) = 2; \quad shift(3, 4) = 3;$$

### 3.2.1.3 Преобразование MixColumns()

Преобразование MixColumns() обрабатывает столбцы состояния, рассматривая их как многочлены над  $GF(2^8)$  и умножая по модулю  $x^4 + 1$  на многочлен  $a(x)$  [25], определенный следующим образом:

$$a(c) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \quad (3.3)$$

Уравнение (3.3) можно представить в матричной форме:

$$s'(x) = a(x) \otimes s(x) : \begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{для } 0 \leq c < Nb \quad (3.4)$$

### 3.2.1.4 Преобразование AddRoundKey()

В данной операции итерационный ключ состояния формируется посредством простого XOR. Каждый итерационный ключ вырабатывается из ключа шифрования посредством алгоритма выработки ключей (key schedule). Длина итерационного ключа равна длине блока Nb.

Работа преобразования определяется [25]:

$$[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c}] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] \oplus [w_{round*Nb+c}] \quad \text{для } 0 \leq c < Nb \quad (3.5)$$

где  $[w_i]$  — текущий выработанный ключ;

$round$  — значение из диапазона  $0 \leq round \leq Nr$ .

### 3.2.1.5 Алгоритм выработки ключей

Итерационные ключи получаются из ключа шифрования посредством алгоритма выработки ключей. Общее число бит итерационных ключей равно длине блока, умноженной на число циклов плюс 1 (например, для длины блока 128 бит и 10 циклов требуется 1408 бит итерационных ключей).

Алгоритм определяется псевдокодом, представленным в листинге 3.2.

```
KeyExpansion( byte key [4*Nk] , word w[Nb*(Nr+1)] , Nk)
begin
    word temp

    i = 0

    while ( i < Nk)
        w[i] = word(key[4*i] , key[4*i+1] , key[4*i+2] , key[4*i+3])
        i = i+1
    end while

    i = Nk

    while ( i < Nb * (Nr+1)]
        temp = w[i-1]
        if ( i mod Nk = 0)
            temp = SubWord(RotWord(temp)) xor Rcon[ i /Nk]
        else if (Nk > 6 and i mod Nk = 4)
            temp = SubWord(temp)
        end if
        w[i] = w[i-Nk] xor temp
        i = i + 1
    end while
end
```

Листинг 3.2 – Псевдокод алгоритма выработки итерационных ключей AES

Функция `SubWord()` принимает на вход четырехбайтное слово и осуществляет подстановочную замену с помощью таблицы S-box (см.рис.3.6), формируя тем самым четырехбайтное возвращаемое значение. Функция `RotWord()` осуществляет циклическую перестановку четырехбайтного слова:  $[a_0, a_1, a_2, a_3] \rightarrow [a_1, a_2, a_3, a_0]$ . Константный массив слов `Rcon[i]` содержит значения, определяемые как  $[x^{i-1}, \{00\}, \{00\}, \{00\}]$ , где  $x^{i-1}$  степени  $x$  ( $x = \{02\}$ ) в  $GF(2^8)$  [25].

### 3.2.2 Создание защищённой unicast сети между оператором и абонентом

Как уже отмечалось выше, вторым основным компонентом защиты от несанкционированного доступа (после собственно процесса скрамблования) гибридной модели системы IP-вещания является организация защищенного канала «Оператор-Абонент» (блок «Secured Unicast» на схеме на рис.3.4), в рамках которого осуществляется аутентификация

абонента, авторизация (выдача списка разрешенных к просмотру каналов) и собственно передача ключей для дескрамблирования мультимедийных данных.

Эффективной реализацией такой защиты может стать полное шифрование передаваемых данных от абонента к оператору и наоборот с помощью какого либо симметричного шифрования (например с помощью рассмотренного ранее AES) с генерацией и согласованием сессионного ключа этого шифрования во время установления соединения с помощью асимметричного шифрования (шифрование с открытым ключом). Такая гибридная модель необходима, поскольку, для обеспечения сравнимого уровня стойкости, асимметричному шифрованию требуется длина ключа на несколько порядков больше, чем симметричному шифрованию, а следовательно низкая скорость шифрования (около 30 кбит/с при 512 битном ключе на процессоре 2 ГГц).

В шифровании с помощью открытого ключа, например RSA (см.п.[3.2.2.1](#)), используется пара ключей: открытый ключ и частный ключ [26], известный только его владельцу. Открытый ключ может распространяться по сети. Секретный ключ в криптографии с открытыми ключами используется для формирования электронной подписи и расшифрования данных. Однако, непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для определения связи с секретным ключом. Без такой дополнительной защиты злоумышленник (нелегальный пользователь системы IP-вещания) может представить себя как отправителем подписанных данных, так и получателем зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. Другими словами, остро стоит необходимость верификации или проверка подлинности открытого ключа. Для этих целей используется электронный сертификат.

Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с определенным пользователем или приложением. Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра - Центра Сертификации (ЦС). В системе IP-вещания, таким ЦС будет выступать подсистема системы управления пользователями (см.[рис.3.4](#)). Используя открытый ключ ЦС, каждый пользователь (и абоненты, и оператор) может проверить достоверность электронного сертификата, выпущенного ЦС, и воспользоваться его содержимым.

Использование смешанного асимметричного и симметричного шифрования вкупе с электронными сертификатами позволяет защитить от несанкционированного доступа передачу данных от абонента до оператора и обратно. Пара логина и пароля может обеспечить возможность, дополнительно к данным открытого ключа, идентифицировать пользователя. Использование IP и MAC адресов позволяет ограничить использование IP-вещанием одним абонентским устройством (в т.ч. ПК) на один логин/пароль/сертификат.

Процессы шифрования с помощью открытого ключа и работа с электронным сертификатом основаны на одних и тех же принципах работы асимметричного шифрования. В процессе шифрования и дешифрации открытый ключ используется для собственно шифрации данных, а соответствующий ему частный ключ для дешифрации. Процесс подписывания и проверки электронного сертификата обратный: частный ключ используется

для формирования электронной подписи, а публичный ключ - для проверки электронного сертификата. Принцип работы асимметричного шифрования на примере алгоритма RSA показан в следующем параграфе.

### 3.2.2.1 Алгоритм асимметричного шифрования RSA

RSA — криптографический алгоритм с открытым ключом. RSA стал первым алгоритмом такого типа, пригодным и для шифрования и для цифровой подписи. Алгоритм получил широкое распространение и в настоящее время используется в большом числе криптографических приложений.

Безопасность алгоритма RSA основана на трудности задачи разложения на множители. Алгоритм использует два ключа — *открытый* (public) и *секретный* (private), вместе открытый и соответствующий ему секретный ключи образуют пару ключей (keypair). Открытый ключ не требуется сохранять в тайне, он используется для зашифрования данных. Если сообщение было зашифровано открытым ключом, то расшифровать его можно только соответствующим секретным ключом.

#### Генерация ключей

Для того, чтобы сгенерировать пару ключей выполняются следующие действия [26]:

1. Выбираются два больших простых числа  $p$  и  $q$ .
2. Вычисляется их произведение  $n = pq$ .
3. Вычисляется Функция Эйлера  $\varphi = (p - 1)(q - 1)$ .
4. Выбирается целое  $e$ , такое, что  $1 < e < \varphi(n)$  и  $e$  взаимно простое с  $\varphi(n)$ .
5. С помощью расширенного алгоритма Евклида находится число  $d$ , такое, что  $ed \equiv 1 \pmod{\varphi(n)}$ .

Число  $n$  называется модулем, а числа  $e$  и  $d$  — открытой и секретной экспонентами, соответственно. Пара чисел  $(n, e)$  является открытой частью ключа, а  $d$  — секретной. Числа  $p$  и  $q$  после генерации пары ключей могут быть уничтожены, но ни в коем случае не должны быть раскрыты.

#### Шифрование и расшифрование

Для того, чтобы зашифровать сообщение  $m < n$  вычисляется

$$c = m^e \pmod{n} \quad (3.6)$$

Число  $c$  и используется в качестве шифртекста. Для расшифрования нужно вычислить

$$m = c^d \pmod{n} \quad (3.7)$$

Можно показать, что при расшифровании будет восстановлено исходное сообщение

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}$$

Из условия

$$ed \equiv 1 \pmod{\varphi(n)}$$

следует, что

$ed = k\varphi(n) + 1$  для некоторого целого  $k$ , следовательно

$$m^{ed} \equiv m^{k\varphi(n)+1} \pmod{n}$$

Согласно теореме Эйлера:

$$m^{\varphi(n)} \equiv 1 \pmod{n},$$

поэтому

$$m^{k\varphi(n)+1} \equiv m \pmod{n}$$

$$c^d \equiv m \pmod{n}$$

### Цифровая подпись

RSA может использоваться не только для шифрования, но и для цифровой подписи. Подпись  $s$  сообщения  $m$  вычисляется с использованием секретного ключа по формуле:

$$s = m^d \pmod{n} \quad (3.8)$$

Для проверки правильности подписи нужно убедиться, что выполняется равенство

$$m = s^e \pmod{n} \quad (3.9)$$

**Длина ключа** Число  $N$  должно иметь размер не меньше 512 бит. В настоящий момент система шифрования на основе RSA считается надёжной, начиная с размера  $N$  в 1024 бита [26].

#### 3.2.2.2 Безопасная передача данных на основе протокола SSL

Использование только асимметричного шифрования для обеспечения безопасной передачи данных является неэффективным с точки зрения производительности, что обусловило создание специального протокола канального уровня SSL (Secured Socket Layer), интегрирующего асимметричное и симметричное шифрование, позволяя тем самым эффективно реализовать защищённый канал «Оператор-Абонент» в рамках системы IP-вещания.

Протокол SSL предоставляет «безопасный канал», который имеет три основные свойства:

- Канал является частным. Шифрование используется для всех сообщений после

простого диалога, который служит для определения секретного ключа.

- Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, в то время как клиентская - аутентифицируется опционно.
  - Канал надежен. Транспортировка сообщений включает в себя проверку целостности (с привлечением MAC).

Работа SSL включает в себя три основных фазы:

1. Диалог между сторонами, целью которого является выбор алгоритма шифрования
  2. Обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификатов.
  3. Передача данных, шифруемых при помощи симметричных алгоритмов шифрования

Схема работы алгоритма работы установления сессии SSL представлен на рис.3.7 [28]. В случае, если сервер и клиент осуществляют восстановление ранее установленной SSL сессии (например в случае разрыва соединения протокола нижнего уровня), то опциональные сообщения не используются.

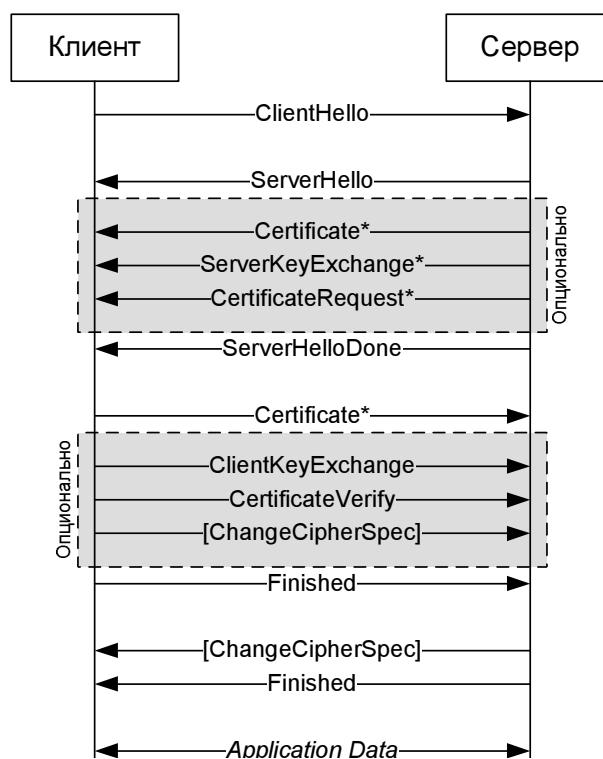


Рисунок 3.7 – Алгоритм установления сессии SSL

Для установления сессии клиенты посылают hello-сообщение *ClientHello*, на которое сервер должен ответить сообщением *ServerHello*, либо сообщить о фатальной ошибке. Сообщения *ClientHello* и *ServerHello* предназначены для определения параметров безопасности сессии и включают следующие параметры: версия протокола, идентификатор сессии, набор возможных алгоритмов шифрования, метод сжатия данных. Кроме того, сервер и клиент могут обмениваться двумя наборами генерированных случайных данных.

После hello-сообщений, сервер, если должен быть аутентифицирован, посыпает свой сертификат. В случае необходимости может быть послано сообщение *ServerKeyExchange*. Сервер может запросить аутентификацию клиента путем запроса сертификата сообщением *CertificateRequest*. После чего, сервер посыпает сообщение окончания приветствия *ServerHelloDone* и ожидает ответа клиента. Если был запрошен, клиент посыпает свой сертификат, после чего (опционально) сообщение *ClientKeyExchange*, содержание которого зависит от выбранного алгоритма шифрования. В случае, если клиент отоспал сертификат с возможностью подписывания, посыпается верифицирующее сообщение подписанного цифрового сертификата *CertificateVerify*.

Далее посыпается клиентом сообщение изменения параметров шифрования [*ChangeCipherSpec*], после чего посыпает завершающее сообщение *Finished* с использование новых алгоритмов и ключей шифрования. В ответ сервер посыпает свои параметры шифрования [*ChangeCipherSpec*] и завершающее сообщение *Finished*. После чего сессия SSL считается установленным и далее происходит работа прикладного протокола.

### 3.2.3 Реализация модели защиты данных IP-вещания с помощью openSSL

Создавать реализацию алгоритмов симметричного и асимметричного шифрования (блока скрамблирования, дескрамблирования и «Secured Unicast» на схеме на рис.3.4) является достаточно сложной задачей, с необходимостью постоянного отслеживания ситуаций ошибок и взломов реализаций крипто-алгоритмов.

В настоящее время существует свободно-распространяемая достаточно легко встраиваемая библиотека OpenSSL, эффективно реализующая набор симметричных и асимметричных алгоритмов шифрования, а также собственно протокол SSL для организации безопасного канального соединения. Другим, не менее важным достоинством библиотеки OpenSSL является проверенность библиотеки временем, а также ее свободность в плане отсутствия каких либо ограничений на использование ее в коммерческих приложениях [29].

Возможности библиотеки OpenSSL во многом превышают определенные потребности IP-вещания, что открывает перспективы будущих модификаций подсистемы безопасности. Функции OpenSSL включают в себя:

- Создание и управление ключами RSA и DSA (команды rsa, dsa, dsaparam).
- Создание сертификатов формата x509, запросы на сертификацию, восстановление (команды x509, req, verify, ca, crl, pks12, pks7).
- Шифрование данных с помощью симметричного и асимметричного шифрования (команды enc, rsautl).
- Вычисление хеш-значений различных типов (команда dgst).
- Работа с S/MIME (команда s/mime).
- Проверка работы серверов и клиентов ssl (команды s\_client, s\_server).

Эффективность работы OpenSSL может быть проверена с помощью встроенной утилиты:

---

```
#> openssl speed [список_алгоритмов_хеширования_или_шифрования]
```

---

Результат тестирования алгоритмов симметричного и асимметричного шифрования на компьютере Intel Pentium 4/2.4GHz/RAM 1536Mb представлены в таблицах 3.3 и 3.4 соответственно.

Таблица 3.3 – Результат тестирования работы симметричного шифрования с помощью библиотеки OpenSSL

Алгоритм	16 байт	64 байт	256 байт	1024 байт	8192 байт
<b>des cbc</b>	31953.56k	32260.77k	32650.03k	32977.33k	32183.42k
<b>des ede3</b>	12460.80k	12337.09k	12233.18k	12439.93k	12431.41k
<b>aes-128 cbc</b>	40354.10k	40050.65k	42902.99k	42490.10k	43279.29k
<b>aes-192 cbc</b>	34397.16k	36412.84k	38121.37k	37440.79k	35991.02k
<b>aes-256 cbc</b>	31699.98k	32316.70k	32967.61k	33807.99k	32768.00k

*Примечание.* Результат тестирования показывает скорость шифрования/десифрования данных кибибайт в секунду (KiB/s)

Таблица 3.4 – Результат тестирования работы асимметричного шифрования с помощью библиотеки OpenSSL

Алгоритм	Подпись, сек	Проверка, сек	Подпись, 1/сек	Проверка, 1/сек
<b>rsa 512 bits</b>	0.001339	0.000137	746.6	7313.2
<b>rsa 1024 bits</b>	0.006913	0.000351	144.7	2846.3
<b>rsa 2048 bits</b>	0.040080	0.001199	25.0	834.2
<b>rsa 4096 bits</b>	0.283700	0.004046	3.5	247.1
<b>dsa 512 bits</b>	0.001127	0.001320	887.6	757.5
<b>dsa 1024 bits</b>	0.003159	0.003884	316.5	257.5
<b>dsa 2048 bits</b>	0.011590	0.013748	86.3	72.7

Из таблицы 3.3 можно видеть, что наиболее быстрым является алгоритм симметричного шифрования с длиной ключа 128 бит. Увеличение длины ключа приводит к снижению скорости работы. Полученная в результате тестирования скорость работы  $> 40 \text{ MiB/s}$  достаточна для скрамблования с помощью одного недорогого ПК одновременно более 80 каналов, при использовании стандартного качества MPEG-4/AVC кодирования видео. Масштабирование, в случае вещания большего числа каналов, может легко реализовано с помощью увеличения числа скрамблирующих ПК в рамках головной станции оператора.

Таблица 3.4 показывает, что при использовании алгоритма RSA асимметричного шифрования с длиной ключа 1024 бит, который сможет обеспечить высокий уровень криптостойкости в ближайшем будущем [26] скорость операций подписывания и верификации сертификатов составляет  $114.7 \text{ сек}^{-1}$  и  $2846.3 \text{ сек}^{-1}$  соответственно. Такое быстродействие во много раз превышает потребности системы IP-вещания с использованием SSL протокола, поскольку операции подписывания/верификации осуществляются только в момент установления соединения «Абонент-Оператор», а вся дальнейшая передача данных шифруется симметричным алгоритмом (DES, AES).

## Выводы

Защита от несанкционированного доступа (ЗНД) к вещанию является одним из важнейших элементов любой вещательной деятельности, в том числе, важнейшим элементом мультимедийного вещания в сетях передачи данных. Цели ЗНД могут быть различными: защита авторских и смежных прав (ограничение зоны вещания: эфирное телевидение - естественное ограничение зоны; спутниковое телевидение - ограничение на основе системы защиты без идентификации конкретного абонента), продажа услуг пользователям (т.е. защита от нелегальных пользователей - ограничение на основе системы защиты с идентификацией конкретного абонента). Кроме того, при использовании различных типов вещания, существенно различаются способы реализации ЗНД: аналоговые, цифровые, с использованием встроенных в оборудование чипов, специальных смарт-карт, аппаратных ключей, на основе шифрования с публичным ключем, доступ по логину/паролю.

Используемая многоуровневая модель разграничения доступа к вещанию в стандарте DVB скрамблирует транспортный поток с помощью симметрично шифрования, ключи которого передаются абонентам в рамках этого же транспортного потока, используя проприетарные механизмы (Viacess, Conax, BISS, Mediaguard и другие) шифрования и управления абонентами (на основе смарт-карт).

Непосредственное перенесение технологии DVB-CSA в рамки IP сетей возможен, но сталкивается с рядом трудностей: проблемы лицензирования разработки и использования скрамблера и дескрамблеров DVB-CSA, что зачастую является неприемлемым для сетей малых и средних сетей; алгоритм DVB-CSA заточен на простую реализацию в аппаратной форме, но затратную реализацию в программной форме (большое число битовых перестановок); трансформированное понятие транспортного потока.

Преодоление трудностей использования алгоритмов скрамблирования DVB-CSA, в рамках IP-вещания целесообразно воспользоваться алгоритмом AES симметричного блочного шифрования, а для передачи ключей использовать безопасное (SSL) двунаправленное соединение абонентского терминала с системой управления пользователями оператора с непосредственной аутентификацией и авторизацией абонента.

Протокол SSL предоставляет безопасный канал, который имеет основные свойства: канал является частным, шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа; канал аутентифицирован, канал надежен. В основе шифрования с открытым ключем предлагается использовать алгоритм RSA – криптографический алгоритм с открытым ключом, безопасность которого основана на трудности задачи разложения на множители.

## 4 РЕАЛИЗАЦИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

В данном разделе производится системное исследование мультимедийного вещания в сетях передачи данных. Система мультимедийного вещания (СМВ) представляет собой комплекс программно-аппаратных средств, комбинация которых обеспечивает абонентам качественный приём и визуализацию заказанных мультимедийных данных. Если ограничить понятие приёма рамками сети передачи данных, то в общем виде СМВ будет состоять из четырёх подсистем: управления и контроля IP-вещания, формирования контента, сетевой и абонентской подсистемы (рис.4.1).



Рисунок 4.1 – Структурная схема системы IP-вещания

Могут существовать различные варианты реализации каждой подсистемы: чисто программная, программно-аппаратная (на базе ПК), либо чисто аппаратная (микропрограммная). Выбор той или иной конфигурации системы во многом определяется предъявляемыми требованиями: количество, качество и тип вещаемых каналов, необходимый уровень защиты от несанкционированного доступа к системе. При этом должны учитываться ограничения: общая стоимость системы и цена необходимой модернизации сети передачи данных.

Смысль распределенности разрабатываемой СМВ закладывается в подсистемы формирования контента и сетевую подсистему. В распределенной или GRID-подсистеме формирования контента множество мультимедийного материала доступного в сети формируется с помощью независимых формировательных элементов (IP-TV формирователей), объединенных в единую логическую структуру (см. п.4.2). В распределенной сетевой подсистеме доставка контента осуществляется с использованием не только собственно сетевого оборудования, а с задействованием специальных шлюзовых компонентов (IP-TV шлюзов), формирующих и ретранслирующих на основе доступного сетевого контента подмножество мультимедийных данных (см. п.4.3). Оба элемента позволяют, создав систему IP-вещания в рамках одной сети, при расширении этой сети или создание IP-вещания в

другой сети использовать инвестиции в IP-TV инфраструктуру не для реализации базовых возможностей IP-TV сети (базового набора каналов), а для расширения спектра возможностей как новой, так и старой IP-TV за счет использования вещательных ресурсов обоих сетей в рамках единого IP-TV поля.

## 4.1 Подсистема управления и контроля распределенной системы IP-вещания

Главным элементом любой системы является управляющий орган, которым, в нашем случае, является подсистема управления и контроля системы IP-вещания. Основной целью подсистемы управления является задание нужного режима работы системы в целом, т.е. формирование и контроль передачи данных из подсистемы формирования контента в абонентскую подсистему посредством сетевой подсистемы. Контрольная часть должна обеспечить необходимый уровень качества работы путем сбора статистической информации на каждом этапе формирования, передачи и получения данных.

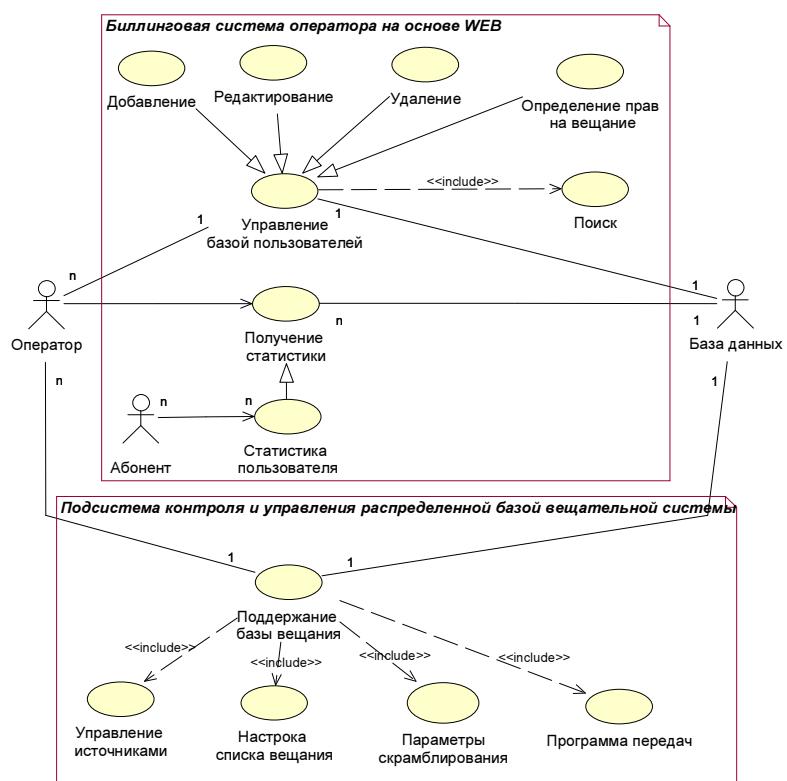


Рисунок 4.2 – Диаграмма вариантов использования подсистемы управления пользователей

В рамках подсистемы управления вещанием можно выделить ряд основополагающих компонентов: абонентское управление, управление вещанием и получение статистической информации вещания (обратная связь). Интерфейсную часть этих компонентов целесообразно реализовывать в рамках WEB-интерфейсов. Разработанная схема вариантов использования подсистемы управления и контроля (интерфейсная часть) представлена на диаграмме (рис.4.2) с комментариями в таблице 4.1.

Таблица 4.1 – Спецификация диаграммы вариантов использования подсистемы управления пользователями

Наименование	Примечание
<b>Актеры</b>	
Оператор	Оператор системы IP-вещания
Абонент	Абонент системы IP-вещания
База данных	Единая СУБД оператора, хранящая всю абонентскую и вещательную информацию
<b>Варианты использования</b>	
Управление базой пользователей	Актуализация посредством WEB интерфейса абонентской базы
<i>Добавление</i>	Интерфейс добавления новых абонентов
<i>Редактирование</i>	Интерфейс редактирования информации существующих абонентов
<i>Удаление</i>	Интерфейс удаления абонентской информации
<i>Определение прав на вещание</i>	Интерфейс определения доступных абоненту вещательных программ, а также реквизиты доступа абонента к системе вещания (логин, пароль, IP-адрес)
<i>Поиск</i>	Интерфейс поиска абонентской информации в базе
Получение статистики	Интерфейс получения статистической информации мультимедийного вещания: статистика по каждому пользователю, суммарная статистика использования системы, статистика использования пропускной способности магистральных каналов, статистика работы вещательных серверов
<i>Статистика пользователя</i>	Интерфейс получения статистики работы конкретного пользователя
Поддержка базы вещания	Актуализация посредством WEB интерфейса вещательной базы
<i>Управление источниками</i>	Интерфейс определения и управления источниками вещания (управление подсистемой формирования контента)
<i>Параметры скрамблирования</i>	Интерфейс определения параметров скрамблирования, в т.ч. формирование списка скрамблруемых и нескрамблруемых каналов и выбор типа скрамблирования (составная часть управления подсистемой формирования контента)

## Продолжение таблицы 4.1

Наименование	Примечание
<i>Настройка вещания</i>	Интерфейс управления сетевой подсистемой: параметры вещания конкретных каналов (протокол, мультикаст группа, протокол и проч.), планирование вещания (запросы переключение источников, вещательные плейлисты)
<i>Программа передач</i>	Интерфейс формирования и актуализации программы передач на вещаемые каналы

Разработанная подсистема управления IP-вещанием распадается на два основных компонента - абонентское и вещательное управление. Компоненты в свою очередь стыкуются с базой данных, которая, посредством различного рода интерфейсов, является связующим звеном как между этими компонентами, так и подсистемами в целом.

### 4.1.1 Абонентское управление

Как можно видеть из представленной диаграммы вариантов использования (рис.4.2), в подсистеме управления абонентами должны присутствовать интерфейсы добавления, редактирования и удаления абонентов, определения прав абонентов на использование вещания, интерфейс доступа к статистической информации системы вещания в целом и абонентской статистике.

В реализации часть интерфейсов целесообразно было объединить (см.рис.4.3). С помощью представленных интерфейсов может осуществляться полный цикл управления клиентами: добавление, редактирование, получение статистики, удаление.

### 4.1.2 Управление вещанием

Подсистема управление вещанием в свою очередь включает в себя компоненты управления источниками контента (приемным оборудованием), определение общих параметров безопасности системы (параметры скрамблирования на схеме) и формирование списка вещания с информационной поддержкой этого вещания (программа передач). На рис.4.4 показан разработанный интерфейс подсистемы управления вещанием, при использовании в качестве источника мультимедийных данных — спутниковое вещание. Таким образом настройка источников включает в себя конфигурацию собственно приемного оборудования (модем DVB-S), внесение информации о спутниках и транспондерах, доступных для использования в вещании (рис.4.4а и 4.4б), формирования используемых сетевых каналов для IP-вещания (рис.4.4в), а также составление списка вещания, т.е. связь программ конкретных транспондеров с конкретными сетевыми каналами вещания (рис.4.4г).

(a) Добавление абонента

(b) Поиск абонентов

(c) Редактирование контактных данных и прав абонента

(d) Получение общей статистики вещания

Рисунок 4.3 – Разработанные интерфейсы подсистемы абонентского управления

(a) Настройка доступных спутников

(b) Настройка доступных транспондеров

(c) Настройка сетевых каналов

(d) Настройка списка вещания

Рисунок 4.4 – Разработанные интерфейсы подсистемы управления вещанием

### 4.1.3 Вещательная база данных

Разработанные логические структуры базы данных для использования в рамках подсистем управления абонентами и вещание представлены на рис.4.5 и рис.4.6 со спецификациями в таблицах 4.2 и 4.3 соответственно.

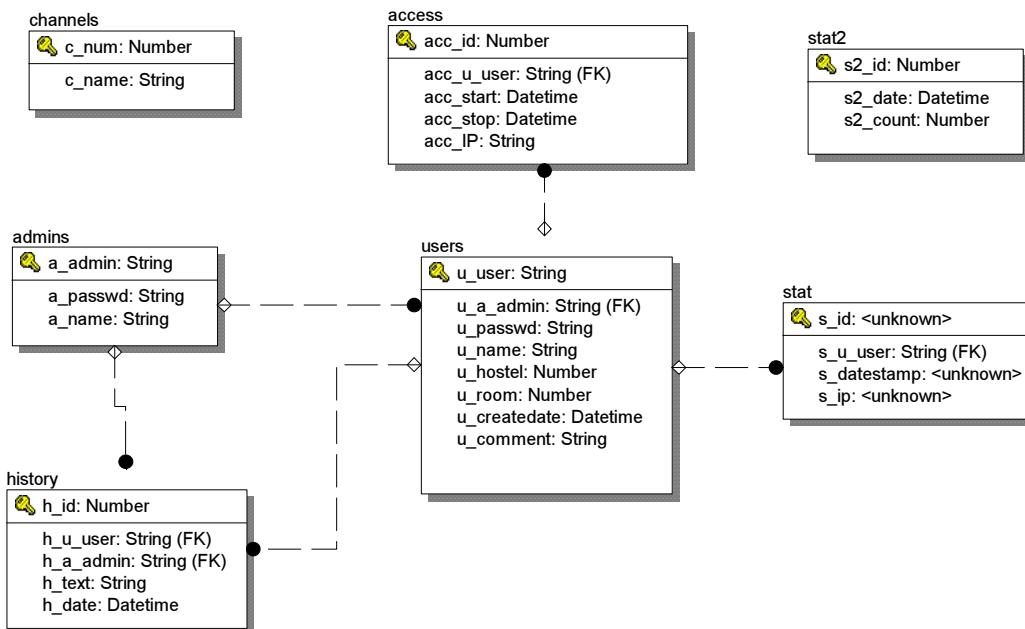


Рисунок 4.5 – Логическая модель базы данных управления пользователями

Таблица 4.2 – Спецификация логической модели базы данных управления пользователями

Наименование	Примечание
channels	Таблица информации о текущих вещаемых каналах
c_num	Внутренний идентификатор канала в системе
c_name	Название канала
access	Таблица назначения пользователям (абонентам) прав использования вещания
acc_id	Идентификатор записи
acc_u_user	Внешний ключ, идентификатор абонента
acc_start	Начало действия правила
acc_stop	Окончания действия правила
acc_IP	IP адрес, с которого абоненту в определенные рамки разрешено использование вещания
admins	Таблица идентификационной информации администраторов (операторов) системы вещания
a_admin	Идентификатор администратора
a_passwd	Пароль доступа
a_name	Контактная информация

Продолжение таблицы 4.2

Наименование	Примечание
users	Таблица идентификационной информации о пользователях (абонента) системы
<i>u_user</i>	Идентификатор пользователя
<i>u_a_admin</i>	Внешний ключ, идентификатор администратора, в зоне ответственности которого находится абонент
<i>u_passwd</i>	Пароль доступа
<i>u_name</i>	Контактная информация
<i>u_hostel</i>	Номер общежития
<i>u_room</i>	Номер комнаты
<i>u_createdate</i>	Дата заключения договора
<i>u_comment</i>	Дополнительная информация по пользователю
history	Таблица отслеживания изменения прав и идентификационной информации пользователей
<i>h_id</i>	Внутренний идентификатор
<i>h_u_user</i>	Внешний ключ, идентификатор пользователя
<i>h_a_admin</i>	Внешний ключ, идентификатор администратора, осуществлявший изменение
<i>h_text</i>	Тип изменения
<i>h_date</i>	Дата изменения
stat	Таблица статистической информации по пользователю
<i>s_id</i>	Внутренний идентификатор
<i>s_u_user</i>	Внешний ключ, идентификатор пользователя
<i>s_timestamp</i>	Время использования вещания
<i>s_ip</i>	IP адрес, с которого было использование вещания
stat2	Таблица интегративной информации использования вещания
<i>s2_id</i>	Внутренний идентификатор
<i>s2_date</i>	Дата и время осуществления сбора информации
<i>s2_count</i>	Количество абонентов, использующих вещания на момент времени <i>s2_date</i>

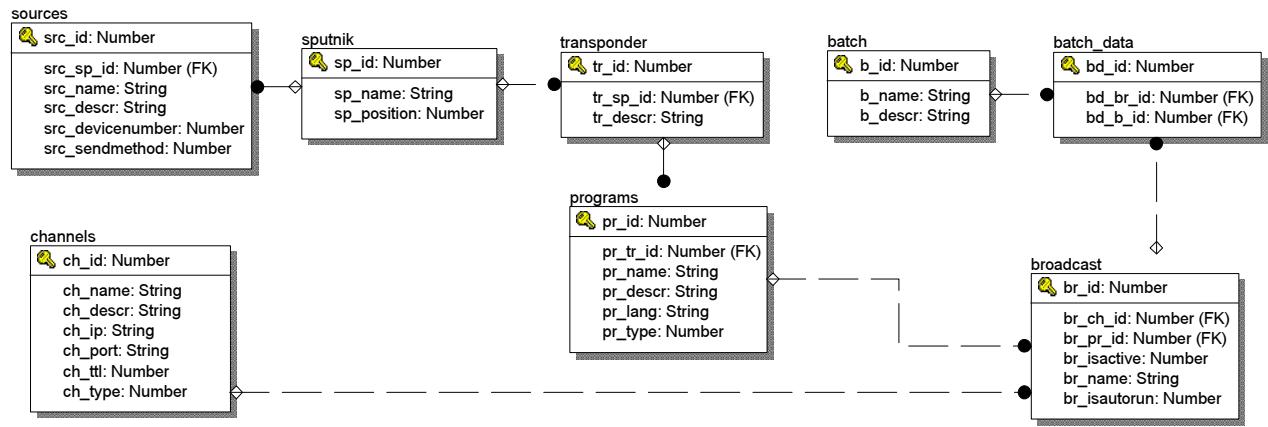


Рисунок 4.6 – Логическая модель базы данных управления вещанием

Таблица 4.3 – Спецификация логической модели базы данных управления вещанием

Наименование	Примечание
sputnik	Таблица спутников, используемых для получения контента
sp_id	Идентификатор спутника в системе
sp_name	Название спутника
sp_position	Позиция спутника
sources	Таблица приемного оборудования (DVB-S модемы)
src_id	Идентификатор оборудования
src_sp_id	Внешний ключ, идентификатор спутника, на который настроена антенна, подключенная к данному DVB-S модему
src_name	Модель модема
src_descr	Место установки модема
src_devicenumber	Номер слота установки
src_sendmethod	Тип работы модема
transponder	Таблица транспондеров, используемых для получения контента
tr_id	Идентификатор транспондера в системе
tr_sp_id	Внешний ключ, идентификатор спутника, к которому относится транспондер
tr_descr	Описание транспондера
programs	Таблица источником контента (программ), доступных для использования в процессе вещания
pr_id	Внутренний идентификатор программы
pr_name	Название программы
pr_desc	Описание программы
pr_lang	Язык программы

Продолжение таблицы 4.3

Наименование	Примечание
<i>pr_type</i>	Тип программы
channels	Таблица сетевых каналов вещания
<i>ch_id</i>	Внутренний идентификатор
<i>ch_descr</i>	Описание
<i>ch_ip</i>	Адрес мультикаст группы
<i>ch_port</i>	Порт
<i>ch_ttl</i>	TTL
<i>ch_type</i>	Тип
broadcast	Таблица формирования текущего вещания
<i>br_id</i>	Внутренний идентификатор
<i>br_ch_id</i>	Внешний ключ, идентификатор сетевого канала
<i>br_pr_id</i>	Внешний ключ, идентификатор источника контента (программы)
<i>br_isactive</i>	Флаг активности элемента вещания
<i>br_name</i>	Описание
<i>br_isautorun</i>	Флаг автозапуска элемента вещания
batch	Таблица групповых заданий включения/выключения элементов вещания
<i>b_id</i>	Внутренний идентификатор группового задания
<i>b_name</i>	Название
<i>b_descr</i>	Описание
batch_data	Таблица связи групповых заданий с таблице формирования вещания (связь многие-ко-многим)
<i>bd_id</i>	Внутренний идентификатор
<i>bd_br_id</i>	Внешний ключ, идентификатор в таблице формирования вещания
<i>bd_b_id</i>	Внешний ключ, идентификатор группового задания

Описанные выше интерфейсы вкупе с базой данных обеспечивают возможность конфигурирования системы в целом, а также осуществлять оперативный контроль работы отдельных элементов системы с целью поддержания и повышения качества работы системы. Сама по себе система управления не существует без объекта управления, которым в IP-вещании является контент, проходящий этапы формирования, передачи и отображения в рамках соответствующих подсистем.

## 4.2 Подсистема формирования контента распределенной системы IP-вещания

Началом цикла работы системы IP-вещания (под управлением подсистемы управления) является формирование контента, который в исходной форме чаще всего является внешним компонентом по отношению к системе вещания (исключение - формируемый в рамках системы контент). В качестве таких внешних компонент могут выступать:

1. Цифровое спутниковое/кабельное/эфирное вещание в формате DVB-S/C/T соответственно.
2. Аналоговое вещание, либо аналоговые источники мультимедийных данных (видеокамеры, видеомагнитофоны) в формате PAL/SECAM/NTSC.
3. Файловые источники мультимедийных данных (DVD, AVI и MP4 файлы).

Кроме трех указанных выше внешних компонент, в рамках распределенной вещательной сети появляется четвертых основополагающий внутренний компонент: *источник в виде данных IP-TV вещания*, с помощью которого осуществляется реализация принципа распределенности вещания на подсистемном уровне.

В разделе 2 было дано обоснование использования в качестве формата представления мультимедийных данных MPEG-4 AVC/H.264 стандарта, обеспечивающего в настоящее время лучшее соотношение качества кодирования естественного изображения к требуемому потоку данных. Поэтому непосредственное использование получаемых от ряда источников данных является неприемлемым (цифровые форматы вещания в настоящий момент в большей степени используют MPEG-2, а аналоговое вещание по определению необходимо перевести в цифровую форму, см.п.1.2) и требует перекодирования в нужный формат. Дополнительно к этому, в реализации системы защиты от несанкционированного доступа (см.раздел 3) необходима дополнительная модификация (скрамблирование) мультимедийных данных непосредственно перед его распространением по сети передачи данных.

Процесс формирования контента разбивается на ряд этапов: получение данных от источника, преобразование, формирование потока, пригодного для передачи в сетевую подсистему. Существование источников различного типа обуславливает создания подсистемы, незаточенной под определенный тип источников, а с возможностью интегрирования мультимедийных данных различного происхождения (гибридная подсистема формирования контента).

### 4.2.1 Базовые блоки подсистемы формирования контента

Произведя декомпозицию подсистемы формирования контента и ее этапов работы, был выделен набор базовых блоков (см. рис.4.7), которые можно разделить на две группы: блоки источников данных и блоки преобразования. Кроме того, при реализации подсистемы ЗНД появляются соответствующие блоки, которые также представляют из себя блок источников данных (сессионных ключей CW) и блок преобразований (непосредственное

скрамблирования потока мультимедийных данных).

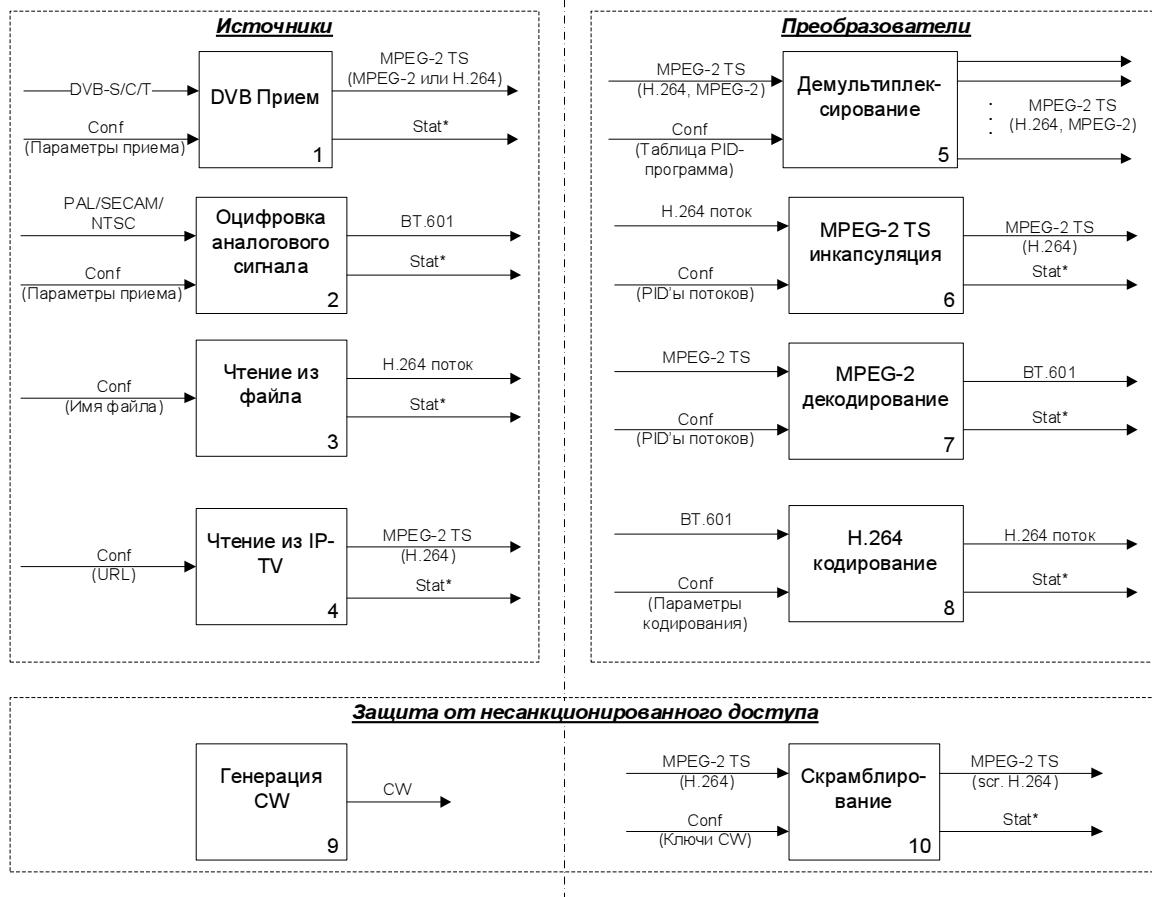


Рисунок 4.7 – Базовые компоненты подсистемы формирования контента IP-вещания

Комбинации базовых компонентов позволяют реализовать все необходимые элементы получения и преобразования необходимого контента. Например последовательное объединение блоков №№1, 5, 7, 8, 6 позволяет организовать открытое IP-вещания в формате H.264. Добавление блоков №№9, 10 позволит защитить либо частично, либо полностью вещания от доступа нелегальных пользователей. В реализации распределенной системы вещания особо важную роль играет блок №4, с помощью которого без использования дополнительных блоков (в т.ч. блоков скрамблирования) возможна реализация расширения зоны действия вещания, например в структуре сети представленной на рис.4.8. В представленной реализации системы имеются два сервера непосредственно формирующие контент (на основе спутникового DVB вещания и аналогового эфирного вещания), который распространяется по высокоскоростной магистральной сети оператора. IP-TV шлюзы, используя комбинации базовых блоков с использованием блока №4, осуществляют трансляцию исходного контента в менее скоростные сети. Трансляция может включать преобразование в меньший формат (IP-TV преобразователь на схеме) или формировать unicast передачу мультимедийных данных абонентам (см.п.4.3).

Практически каждый базовый блок помимо основной задачи (получения или преобразования данных) осуществляет сбор статистической информации (Stat\* на диаграмме рис.4.7). Реализация этого элемента блоков является optionalным, но крайне важным

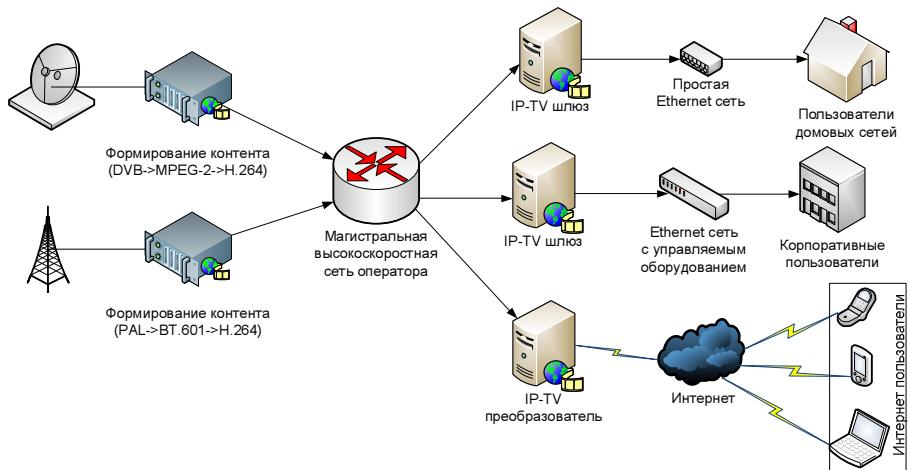


Рисунок 4.8 – Варианты реализации формирования и доставки контента до абонентов

элементом, предназначенным для контроля качества IP-TV вещания на каждом этапе работы. Например, в блоке №1 (DVB Прием) контрольная информация Stat\* может содержать данные о получаемом потоке данных и количестве ошибок приема, что в свою очередь позволит своевременно среагировать на сбой в системе IP-TV из-за каких либо проблем связанных с работой канала «Вещатель-Спутник-DVB Приемник».

#### 4.2.2 Компоненты формирования контента

Часть базовых блоков (например №1 и №2) возможно реализовать только с применением специализированного аппаратного обеспечения (см.п.4.2.3). Однако рамки этого аппаратного обеспечения могут распространяться как на весь блок в целом, так и на его часть. В первом случае реализуется законченное аппаратное устройство, сопрягающееся с остальной частью подсистемы по какому либо протоколу. В случае частичной аппаратной реализации блока, аппаратной основой является шасси ПК, в который установлена плата расширения PCI (для блока №1 это DVB-модем).

Из-за высоких требований к ширине канала протокола BT.601, целесообразным является реализация компонентов системы таким образом, чтобы сочленения потоков данных в формате BT.601 базовых блоков оставались внутри независимого компонента (программного, программно-аппаратного либо аппаратного).

С целью совместимости работы реализаций компонентов (набора базовых блоков), в качестве протокола их сочленения внутри подсистемы формирования контента предлагается использовать протокол TCP/IP. Формат реализации физического и канального уровня определяется построением подсистемы в целом. Таким образом, структура подсистемы формирования контента в случае ее построения из расчета на 2 канала с использованием оцифровки аналогового сигнала и без использования скрамблирования при реализации блоков в программном и программно-аппаратном виде будет выглядеть как показано на рис.4.9. Компонент №1 на схеме реализует базовые блоки оцифровки аналогового сигнала (например с использованием PCI TV тюнера) и H.264 кодирования обменом данными через разделяемую память. В показанной реализации H.264 кодирование вы-

полнено в качестве библиотеки, встраиваемой в компоненты подсистемы. Компонент №2 реализует только один базовый блок - MPEG-2 TS инкапсуляцию, получая и передавая данные по локальному TCP/IP сокету.

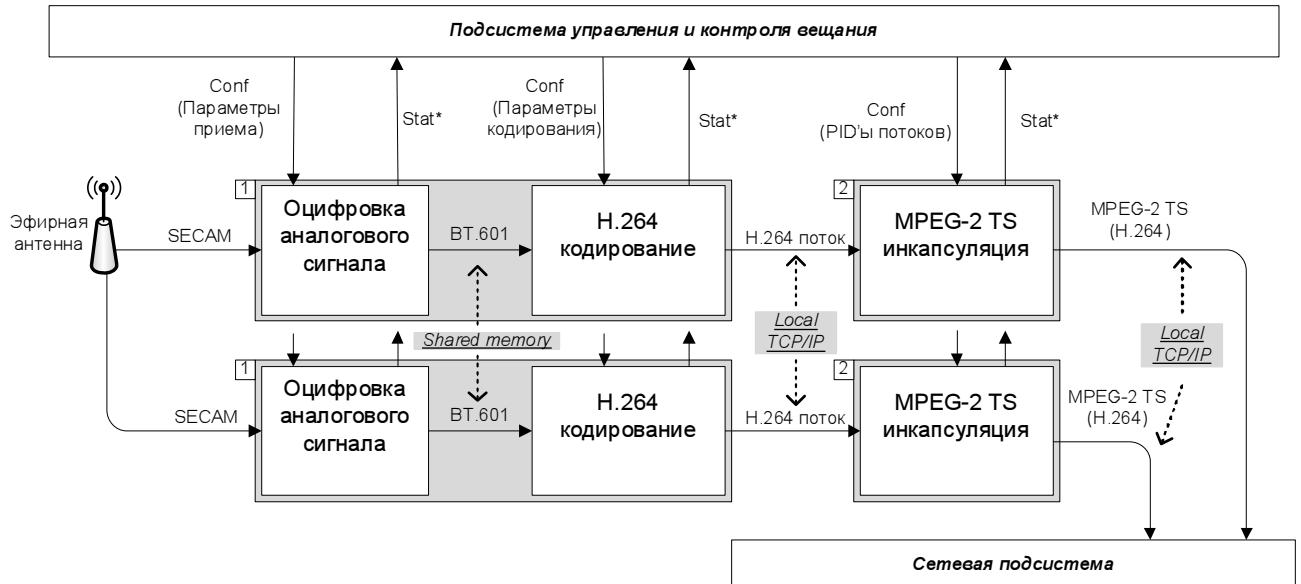


Рисунок 4.9 – Пример построения подсистемы формирования контента

Достоинством такого подхода является возможность свободной замены не только компонентов подсистемы однотипной реализации, но также возможно замены и взаимного использования компонентов различных реализаций (аппаратной, программной).

В общем виде, взаимодействие компонентов подсистемы формирования контента можно пояснить с помощью диаграммы взаимодействий на рис.4.10. Пояснения к используемым на схеме элементам приведено в табл.4.4.

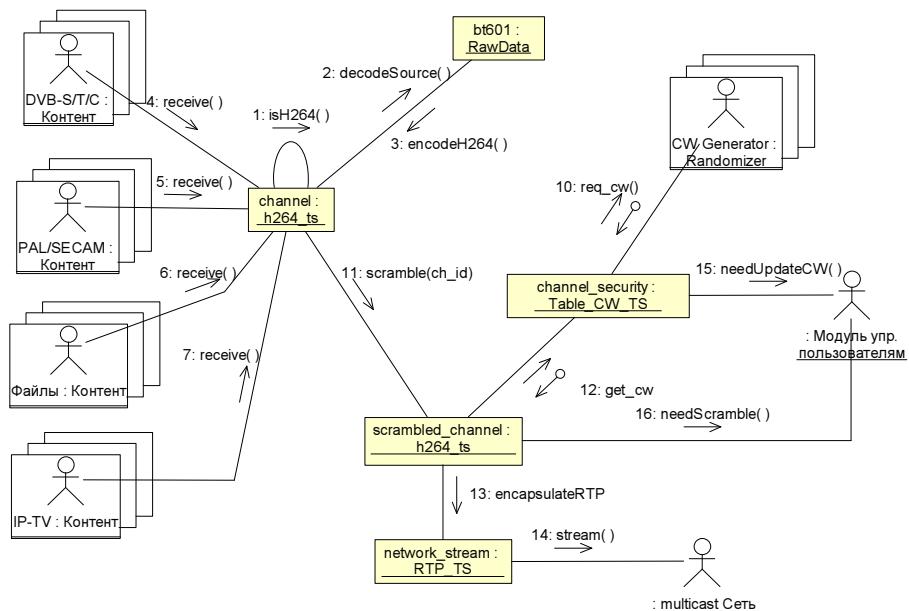


Рисунок 4.10 – Диаграмма взаимодействий подсистемы формирования контента

Таблица 4.4 – Спецификация диаграммы взаимодействий подсистемы формирования контента

Наименование	Примечание
DVB-S/T/C: Контент	Реализация получения контента в цифровом формате DVB-S/T/C
PAL/SECAM: Контент	Реализация получения контента в аналоговом формате PAL/SECAM
Файлы: Контент	Реализация получения контента на основе файлов
IP-TV: Контент	Реализация получения контента на основе IP-TV вещания
channel: h264_ts	Блок формирования MPEG-2 TS H.264 на основе получаемого контента
<i>receive()</i>	Операция запроса и получения контента от соответствующей реализации класса «Контент»
<i>isH264()</i>	Операция проверки полученного контента на соответствие формату MPEG-2 TS H.264 (нужна ли дополнительная конвертация)
<i>decodeSource()</i>	Операция декодирования полученного контента в формат BT.601
<i>encodeH264()</i>	Операция кодирования видео из формата BT.601 в MPEG-2 TS H.264
<i>scramble()</i>	Операция скрамблирования подготовленного MPEG-2 TS H.264 потока (формирование MPEG-2 TS scrambled H.264)
bt601: RawData	Буфер хранения видеоданных в формате BT.601
scrambled_channel: h264_ts	Блок представления канальных данных в скрамблированном виде
channel_security: Table_CW_TS	Блок поддержки и актуализации таблицы сессионных ключей скрамблирования канальных данных
<i>get_cw()</i>	Операция получения сессионного ключа для операции скрамблирования из таблицы сессионных ключей
CW Generator: Randomizer	Блок генерации сессионных ключей на основе генератора (псевдо)случайных чисел
<i>req_cw()</i>	Запрос на генерацию нового сессионного ключа
: Модуль упр. пользователями	Подсистема управления пользователями
<i>needUpdateCW()</i>	Интерфейсная функция запроса необходимости обновления сессионного ключа для скрамблирования канальных данных

Продолжение таблицы 4.4

Наименование	Примечание
<i>needScramble()</i>	Интерфейсная функция запроса необходимости скрамблирования канальных данных
<i>network_stream: RTP_TS</i>	Блок сетевого представления канальных данных
<i>encapsulateRTP()</i>	Процедура инкапсуляции исходного MPEG-2 TS (scrambled) H.264 потока в сетевое (RTP) представление
<i>:multicast Сеть</i>	Сетевая подсистема
<i>stream()</i>	Процедура передачи канальных данных из подсистемы формирования контента в сетевую подсистему

#### 4.2.3 Аппаратное обеспечение программно-аппаратных компонентов источников контента

Разработка аппаратных компонентов формирования контента является долговременной и дорогостоящей задачей. Более простая реализация заключается в применении программно-аппаратного подхода с использованием присутствующих на рынке ряде плат расширения ПК (USB, PCI, PCI-X и других), способных к получению (и, возможно, обработке) данных из различных источников: аналогового (эфирного, кабельного) телевидения и цифрового DVB-вещания.

##### 4.2.3.1 Оцифровка аналогового сигнала (без встроенного кодировщика)

В качестве оборудования для приема и оцифровки аналогового эфирного и/или кабельного телевидения можно рассмотреть недорогие и в настоящее время очень хорошо распространенные платы ТВ-тюнеров. ТВ-тюнер является полностью законченным устройством, реализующим все элементы базового блока №2 (оцифровка аналогового сигнала). Среди разнообразия ТВ-тюнеров подходящими в смысле применения для получения мультимедийного контента являются внутренние ТВ тюнера, подключаемые к ПК по шине PCI, поскольку обеспечивают возможность передачи необходимого информационного потока в формате BT.601 ( $\approx 160$  Мбит/с для видеопотока стандартного телевизионного качества) при использовании базового ПК в качестве шасси для нескольких компонентов формирования контента (2 и более ТВ-тюнеров в рамках одного ПК).

Обобщенная функциональная схема плат расширения, предназначенных для приема аналогового эфирного и кабельного телевидения представлена на рис.4.11.

Основными элементами, как видно из схемы, являются блок приема высокочастотного сигнала, имеющий встроенный стандартный RCA разъем для подключения антенны, декодер видео и звука с функциями мастера на шине PCI, EEPROM для хранения конфигурационной информации, а также цепи регулирования электропитания.

В качестве питающих напряжений обычно используются разделенные на цифро-

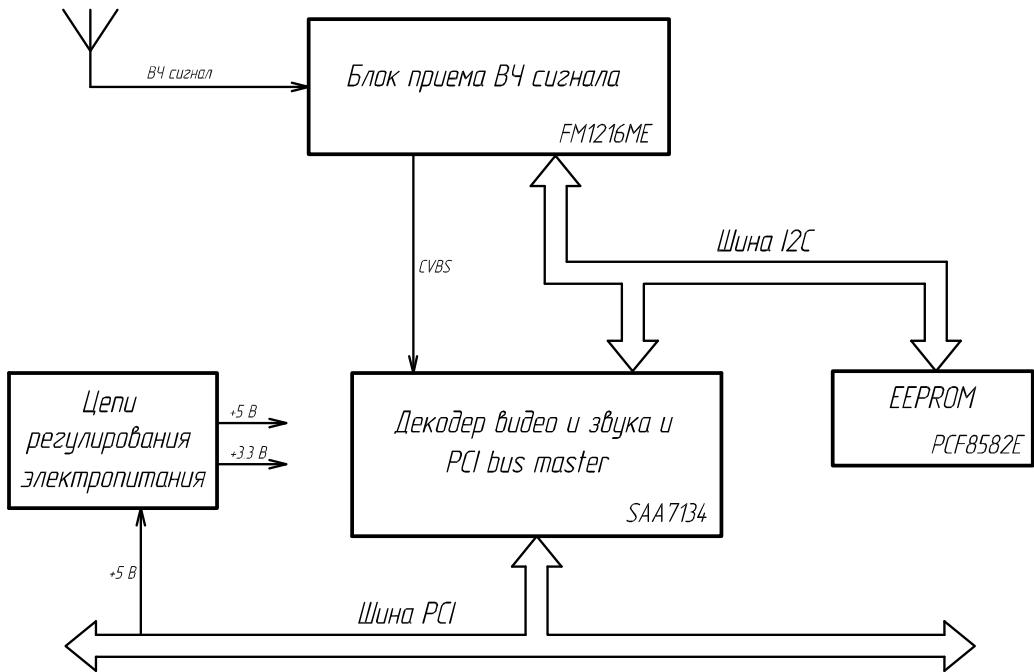


Рисунок 4.11 – Функциональная схема аналогового ТВ тюнера

вую и аналоговую части 3.3В и 5В. Взаимодействие ВЧ блока, декодера видео и звука и EEPROM осуществляется посредством двухпроводной шины I<sup>2</sup>C [30].

### Особенности

В качестве особенностей ТВ-тюнеров относительно мультимедийного вещания можно выделить следующие:

- в ряде ТВ-тюнеров на PCI шину передаются только видеоданные, таким образом, необходимо внимательно изучить возможности конкретного ТВ тюнера, перед непосредственным задействованием его в системе IP-вещания;
- видеоданные передаются в несжатом виде (BT.601), что с одной стороны негативно сказывается на информационной нагрузженности самой PCI шины, а с другой стороны требует дополнительных аппаратных (процессорное время, оперативная память) и программных (алгоритмы, реализованные в программах) ресурсов для необходимой компрессии исходного потока видеоданных в H.264 (т.е. реализация базового блока №8 в рамках компонента формирования контента);
- + все платы ТВ тюнеров позволяют производить «захват» не только телевизионных передач, идущих в эфире или по кабельному телевидению, но также предоставляют возможность «захватывать» поступающий сигнал по низкочастотному входу (выход видеомагнитофона, выход различных аналоговых видеокамер и проч.), что расширяет возможности применения этих устройств при вышеуказанных ограничениях;
- + некоторые платы ТВ тюнеров имеют возможность получения эфирных радиостанций.

#### 4.2.3.2 Оцифровка аналогового сигнала (со встроенным кодировщиком)

Кроме обычных ТВ-тюнеров на рынке присутствуют ТВ-тюнеры и специализированные устройства оцифровки аналогового сигнала со встроенным аппаратным кодировщиком H.264. Такие устройства являются уже практически полностью законченными компонентами (аналог компонента №1 на рис.4.9). На долю программной реализации для этого компонента остается конфигурация устройства (установка необходимых параметров приема и кодирования) и реализация интерфейса получения данных с устройства. Достоинством специализированных устройств по сравнению с ТВ-тюнерами является возможность оцифровки и кодирования сразу нескольких видео потоков одновременно (4 и более).

Обобщенная функциональная схема оборудования оцифровки и H.264 кодирования представлена на рис.4.12.

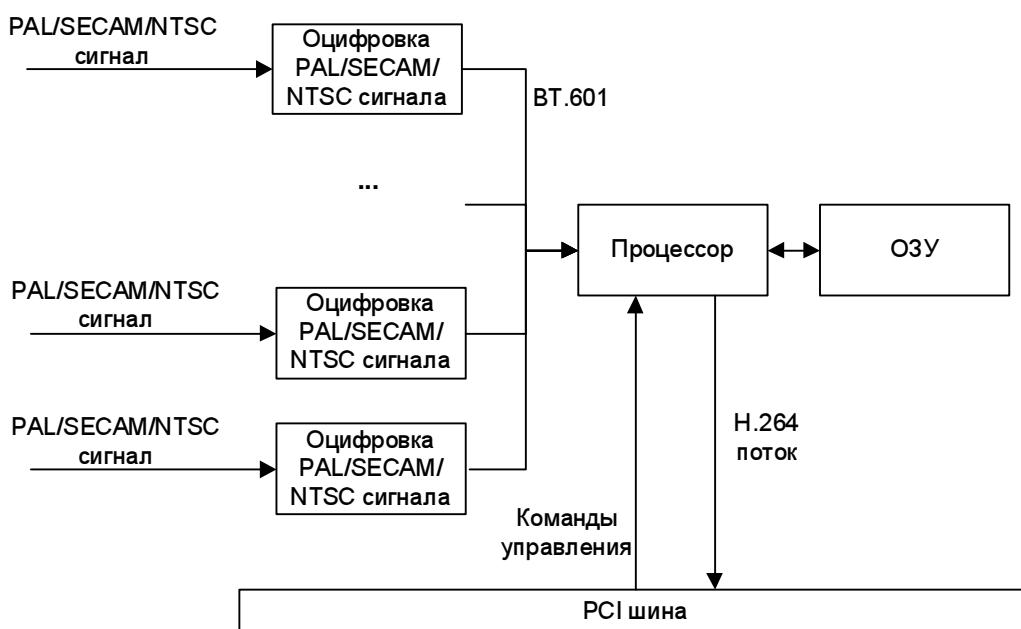


Рисунок 4.12 – Функциональная схема платы захвата с аппаратным MPEG кодированием

Подход объединения оцифровки и кодирования нескольких аналоговых видеопотоков в рамках одной платы расширения обуславливается оптимальным распределением ресурсов (оптимизация соотношения количества занятых PCI слотов к используемой пропускной способностью шины) персонального компьютера, куда устанавливается плата расширения.

#### Особенности

В качестве особенностей данного вида оборудования необходимо отметить следующее:

- использование преконфигурированных параметров оцифровки и кодирования в присутствующих на рынке специализированных плат оцифровки и кодирования и малая, а иногда и вовсе отсутствие возможности по влиянию на выходное качество кодированного видеоизображения и звука;

- плохая или отсутствующая поддержка драйверов для альтернативных операционных систем (например Linux) и необходимость реализации компонентов формирования контента в рамках операционной системы Windows;
- + малая загрузка центрального процессора, задачи оцифровки аналогового сигнала и H.264 кодирования реализуются ресурсами платы расширения без задействования системных ресурсов;
- + возможность одновременной оцифровки и кодирования множества аналоговых источников мультимедийного контента.

#### **4.2.3.3 Прием цифрового эфирного, кабельного и спутникового телевидения**

Наиболее привлекательными с точки зрения доступного мультимедийного контента являются платы для приема цифрового эфирного, кабельного и спутникового телевидения. Если для первых двух случаев (эфирное и кабельное цифровое телевидение) пока не создана (но активно в настоящее время создается) инфраструктура мультимедийного контента, то в случае со спутниковым телевидением таковое имеется. Сейчас практически все поставщики спутниковых мультимедийных данных перешли на цифровую форму вещания в формате MPEG-2 и постепенно переходят на H.264 кодирования с целью более эффективного использований спутникового ресурса. Использование цифровой формы вещания является с одной стороны экономичным решением - меньшие требования к полосе частот, а следовательно меньшие расходы на аренду спутникового ресурса, а с другой стороны - большие возможности по защите мультимедийной информации от несанкционированного использования. Если в случае аналогового сигнала существовали методы по шифрованию исходного сигнала хотя и сложными, но достаточно примитивными алгоритмами (перестановки строк кадра, подавление или внесение ложных синхроимпульсов и проч.), то в случае цифровых данных открылась масса возможностей в данном направлении (симметричное/асимметричное шифрование), чем не преминули воспользоваться разработчики систем безопасности.

Принципиальное различие между приемниками цифрового эфирного, кабельного и спутникового телевидения заключается лишь в реализации высокочастотного блока и методов взаимодействия с приемной антенной. Все остальные блоки и функциональные узлы одинаковы у всех типов устройств данного класса. Поэтому в качестве обобщенной структуры можно рассмотреть функциональную схему PCI приемника цифрового спутникового телевидения (рис.4.13).

На вход тюнера поступает сигнал с приемного устройства спутникового канала. Этот сигнал идет на несущей частоте, находящейся в диапазоне 950-2150 ГГц, перенос на которую осуществляется в преобразователе, расположенному непосредственно у приемной антенны. Тюнер так же переносит сигнал с несущей частоты на промежуточную частоту. Управление выбором режима настройки работы и настройкой на канал осуществляется по шине I<sup>2</sup>C.

ВЧ блок преобразует колебания электромагнитных волн, полученных с антенны в транспортный поток MPEG (MPEG TS). Блок управления приемом обладает возможно-

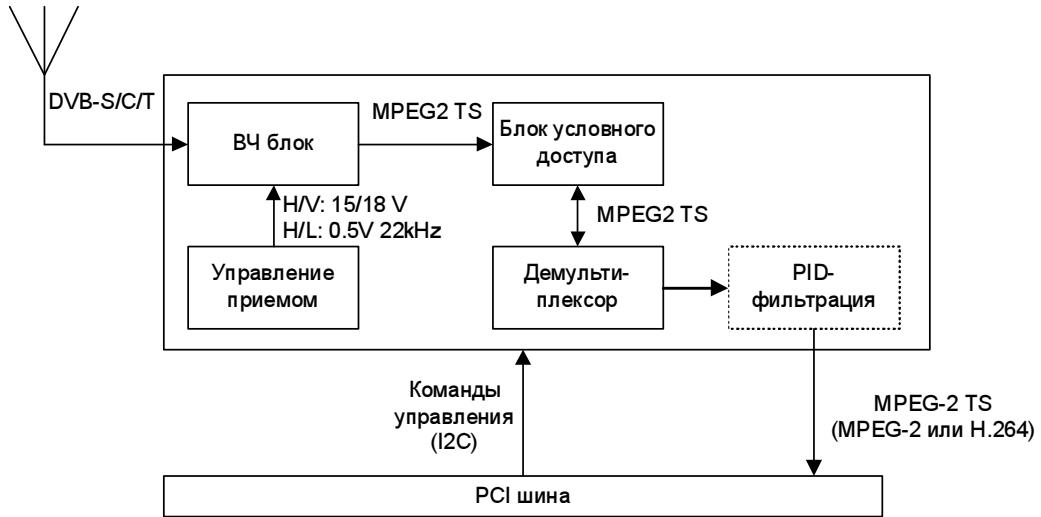


Рисунок 4.13 – Функциональная схема спутникового приемника DVB-S

стью задания поляризации конвертора (вертикальная/горизонтальная или круговая правая/левая), переключения между различными гетеродинами конвертора (верхний/нижний диапазон), а также возможностью управления механизмом переключения спутников (DISEQ) и переориентирования спутниковой тарелки на разные спутники (мультифид).

Далее транспортный поток MPEG проходит блок условного доступа, в рамках которого производится дескрамблование защищенного мультимедийного контента. В части спутникового оборудования данная подсистема может отсутствовать, тем самым пропадает возможность получения зашифрованных каналов. После блока условного доступа поток, в зависимости от типа используемого оборудования, может быть либо передан целиком на шину PCI для дальнейшего программного разделения, либо передан блоку демультиплексора, где производится соответствующая фильтрация транспортного потока, вычленение заданных потоков и передача уже вычлененных потоков на PCI шину.

Поскольку большинство вещаемых в текущий момент телепрограмм в цифровом формате представляют собой поток MPEG-2 данных, то непосредственное их использование в рамках IP-вещания нецелесообразно и необходима дополнительная переконвертация в H.264. Часть процесса перекодирования (декодирование исходного MPEG-2) может быть реализована с помощью доступных на рынке плат расширения, имеющих на борту дополнительный компонент: блок аппаратного декодирования MPEG-2. Дальнейшая обработка декодированных данных (BT.601 потока) может быть либо программно, либо аппаратно скжата в H.264 поток с необходимыми параметрами сжатия.

### Особенности

В качестве особенностей данного типа оборудования необходимо отметить следующие:

- + принимаемый мультимедийный контент может находиться в необходимом сжатом цифровом виде (H.264), одна плата является полностью законченным компонентом формирования контента;
- + в некоторых моделях используемого оборудования (например, TT-PCLine Budget

ТТ-1400) есть возможность получения для дальнейшей обработки всего транспортного потока с транспондера, что позволяет осуществить одновременное получение не одного, а нескольких мультимедийных потоков данных, что является серьезным преимуществом данного типа оборудования.

- вещание в формате H.264 на настоящий момент не является превалирующим и присутствует только в ограниченном количестве. Для использования в IP-вещании таких данных необходимо реализовывать блоки перекодирования из MPEG-2 в H.264;

#### 4.2.4 Исследование реализаций компонентов для мультимедийного вещания

Выбор структуры (набор базовых блоков) и способа реализации (программный, программно-аппаратный) компонентов системы мультимедийного вещания необходимо начинать с анализа доступных источников мультимедийного контента.

В случае необходимости использования аналоговых мультимедийных данных в качестве источника контента, то структура компонента формирования контента должна состоять из трех базовых блоков: блок оцифровки аналогового сигнала, блок H.264 кодирования и блок MPEG-2 TS инкапсуляции (рис.4.14).

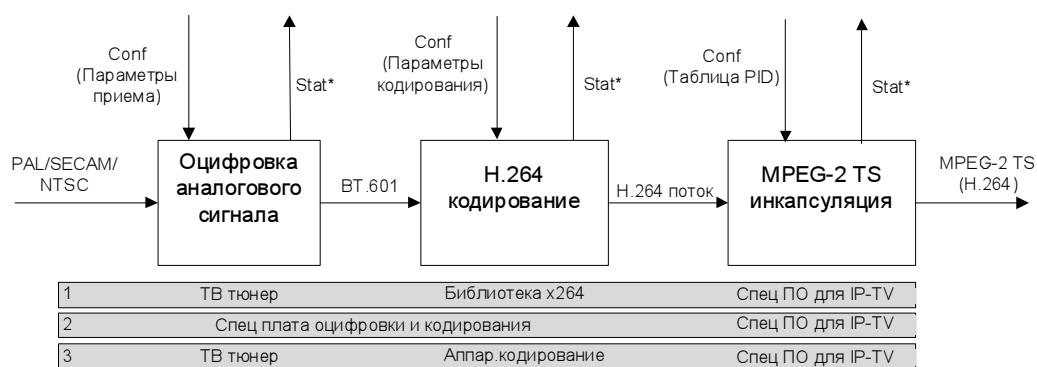


Рисунок 4.14 – Варианты реализации формирования контента на основе аналогового вещания

Существует несколько видов реализации блоков:

1. ТВ тюнер, программное сжатие с помощью библиотеки x264, программная инкапсуляция в MPEG-2 TS с помощью специализированного ПО;
2. специализированная плата оцифровки и кодирования x264 с программной инкапсуляцией в MPEG-2 TS с помощью специализированного ПО;
3. ТВ тюнер, аппаратное сжатие с помощью платы расширения, программная инкапсуляция в MPEG-2 TS с помощью специализированного ПО.

Вариант №1 позволит формировать одновременной от 1 до 4 (в зависимости от параметров кодирования) в рамках одного базового ПК из-за больших требований к процессорному времени у процесса H.264 кодирования. Для получения большего числа различного контента необходимо применять специализированные платы либо только для процесса H.264 кодирования (вариант №3), либо для всего процесса оцифровки и кодирования

(вариант №2).

При использовании в качестве источника спутниковое вещание, процесс формирования распадается на два принципиально различных элемента: без необходимости перекодирования (источник в H.264 формате) и с необходимостью перекодирования (источник в MPEG-2 формате). Необходимый набор базовых блоков в компонентах представлены на рис.4.15 и 4.16 соответственно.

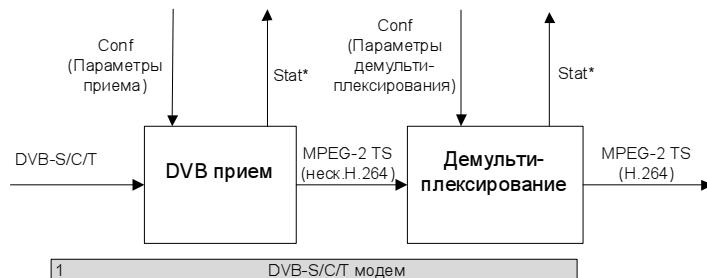


Рисунок 4.15 – Варианты реализации формирования контента на основе цифрового вещания в формате H.264

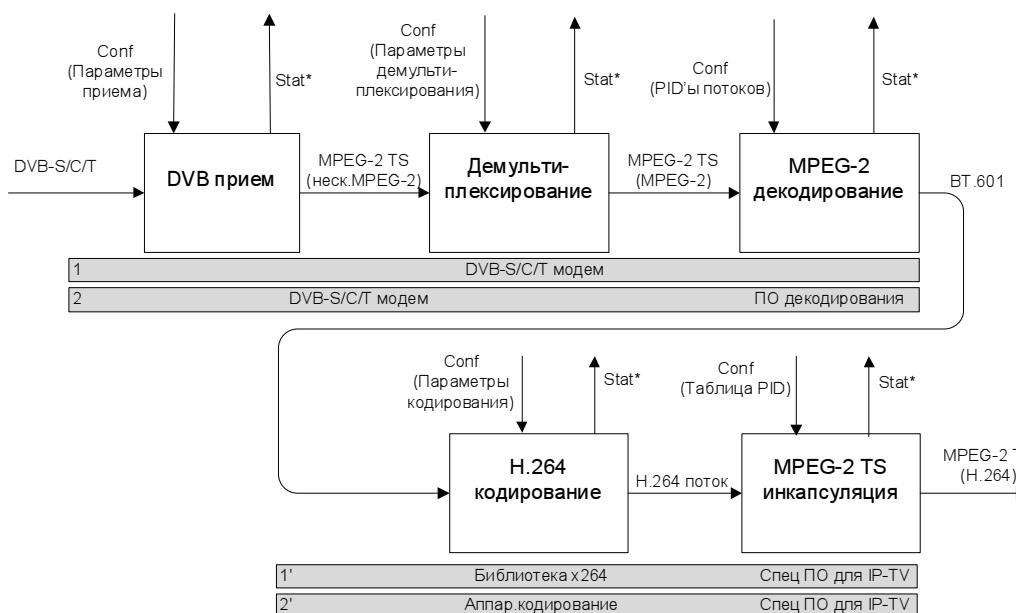


Рисунок 4.16 – Варианты реализации формирования контента на основе цифрового вещания в формате MPEG-2

Варианты реализации в случае использования источника в H.264 формате ограничиваются применением дешевого DVB-модема, реализующий все необходимые базовые блоки.

В случае необходимости перекодирования появляется набор вариантов:

- 1-1'. Дорогой DVB-модем с аппаратным MPEG-2 декодированием, программное кодирование в H.264 с помощью библиотеки x264, инкапсуляция в MPEG-2 TS с помощью специализированного ПО
- 1-2'. Дорогой DVB-модем с аппаратным MPEG-2 декодированием, аппаратное сжатие в H.264 с помощью платы расширения, инкапсуляция в MPEG-2 TS с по-

мощью специализированного ПО

- 2-1'. Дешевый DVB-модем, программное декодирование MPEG-2, программное кодирование в H.264 с помощью библиотеки x264, инкапсуляция в MPEG-2 TS с помощью специализированного ПО
- 2-2'. Дешевый DVB-модем, программное декодирование MPEG-2, аппаратное сжатие в H.264 с помощью платы расширения, инкапсуляция в MPEG-2 TS с помощью специализированного ПО

Самым эффективным относительно использования системных ресурсов является вариант реализации №1-2', но он имеет ограничение на работу только с одним исходным каналом на DVB-модем. Преодоление этого ограничение можно осуществить либо за счет системных ресурсов (вариант №2-2'), либо за счет применения специализированных плат MPEG-2 декодирования (модифицированный вариант №2-2').

Использование в качестве источника мультимедийного контента данные самого IP-вещания приводит к структуре компонента, состоящего только из одного базового блока с единственным вариантом программной реализации (рис.4.17). Это еще раз показывает достоинство распределенной (GRID-) сети вещания, в которой сложное и дорогое оборудования формирования контента из исходной формы (аналоговое или цифровое вещания) устанавливается в различных точках сети используя различные источники финансирования (например, единое вещательное поле формируется за счет средств нескольких операторов домовых сетей), а фактическое распределение мультимедийного вещания осуществляется посредством IP-TV шлюзов с реализованными программными компонентами получения контента из IP-TV сети.

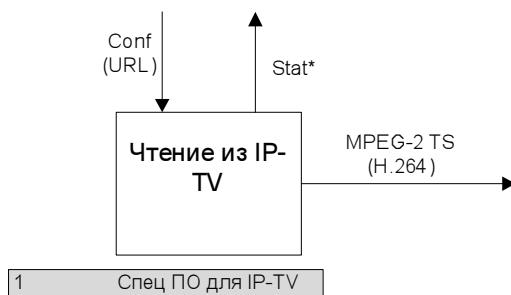


Рисунок 4.17 – Вариант реализации формирования контента на основе IP-TV вещания

### 4.3 Сетевая подсистема распределенной системы IP-вещания

Задача передачи данных из подсистемы формирования контента в абонентскую полностью лежит на сетевой подсистеме. Подсистема управления и контроля осуществляет лишь конфигурацию сети (настройку параметров приоритетизации трафика — QoS [3]), мониторинг и своевременное извещение оператора о проблемах в сетевой подсистеме. В п.1.1.1 были определены две возможные схемы доставки данных в рамках IP-сети: юникаст (unicast, точка-точка) и мультикаст (multicast, точка-многоточка). Однако использование только какой то одной схемы будет вступать в противоречия (п.1.1.2) либо с желаниями

оператора, либо абонентов относительно IP-вещания.

Применение технологии юникаст технологии позволяет максимально защитить систему от несанкционированного доступа (посредством выделения отдельного виртуального, в т.ч. шифрованного канала передачи), однако вступает в противоречие либо с качеством изображения, либо с количеством одновременно подключенных пользователей. Другими словами, не жертвуя качеством передаваемого мультимедийного контента (1-2 Мбит/с для стандартного телевизионного качества в H.264 формате), будет ограничено общее количество одновременно подключенных пользователей в сети (в случае использования сети 100BaseTX количество одновременно подключенных абонентов не превышает 50-80), т.е. неприемлемо для оператора. С другой стороны, ухудшение качества (ширина канала канал 0.4-0.7 Мбит/с и меньше) будет неприемлемо для абонентов.

Использование только технологии мультикаст, решая проблемы качества каналов и количество работающих абонентов, создает ряд других проблем: необходимость наличия каналаобразующего оборудования, поддерживающего технологию мультикаст (IGMP маршрутизацию или IGMP Snooping) и технологию QoS для обеспечения необходимого уровня качества доставки данных с серверов оператора до абонентов, а также проблему защиты системы вещания от несанкционированного доступа. В принципе, последняя проблема решается чисто мультикаст-подходом в рамках DVB-технологии (см.п.[3.1](#)), однако требует наличия у абонента идентификационного оборудования (смарт-карты и блоки условного доступа), что затрудняет или сводит на нет использования вещания в рамках персонального компьютера (не используя приставки STB).

#### **4.3.1 Гибридная схема доставки мультимедийных данных**

Разрешение определенных выше противоречий лежит в использовании гибридной схемы доставки данных в рамках сети передачи данных, включая гибридную модель защиты от несанкционированного доступа (см.п.[3.2](#)). Смысл гибридности доставки данных заключается в использовании как мультикаст-распространения данных там где это возможно (например магистральная сеть оператора, построенная на высокоскоростном оборудовании поддерживающем все необходимые технологии) и юникаст технологий там, где мультикаст использовать нецелесообразно (домовые и офисные сети, построенные на базе неуправляемых коммутаторов (switch) и накопителей (hub)). Если попытаться в такой сети запустить мультикаст вещание, то это будет означать уменьшение общей пропускной способности сети на ширину этого мультикаст вещания, причем качество доставки данных до абонентов будет невозможно гарантировать (потери пакетов, а следовательно неприемлемое качество сервиса). На рис.[4.18](#) показана гибридная архитектура сетевой подсистемы мультимедийного вещания.

В рамках гибридной архитектуры можно выделить три класса пользователей:

1. Пользователя мультикаст сети
2. Пользователи юникаст сети
3. Интернет пользователи

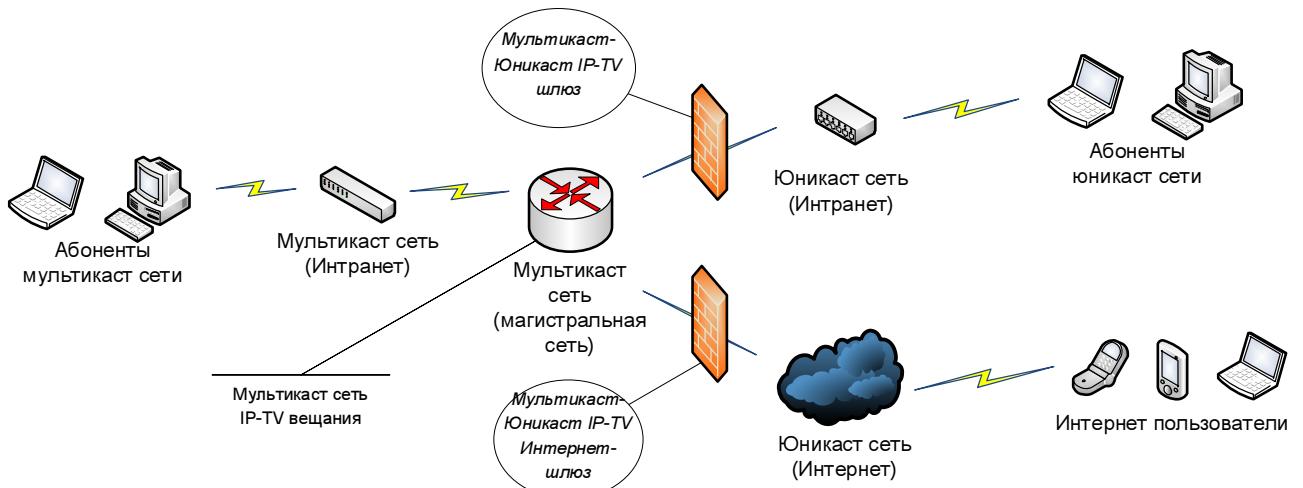


Рисунок 4.18 – Гибридная архитектура сетевой подсистемы мультимедийного вещания

Каждый из классов пользователь должен быть обеспечен максимально возможным качеством сервиса. Первая группа обладает максимальными возможностями, по определению полностью используя возможности магистральной вещательной сети (доступ ко всем каналам с максимальным качеством без ограничения на количество работающих абонентов). Вторая группа обеспечивается подмножеством сервисов, предоставляемых магистральной сетью. Ограничения в данном случае касаются на возможный выбор каналов, а также ограничения, связанные с количеством одновременно работающих абонентов, которые снимаются с помощью использования достаточного количества мультикаст-юникаст IP-TV шлюзов и сегментацией сети. Третья группа пользователей является обособленной, поскольку позволяет предоставлять сервис IP-TV вещания не только в рамках инфраструктуры конкретной сети передачи данных, а в рамках сети Интернет. В данном случае основным ограничением является ширина каналов доступа, поэтому необходимо применение достаточного числа IP-TV Интернет шлюзов, обеспечивающих конвертацию видео потоков исходного качества в поток с приемлемыми для Интернет вещания скоростными характеристиками (50-200 Кбит/с), существенно ухудшая тем самым качество вещания.

#### 4.3.2 Протоколы работы сетевой подсистемы мультимедийного вещания

В работу сетевой подсистемы мультимедийного вещания вовлечены все другие подсистемы (управления и контроля, формирования контента и абонентская). Сама работа в рамках сети представляет собой ряд отдельных процессов:

- Сбор статистической информации по работе подсистем системы мультимедийного вещания (мгновенный и суммарный трафик, ошибки и сбои формирования, пакетизации и передачи контента в сеть, качество приема вещания абонентами).
- Пакетизация сформированного контента и формирование вещательного поля.
- Доступ абонентов к ресурсам вещания:
  - Установление соединения (аутентификация, авторизация).
  - Получение мультимедийных данных, которые могут быть скрамбли-

рованы.

- Получение ключей дескрамблирования мультимедийных данных (если нужны)

В основу сбора статистической информации ложится протокол SNMP, предоставляющий возможности одновременно и мониторинга сетевого оборудования и его управления. Доступное программное обеспечение (MRTG, rrdtool) позволяет без создания дополнительного программного обеспечения реализовать визуализацию сетевых событий по временной шкале (текущий трафик, количество работающих абонентов, количество ошибок приемо-передачи данных), а также уведомления оператора о различного рода событиях (пропадания связи с серверами вещания, выход из строя сегментов сети и т.п.). Другими словами подсистема контроля (обратная связь из подсистем) реализуется посредством SNMP протокола с применением программных средств визуализации и уведомления MRTG и/или rrdtool.

#### 4.3.2.1 Протокол передачи мультимедийных данных

В качестве протокола передачи мультимедийных данных в рамках мультикаст сетей целесообразно использовать специализированный протокол RTP, предназначенный для передачи критических к временным задержкам данных (в нашем случае - потоковое видео).

Протокол RTP представляет собой надстройку над транспортным протоколом и в рамках IP сетей работает поверх протокола UDP/IP, может работать как в юникаст, так и в мультикаст сетях [31]. Дополнительный протокол RTCP (Real Time Control Protocol) реализует возможность мониторинга и контроля качества принимаемых данных на стороне клиента, таким образом формируя обратную связь с подсистемой контроля и управления.

Поскольку протокол RTP является надстройкой над UDP, то он добавляет ряд служебных данных (RTP-заголовок) к каждому посылаемому пакету. Определение заголовка RTP пакета в общем виде показано на рис.4.19.

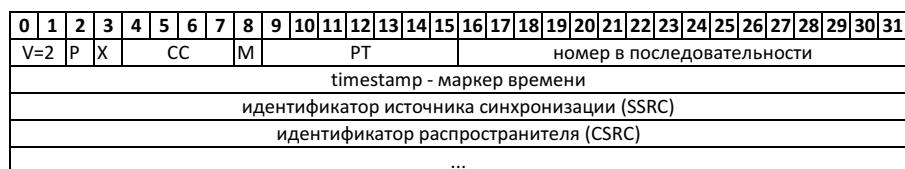


Рисунок 4.19 – Формат заголовка RTP пакета

Первые 12 байт (октетов) присутствуют в каждом RTP пакете, список идентификаторов CSRC присутствует только в случае добавления RTP-микшером. Поля заголовка RTP имеют следующий смысл:

**версия (V): 2 бита** — поле, идентифицирующее версию RTP протокола. Последней спецификации RTP соответствует версия 2.

**дополнение (P): 1 бит** — бит дополнения, свидетельствующий о наличии в конце пакета дополнительный октетов, не являющихся частью полезных данных.

**расширение (X): 1 бит** — индикаторный бит наличия расширения RTP заголовка.

**количество CSRC (CC): 4 бит** — число идентификаторов CSRC.

**маркер (M): 1 бит** — определяемый профайлом (спецификацией RTP для полезных данных определенного типа) бит.

**тип полезных данных (PT): 7 бит** — идентификатор полезных данных для возможности интерпретирования данных приложения.

**номер в последовательности: 16 бит** — номер, последовательно увеличивающийся с каждым новым посылаемым RTP пакетом, служащий для детектирования потерь пакетов и восстановления исходной последовательности пакетов на стороне приемника.

**маркер времени timestamp: 32 бит** — маркер времени отражает момент времени оцифровки первого байта в полезных данных RTP пакета, служащий для синхронизации приема/передачи пакетов по сети (например при реализации RTP-буфера).

**SSRC: 32 бит** — идентификатор источника синхронизации.

**список CSRC: 0 to 15 элементов, 32 бит каждый** — список идентификаторов распространителей RTP данных (CSRC).

В рамках мультикаст-юникаст шлюзов IP-TV осуществляется получение запрашиваемых абонентами каналов из мультикаст сети (т.е. RTP-пакетов) и дальнейшая их передача по юникаст сети с использованием в качестве транспортного TCP протокола, обеспечивающего гарантию доставки данных. Такой подход обеспечит качественный прием вещания в сетях, где присутствуют большие вероятности коллизий и задержек передачи. Заголовок RTP пакета вносит незначительную роль в увеличение общего потока данных канала вещания, но значительно упрощает реализацию IP-TV шлюза и абонентского ПО. На основании заголовка IP-TV шлюз может принять решение о пропуске в передачи определенных типов данных, например передача только опорных кадров видео и звукового сопровождения в случае затруднения передачи данных клиенту по TCP протоколу (недостаточная мгновенная пропускная способность). Такой подход обеспечит хотя и будет способствовать ухудшению качества приема, однако не приведет к полному отказу абонента от использования услуг вещания. Пример такой выборочной отправки показан в листинге 4.1.

```
inputencoding=utf8,
```

Таким образом RTP протокол является общим и для мультикаст, и для юникаст передачи в рамках гибридной архитектуры IP-TV сети. Анализ заголовков RTP позволяет промежуточным (на пути от подсистемы формирования контента из исходного материала до абонентской подсистемы) элементам системы (IP-TV шлюзам, IP-TV Интернет шлюзам и проч.) отслеживать идущий поток и принимать решение о пропуске определенного типа пакетов в случае невозможности передачи полного потока из-за ограничений сетевой подсистемы.

```

UINT size=myFIFO.SendBufferSize( );
/* Включениережимапередачиполный      ( поток ,  ключевыекадрызвук +,толькозвук
   ) наоснованиизразмерабуфераотправкиданныхклиенту
*/
if( mySendState==FULLAV )
{
    if( size>FULLVIDEOLIMIT )      mySendState=HALFAV;
    else if( size>HALFVIDEOLIMIT )  mySendState=ONLYV;
    else if( size>AUDIOLIMIT )     mySendState=SILENCE;
}
else if( mySendState==HALFAV )
{
    if( size>HALFVIDEOLIMIT )      mySendState=ONLYV;
    else if( size>AUDIOLIMIT )     mySendState=SILENCE;
    else if( size<LOWBUFFER )       mySendState=FULLAV;
}
else if( mySendState==ONLYV )
{
    if( size>AUDIOLIMIT )         mySendState=SILENCE;
    else if( size<LOWBUFFER )       mySendState=FULLAV;
}
else if( mySendState==SILENCE )
{
    if( size<LOWBUFFER )          mySendState=FULLAV;
    else if( size<FULLVIDEOLIMIT ) mySendState=HALFAV;
}

/*Анализ RTP заголовка*/
bool abortpacket=false; // Индикатор необходимости
                         // пропуска RTP пакета
char pkttype=pkt->FrameType( );
if( pkttype==PktSysHeader )
{
    abortpacket=false;
}
else if( pkttype==PktIFrames || pkttype==PktSFrames )
{
    if( mySendState==ONLYV || mySendState==SILENCE )
        abortpacket=true;
}
else if( pkttype==PktPFrames || pkttype==PktBBPFrames )
{
    if( mySendState==HALFAV || mySendState==ONLYV ||
        mySendState==SILENCE )
        abortpacket=true;
}
else if( pkttype==PktAudioFrames )
{
    if( mySendState==SILENCE ) abortpacket=true;
}

```

Листинг 4.1 – Фрагмент выборочной отправки данных клиенту на основании заголовка RTP пакета

#### 4.3.2.2 Протокол установления соединения для доступа абонентов к ресурсам вещания

Для получения RTP потока мультимедийных данных IP-TV вещания, необходимо осуществить этап инициализации, заключающийся в формировании защищенного канала связи «Абонент-Оператор» (с использованием технологии SSL, см.п.3.2.2), аутентификации и авторизации пользователя, после чего пользователь может получить полный перечень доступного в рамках пользовательской подписки IP-вещания. Для этого был разработан специализированный протокол, показанный на диаграмме состояния методологии проектирования RUP на рис.4.20.

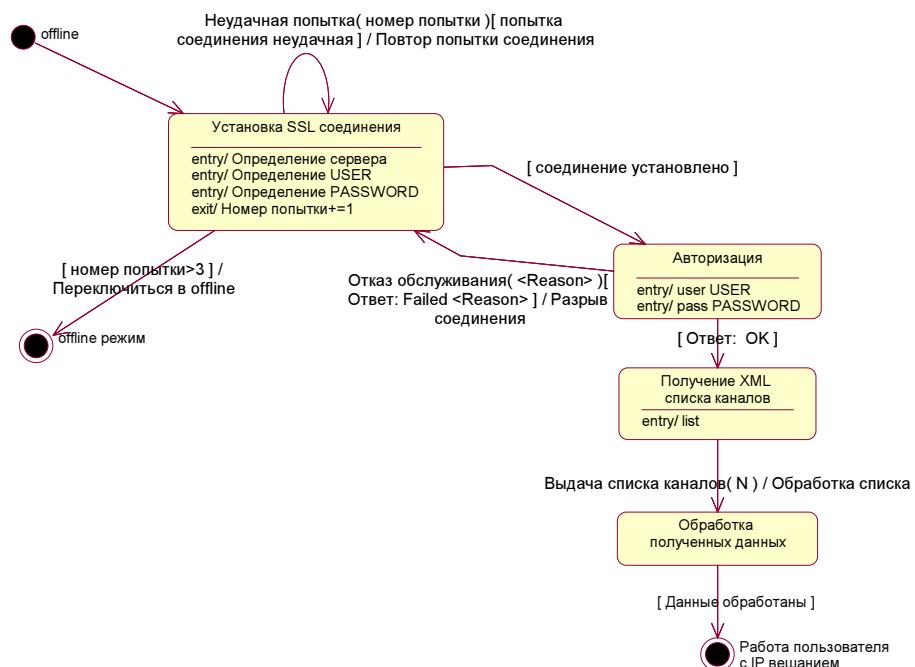


Рисунок 4.20 – Диаграмма состояния протокола взаимодействия клиента с сервером

Данный протокол взаимодействия обеспечивает возможность аутентификации и авторизации пользователей, возможность получения списка каналов, а также подключение запрос одного или нескольких мультимедийных потоков (каналов) для просмотра или записи на жесткий диск.

Спецификация элементов, использованных на диаграмме представлена в таблице 4.5.

Таблица 4.5 – Спецификация диаграммы состояния протокола установления соединения для доступа абонентов к ресурсам вещания

Наименование	Примечание
offline, offline режим	Режим неустановленного соединения с сервером (шлюзом IP-TV)
Установка соединения	Процесс установления сетевого соединения с сервером по протоколу TCP на порт 11112

Продолжение таблицы 4.5

Наименование	Примечание
Авторизация	Аутентификация пользователя с помощью логина и пароля (с учетом IP адреса) и авторизация в виде выделения ему ресурсов (формирование списка разрешенных к просмотру каналов)
Получение списка каналов	Запрос клиента на получение списка каналов и выдача сервером необходимой информации клиенту по TCP соединению в формате XML
Обработка полученных данных	Обработка клиентов выданной информации о списке каналов от сервера
Работа пользователя с IP-вещанием	Нормальная работа авторизованного пользователя с системой IP-вещания

Передача/получение разрешенного списка каналов осуществляется посредством XML. Спецификация формата представлена в листинге 4.2.

#### 4.3.2.3 Протокол запросов мультимедийных данных и получения ключей дескрамблирования

Для возможности организации гибридной модели защиты от несанкционированного доступа к мультимедийному вещанию (см.п.3.2) необходимо в рамках установленного посредством протокола установления соединения безопасного аутентифицированного и авторизованного соединения осуществлять запросы на подключение к конкретным каналам и передавать абоненту ключи для дешифрации мультимедийного потока. Каждый мультимедийный поток IP-вещания шифруется уникальным постоянно изменяющимся ключем, что обуславливает необходимость разработки специализированного протокола запроса и передачи ключевой информации.

Протокол должен предоставлять следующие возможности:

- Получение реквизитов для доступа к каналу.
- Запрос и получение ключа дешифрации по идентификатору канала.

Поскольку в рамках протокола осуществляется прием данных различного формата (реквизиты доступа, ключи дешифрации), то формат протокола целесообразно выбрать XML, предоставляющий возможности простого структурирования данных. Спецификация протокола представлена в листинге 4.3.

Сетевая подсистема посредством гибридной схемы доставки мультимедийного контента с использованием протоколов установления соединения, запросов мультимедийных данных и ключей дешифрации, а также собственно протокола передачи мультимедийных данных обеспечивает надежную доставку данных из подсистемы формирования контента в абонентскую подсистему, где осуществляется визуализация мультимедийных данных на абонентских терминалах.

```

<ICNTV>
  <info>
    <iptvoperator goid="Уникальный_идентификатор_оператора_IPTV"
      name="Название_оператора_IPTV">Определяемые оператором данные

    </iptvoperator>
  </info>

  <program pid="Уникальный_идентификатор_программы"
    name="Название_программы" lang="Язык"
    scrambled="true | false"
    type="Идентификатор_типа_радио( , _ТВ )"
    genre="Жанр_программы_Развлекательная( , _новости_и_проч. )">
    <!-- Опциональные элементы --!>
    <schedule start="Время_начала"
      end="Время_окончания">Название программы при
      ( получении общего списка — текущей ), идущей на канале

    </schedule>
  </program>
</ICNTV>

```

Листинг 4.2 – Спецификация формата получаемых данных во время установления соединения

## 4.4 Абонентская подсистема распределенной системы IP-вещания

В результате анализа гибридной архитектуры сетевой подсистемы в абонентской подсистеме можно выделить 2 компонента: подсистема доступа к потоковому вещанию и подсистема доступа к Интернет вещанию. В первом случае организуется доступ абонентов сети оператора в рамках мультикаст и/или юникаст сетей к набору сервисов вещания (потоковое, вещание по запросу). В случае Интернет вещания (посредством IP-TV Интернет шлюза, обеспечивающим необходимый уровень перекодирования исходных данных) осуществляется доступ авторизованных Интернет пользователей к подмножеству мультимедийных ресурсов сети оператора.

### 4.4.1 Подсистема доступа к потоковому вещанию

Подсистема доступа к потоковому вещанию должна реализовывать удобный и понятный интерфейс пользователя, клиентскую часть сетевого протокола взаимодействия сервера и клиента, а также обеспечивать прием, декодирование и визуализацию запрашиваемого мультимедийного потока с отображением сопутствующей информации при ее наличии.

На рис.4.21 приведена диаграмма вариантов использования, в которой отражены все необходимые функциональные возможности клиентской части ПО. Спецификация диаграммы представлена в таблице 4.6.

```

<!-- Запрос списка доступных каналов --!>
<ICNTVrequest><getlist /></ICNTVrequest>
<!-- Ответ согласно спецификации в листинге | ref{lst:xml_prglists} --!>

<!-- Запрос телепрограммы канала за период <Начало> Конец--!>
<ICNTVrequest>
    <getschedule id="Идентификатор_канала"
                  start="Начало" end="Конец" />
</ICNTVrequest>
<!-- Ответ сервера --!>
<ICNTV>
    <program id="Идентификатор_программы">
        <schedule start="Время_начала"
                  end="Время_окончания" rating="Тип_программы">Название программы
        </schedule>
        ...
    </program>
</ICNTV>

<!-- Запрос реквизитов доступа к каналу --!>
<ICNTVrequest><getkey id="Идентификатор_канала" /></ICNTVrequest>
<!-- Ответ сервера --!>

<!-- Запрос получения ключей дешифрации мультимедийных данных --!>
<ICNTVrequest><getkey id="Идентификатор_канала" /></ICNTVrequest>
<!-- В качестве ответа сервер вернет начающуюся с периодичной отправкой сообщений следующего вида
    : --!>
<ICNTV>
    <key type="Тип_ключа" id="Идентификатор_канала" value="Ключ" />
</ICNTV>

<!-- Прекращение передачи ключей дешифрации осуществляется либо путем запроса ключей для других мультиплексоров
    , либо путем разрывов в безопасном соединении
    , либо спомощью команды : --!>
<ICNTVrequest><stopkey id="Идентификатор_канала" /></ICNTVrequest>

```

Листинг 4.3 – Спецификация протокола запросов мультимедийных данных и получения ключей дескрамблирования

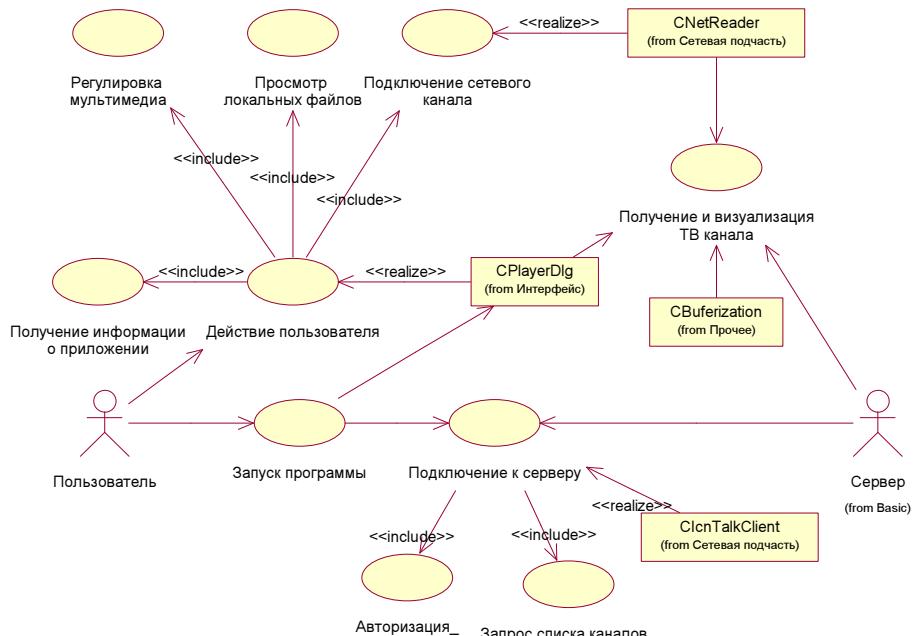


Рисунок 4.21 – Диаграмма вариантов использования подсистемы доступа к потоковому вещанию

Таблица 4.6 – Спецификация для диаграммы вариантов использования подсистемы доступа к потоковому вещанию

Наименование	Примечание
<b>Актеры</b>	
Пользователь	Пользователь имеющий доступ к системе мультимедийного вещания (логин, пароль), запускающий и работающий с клиентским ПО
Сервер	Сервер мультимедийного вещания
CPlayerDlg	Класс, реализующий интерфейс основного окна приложения
CBuferization	Класс, реализующий функцию буферизации принимаемого мультимедийного потока
ClcnTalkClient	Класс, реализующий клиентскую часть сетевого протокола взаимодействия сервера и клиента
CNetReader	Класс, реализующий получение по сети передачи данных мультимедийного потока
<b>Варианты использования</b>	
Запуск программы	Запуск программы пользователем
Подключение к серверу	Процесс установления соединения клиентского и серверного ПО
Авторизация	Ввод имени и пароля пользователя, передача их соответствующим образом серверу
Запрос списка каналов	Запрос и получение списка каналов

## Продолжение таблицы 4.6

Наименование	Примечание
Действие пользователя	Некоторое действие пользователя направленное на изменение состояния клиентской части ПО
Получение информации о приложении	Запрос и выдача в новом окне информации о приложении
Регулировка мультимедиа	Настройка пользователем режима отображения мультимедийного потока (размер изображения, пропорции, яркость, контрастность, уровень звука и проч.)
Просмотр локальных файлов	Просмотр ранее записанных мультимедийных потоков на жесткий диск
Подключение сетевого канала	Запрос серверу на подключение выбранного мультимедийного потока
Получение и визуализация ТВ канала	Получение, визуализация основном окне программы, либо сохранение на диск, либо и то и другое одновременно получаемого мультимедийного потока

Интерфейсная часть подсистемы доступа к потоковому вещанию состоит из главного окна программы и контекстного меню (рис.4.22), через которое может осуществляться доступ ко всем функциям приложения. Для удобства использования приложения, часть функций (переключение каналов, регулировка громкости) продублирована с помощью горячих клавиш.

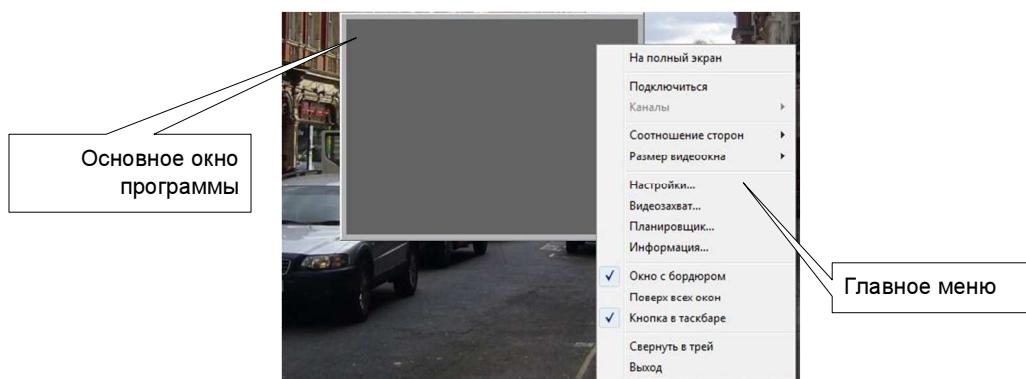


Рисунок 4.22 – Внешний вид и компоненты управления ПО доступа к потоковому вещанию

Основные функции реализуемые в рамках подсистемы доступа к потоковому вещанию:

- Общая настройка программы: адрес и порт IP-TV шлюза для организации безопасного аутентифицированного соединения (рис.4.23).

- Запрос и отображение мультимедийных данных в рамках главного окна приложения.
- Запись принимаемых мультимедийных данных на диск (рис.4.24).
- Формирование заданий планировщика — включение/запись трансляций в заданное время (рис.4.25).

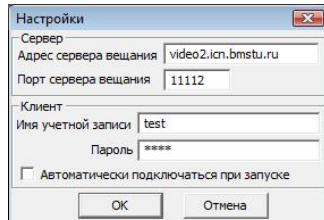


Рисунок 4.23 – Окно общей настройки программы

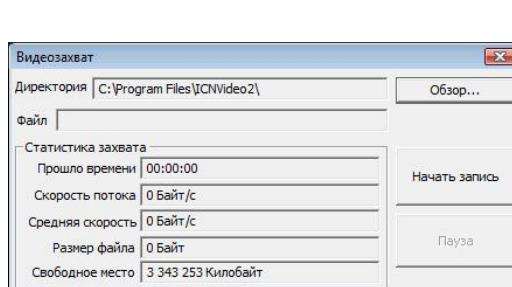


Рисунок 4.24 – Окно записи принимаемых мультимедийных данных на диск

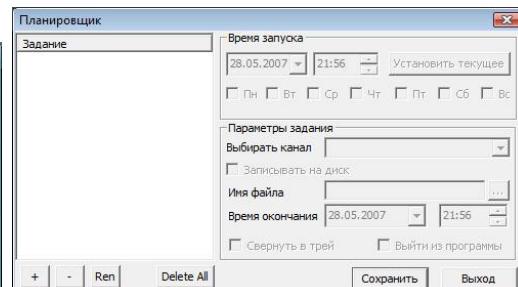


Рисунок 4.25 – Окно создания и редактирования элементов планировщика заданий

При работе с программой существует возможность переключения в полноэкранный режим отображения видео данных, изменения соотношения сторон отображения ( $4 \times 3$ ,  $16 \times 9$  или свободное), установить одно из предопределенных значений размеров окна программы, свернуть окно программы в системный трей (временная приостановка работы с IP-TV).

Выбор канала доступа осуществляется посредством иерархического контекстного меню, в котором отображены названия и жанры каналов вещания, а также путем переключения с использованием клавиатуры (цифровые клавиши, стрелки вверх-вниз) или мышки (колесо прокрутки с нажатой правой кнопкой).

После начала просмотра возможно начать запись принимаемого мультимедийного потока с помощью кнопки управления записью канала на диск.

#### 4.4.2 Подсистема доступа к Интернет-вещанию

Интернет вещание открывает возможности предоставления вещательных услуг не только абонентам какой либо конкретной сети, но также пользователям всемирной сети Интернет. Сетевую поддержку такого вещания обеспечивает мультикаст-юникаст IP-TV интернет шлюз (см.п.4.3) преобразующий исходный высокоскоростной поток мультимедийных данных (1-2 Мбит/с) в приемлемый для передачи по публичным сетям (100-

200 Кбит/с) за счет потери качества. Кроме того, интернет шлюз может осуществлять запись по расписанию заданных каналов (перекодированных в худшее качество) с целью использования этих записей в рамках интернет системы видео-по-запросу.

Максимальное распространение в настоящее время получила мультиплатформенная технология отображения видео в рамках WEB-страниц с помощью Flash-проигрывателя. В рамках интернет системы видео-по-запросу к публичным данным, например как студия мультимедийных образовательных технологий кафедры ИУ4 МГТУ им.Н.Э.Баумана (рис.4.26), на долю подсистемы управления и контроля выпадает лишь поддержание базы контента и его информационного сопровождения, а весь функционал отображения данных осуществляется посредством WEB-браузера.

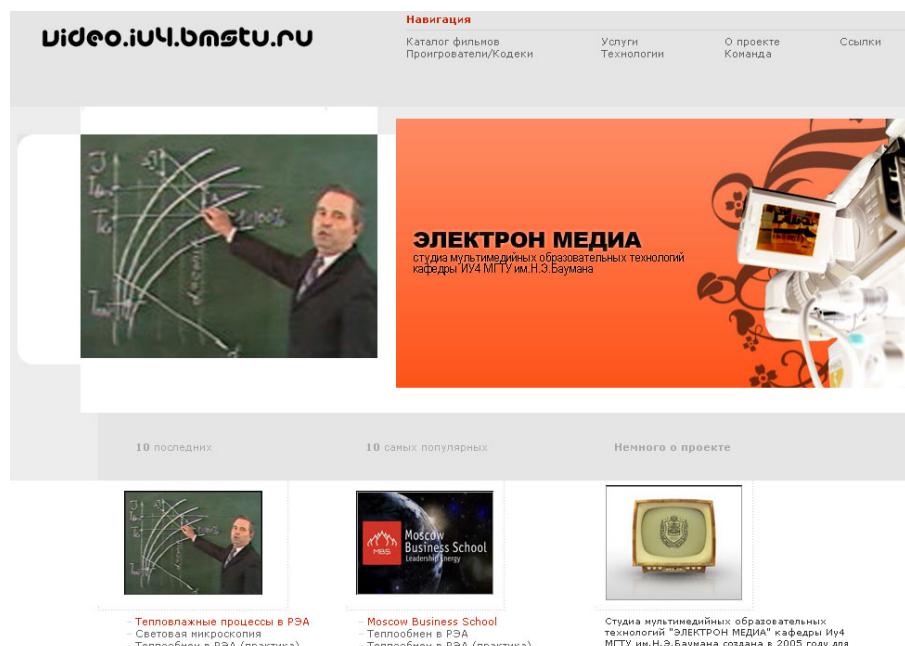


Рисунок 4.26 – Домашняя страница студии мультимедийных образовательных технологий кафедры ИУ4 МГТУ им.Н.Э.Баумана

Потоковое Интернет-вещание ограничено общей пропускной интернет канала оператора и аппаратными возможностями Интернет шлюза. Использование Flash-технологии отображения потоковых данных является перспективным как с точки зрения охвата пользователей, так и простоты реализации.

## Выводы

В рамках системы мультимедийного вещания в сетях передачи данных выделены четыре подсистемы: подсистема контроля и управления, подсистема формирования контента, сетевая и абонентская подсистема, а также объединяющий подсистемы элемент - база данных.

Распределенность СМВ закладывается в подсистемы формирования контента (множество мультимедийного материала доступного в сети формируется с помощью независимых формировательных элементов) и сетевую подсистему (доставка контента осуществляется с использованием не только собственно сетевого оборудования, а с задействованием специальных шлюзовых компонентов).

Главным элементом системы является подсистема управления и контроля системы IP-вещания, основной целью которой является формирование и контроль передачи данных из подсистемы формирования контента в абонентскую подсистему посредством сетевой подсистемы. В рамках контрольно-управляющей подсистемы можно выделить абонентское управление, управление вещанием и получение статистической информации вещания.

Формирование контента разбивается на ряд этапов: получение данных от источника, преобразование, формирование потока, пригодного для передачи в сетевую подсистему. Существование источников различного типа обуславливает создание подсистемы, незаточенной под определенный тип источников, а с возможностью интегрирования мультимедийных данных различного происхождения (гибридная подсистема формирования контента), для чего осуществлена декомпозиция подсистемы и был выделен набор базовых компонентов: компоненты источников данных и компоненты преобразования. Комбинации базовых компонентов позволяют реализовать все необходимые элементы получения и преобразования необходимого контента, формируя тем самым модульную архитектуру системы.

Задача передачи данных из подсистемы формирования контента в абонентскую полностью лежит на сетевой подсистеме. Разрешение противоречия между использованием дешевой структуры сети и желанием использовать качественное мультимедийное вещание в рамках этой сети лежит в использовании гибридной схемы доставки данных в рамках сети передачи данных, включая гибридную модель защиты от несанкционированного доступа.

В абонентской подсистеме выделяются два компонента: подсистема доступа к потоковому вещанию и подсистема доступа к Интернет-вещанию. В первом случае организуется доступ абонентов сети оператора в рамках мультикаст и/или юникаст сетей к набору сервисов вещания (потоковое, вещание по запросу). В случае Интернет-вещания (посредством IP-TV Интернет-шлюза, обеспечивающим необходимый уровень перекодирования исходных данных) осуществляется доступ авторизованных Интернет пользователей к подмножеству мультимедийных ресурсов сети оператора.

## **5 РАЗРАБОТКА НЕСУЩЕЙ КОНСТРУКЦИИ СЕРВЕРА ВЕЩАНИЯ И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СИСТЕМЫ МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ**

Важным этапом разработки системы мультимедийного вещания является построение опытного сервера вещания (т.е. контрольно-управляющей и формировательной подсистемы) и экспериментальное исследование функциональности системы в целом. Благодаря наличию обратной связи в управляемых подсистемах, экспериментальное исследование сводится к накоплению статистических данных работы системы и анализ этих данных. В основе сервера вещания лежит несущая конструкция, обеспечивающая возможность установки необходимого базового оборудования (материнская плата) и специализированных плат расширения (ТВ-тюнеры, DVB-модемы). Несущая конструкция также должна обеспечивать лёгкий доступ к разъёмам плат расширения для коммутации.

В рамках экспериментального исследования системы вещания производится получение информации о надежности и отказоустойчивости системы, подтверждения требований к пропускной способности канала в пересчете на одного подключенного пользователя для юникаст сетей и в пересчете на один канал для мультикаст сетей, оценка потребительской заинтересованности сервисом. Кроме того, получение сведений о качестве получения мультимедийных потоков клиентами, качестве работы механизма буферизации, а также различных сведений и пожеланий пользователей системы, направленных на улучшение потребительских и функциональных свойств комплекса.

Требования к пропускной способности каналов передачи данных оценивались с помощью программного обеспечения MRTG.

### **5.1 Несущая конструкция сервера вещания**

#### **5.1.1 Разработка несущей конструкции**

Сервер вещания, интегрирующий подсистемы формирования контента и, опционально, подсистему контроля и управления (в случае использовании в качестве головного сервера) должен отвечать следующим требованиям:

1. Компактный размер;
2. Возможность установки 19" конструктивов;
3. Иметь встроенную систему ввода-вывода для конфигурирования сервера вещания
4. Обеспечивать легкий доступ к коммуникационным разъемам специализированного аппаратного обеспечения;

Учитывая приведенные выше требования было решено в качестве НК разрабатывать тумбу высотой 14U. Высота 14U была выбрана исходя из необходимости установки источника бесперебойного питания 4U, двух вещательных серверов 4U и коммутационной панели 2U. Система ввода-вывода должна располагаться в рамках верхней крышки тумбы

и иметь выдвижную конструкцию.

Используя пакет SolidWorks была разработана модель тумбы (рис.5.1), а также необходимые чертежи (см.приложение А). Реализованная НК сервера вещания представлена на рис.5.2.

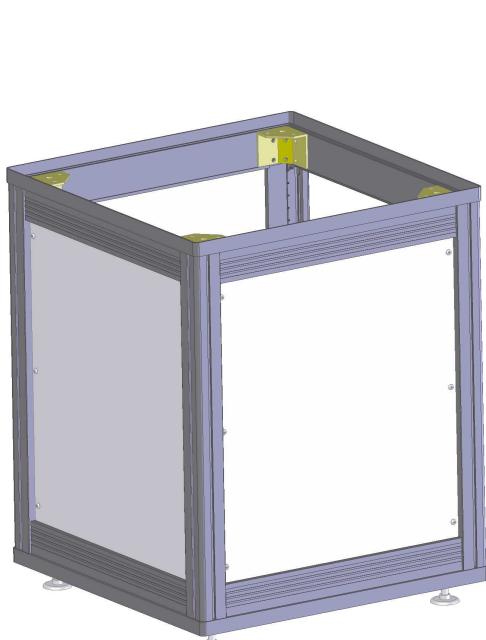


Рисунок 5.1 – Модель SolidWorks НК сервера вещания



Рисунок 5.2 – Реализованная НК сервера вещания

### 5.1.2 Испытания несущей конструкции

Целью испытаний несущей конструкции сервера вещания является оценка выполнения требований по живучести и стойкости изделия к внешним воздействиям.

Испытания проводились в период с 09.06.06 г. по 14.07.06 г. на базе ЗАО «Технологические системы».

Несущая конструкция сервера вещания подвергается испытаниям на обнаружение резонансов и на устойчивость при воздействии синусоидальной вибрации. Порядок проведения испытаний приведен на блок-схемах рис.5.3 и рис.5.4.

В рамках испытаний проведен анализ причин, вызвавших отказы и выполнены доработки конструкции изделия, даны рекомендации по модификации несущей конструкции. После внесения модификаций, несущая конструкция подверглась повторным испытаниям.

Результаты испытаний:

1. После окончания воздействия вибрации изделие полностью работоспособно и признано выдержавшим испытания.
2. Резонансов конструкции изделия в диапазоне частот 5 -25 Гц не обнаружено.

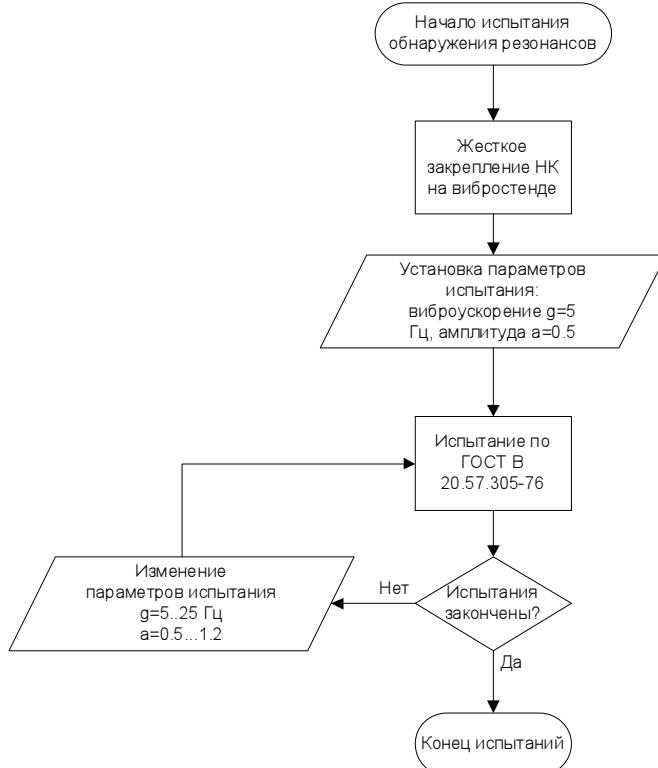


Рисунок 5.3 – Блок схема испытания на обнаружение результатов

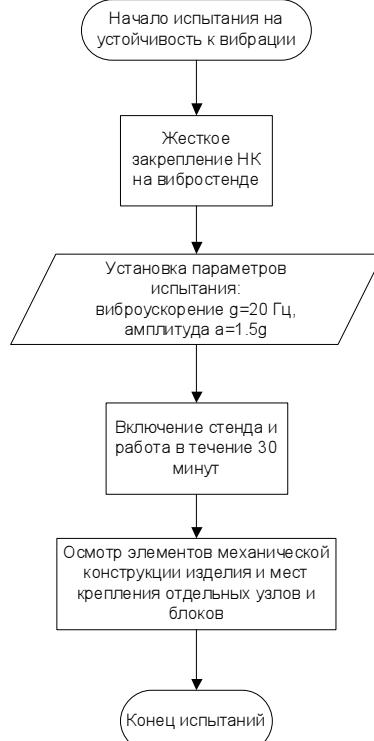


Рисунок 5.4 – Блок схема испытания на устойчивость к синусоидальной вибрации

## 5.2 Построение экспериментальной системы мультимедийного вещания

В рамках построения экспериментальной системы мультимедийного вещания в рамках существующей сети необходимо реализовать контрольно-управляющую, формировать и абонентскую подсистемы. Первые две подсистемы объединяются в рамках единого экспериментально сервера вещания. Экспериментальная система мультимедийного вещания и ее экспериментальное исследование проводилось на базе сети передачи данных Измайлловского студгородка МГТУ им.Н.Э.Баумана.

Конфигурация экспериментального сервера вещания выбрана следующей:

- Процессор: Pentium 4 2.4Ghz
- ОЗУ: 512 Мбайт
- Жесткий диск: 40 Гбайт

В качестве источника мультимедийного контента выбрано цифровое спутниковое вещание. В качестве аппаратной части программно-аппаратных компонентов формирования используется:

1. спутниковые тарелки диаметром 60 см и 90 см для приема сигнала со спутника Eutelsat W4 (36° в.д.) и Sirius 2/3 (5° в.д.) соответственно (см.рис.5.5).
2. блокцифро-аналоговых ресиверов для приема и декодирования получаемого мультимедийного контента со спутников и сам сервер вещания, установленные

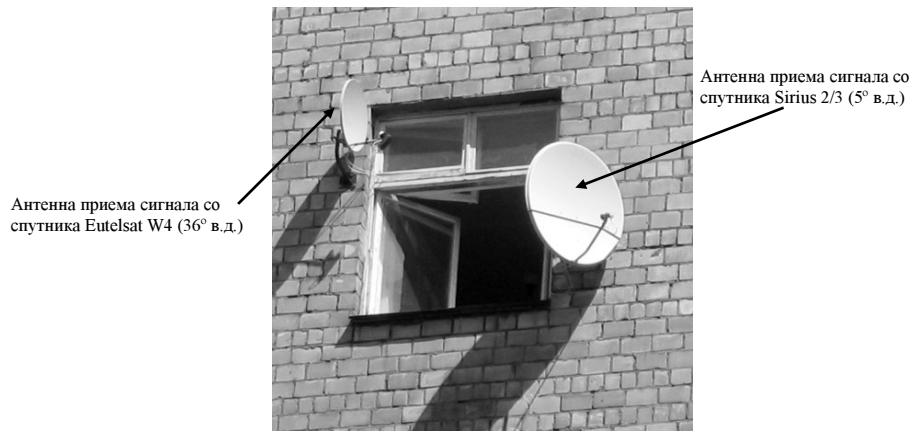


Рисунок 5.5 – Расположение спутниковых тарелок приема сигнала со спутников

в стоечную конструкцию (экспериментальный станд, рис.5.6)

### 3. блок сервера вещания (опытный образец, рис.5.7)



Рисунок 5.6 – Экспериментальный  
вещательный сервер



Рисунок 5.7 – Опытный образец блока  
сервера вещания

### 4. Специализированные платы оцифровки аналогового сигнала

Абонентская подсистема представляет собой программное обеспечение приема потокового вещания. В рамках тестирования, ПО устанавливалось на рабочие станции пользователей сети передачи данных Измайловского студгородка МГТУ им.Н.Э.Баумана для проведения оценок требований ПО к аппаратному обеспечению.

### **5.3 Методика и порядок испытаний системы мультимедийного вещания**

Серверная часть комплекса должна устойчиво и надежно функционировать без вмешательства оператора на протяжении не менее 30 дней в условиях штатных и стрессовых нагрузок.

Программное обеспечение клиентской части комплекса должно обеспечивать бесперебойную непрерывную работу по получению от сервера вещания и декодированию мультимедийных потоков на протяжении не менее 24 часов с прерыванием на буферизацию не чаще 1 раза в час не более чем на 10 секунд при достаточной пропускной способности сети передачи данных.

Перечень тестовых заданий, применяемых для проведения дифференциальных оценок качества серверного и клиентского программного обеспечения, приведен в табл.5.1.

Для тестирования серверной и клиентской части программного обеспечения используются штатные средства мониторинга сервисов операционных систем сервера, клиента, а также операционной системы маршрутизатора (ОС Linux), являющегося одним из центральных звеньев сети передачи данных.

Кроме того, для интегральной оценки эксплуатационных параметров использовалось программное обеспечение MRTG, реализующее построение графиков используемой пропускной способности сети в различных временных промежутках (сутки, неделя, месяц, год). Для оценки использования сервера вещания пользователями сети используются штатные средства серверного программного обеспечения (внесение данных в базу статистики), а также реализация визуализации информации из mysql базы, реализованная на PHP.

Порядок проведения испытаний для получения дифференциальных оценок качества серверного и клиентского ПО:

1. запуск ПК сервера вещания;
2. запуск ПК, где установлено клиентское ПО;
3. удаленное соединение с маршрутизатором;
4. выполнение команды `ping -f <адрес сервера>` в течение 10 минут
5. выполнение команды `ping -f <адрес клиента>` в течение 5 минут
6. отключение от сервера
7. последовательный запуск и выключение клиентского ПО
8. запуск клиентского ПО и запрос мультимедийного потока (канала)
9. запуск еще трех экземпляров клиентского ПО и запрос в каждом из них мультимедийного потока (канала).

Таблица 5.1 – Перечень тестовых заданий для определения дифференциальных оценок качества программного обеспечения

№п/п	Наименование функции и ее характеристики	Наименование тестового задания и описание	Критерий положительного результата
<b>Серверное ПО</b>			
1	Поддержка протокола IP	Проверка качества канала связи сервер вещания - маршрутизатор путем запуска на маршрутизаторе команды ping -f <адрес сервера> и ее работа в течение не менее 10 минут	Количество потерянных пакетов должно составлять менее 10 пакетов
2	Прием соединений с клиентом	Последовательное соединение, аутентификация и разъединение с помощью клиентского программного обеспечения 100 раз в течение 5 минут	Отсутствие отказа приема хотя бы одного соединения
3	Передача в сеть мультимедийного потока	Проверка используемой пропускной способности на один канал. Использование штатных средств Windows XP	Загрузка в пересчете на одного клиента не более (1 ± 0.2)% общей пропускной способности сети стандарта 100BaseTX
<b>Клиентское ПО</b>			
4	Поддержка протокола IP	Проверка качества канала связи клиент - маршрутизатор путем запуска на маршрутизаторе команды ping -f <адрес клиента> и ее работа в течение не менее 5 минут	Количество потерянных пакетов должно составлять менее 1000 пакетов
5	Декодирование мультимедийного потока в различных условиях	Запуск клиента, подключение к серверу и запрос канала, а также его просмотр в условиях 70-100% загрузки ЦПУ (параллельная загрузка процессора) Параллельный запуск 4 клиентов и контроль процесса декодирования	Остановки и прерывания не превышают 1% времени просмотра и не мешают восприятию аудиовизуальной информации

## 5.4 Результаты испытаний системы мультимедийного вещания

### 5.4.1 Дифференциальные оценки качества ПО

Результаты испытаний серверного и клиентского программного обеспечения с учетом вышеуказанных требований представлены в табл.5.2.

Таблица 5.2 – Результаты испытаний программного обеспечения

№ п/п	Наименование функции и ее характеристики	Достигнутый показатель
Серверное ПО		
1	Поддержка протокола IP	[root@www root]# ping -f 192.168.5.253 PING 192.168.5.253 (192.168.5.253) 56(84) bytes of data. -- 192.168.5.253 ping statistics -- 1599110 packets transmitted, 1599110 received, 0% packet loss, time 732329ms rtt min/avg/max/mdev = 0.174/0.436/20.360/0.260 ms, pipe 2, ipg/ewma 0.457/0.614 ms Количество потерянных пакетов 0 - испытание пройдено
2	Прием соединение с клиентом	Все соединения были приняты и соответствующим образом обработаны сервером - испытание пройдено
3	Передача в сеть мультимедийного потока	Передача в сеть мультимедийного потока Средняя полчасовая используемая пропускная способность канала при четырех подключенных клиентах составила 2.5% - испытание пройдено
Клиентское ПО		
4	Поддержка протокола IP	[root@www root]# ping -f cawka PING cawka.icn.bmstu.ru (192.168.56.208) 56(84) bytes of data. -- cawka.icn.bmstu.ru ping statistics -- 704960 packets transmitted, 704960 received, 0% packet loss, time 314114ms rtt min/avg/max/mdev = 0.212/0.423/20.447/0.149 ms, pipe 2, ipg/ewma 0.445/0.396 ms Количество потерянных пакетов 0 - испытание пройдено
5	Декодирование мультимедийного потока в различных условиях	При параллельной загрузке процессора клиентской системы процессом компиляции программного обеспечения (общая загрузка процессора 100%) процесс декодирования и визуализации проходил без сбоев. Одновременное декодирование 4 мультимедийных потоков на протяжении 30 минут проходило без сбоев. Испытание пройдено.

По результатам испытаний и получения дифференциальных оценок качества, комплекс мультимедийного вещания принят к опытной эксплуатации для более детального изучения и накопления интегральных характеристик по качеству работы.

### 5.4.2 Интегральные оценка качества ПО

В результате 5 месячной опытной эксплуатации комплекса мультимедийного вещания в рамках сети передачи данных Измайловского студгородка МГТУ им.Н.Э.Баумана была получена информация о стабильности работы аппаратного и программного обеспечения комплекса, а также получен интегральные оценочные характеристики: статистика использования услуг сервера вещания и используемая пропускная способность канала передачи данных осредненная по различным временными промежуткам.

#### 5.4.2.1 Стабильность аппаратного и программного обеспечения

Во время эксплуатации не выявлено особых требований и не поступило жалоб на стабильность и качество работы базового ПК сервера вещания, а также платы H.264 кодирования.

Опытная эксплуатация выявила ряд дестабилизирующих факторов серверного программного обеспечения, после чего была произведена работа по доработке ПО и повышению его надежности. В целом надежность работы без вмешательства оператора находится на удовлетворительном уровне и входит в поставленные рамки (30 дней).

#### 5.4.2.2 Использование канала передачи данных

В результате опытной эксплуатации были получены характеристики использования канала передачи данных. На рис.5.8 представлена статистика использования каналов передачи данных за последние два дня, за неделю, за месяц и за год соответственно.

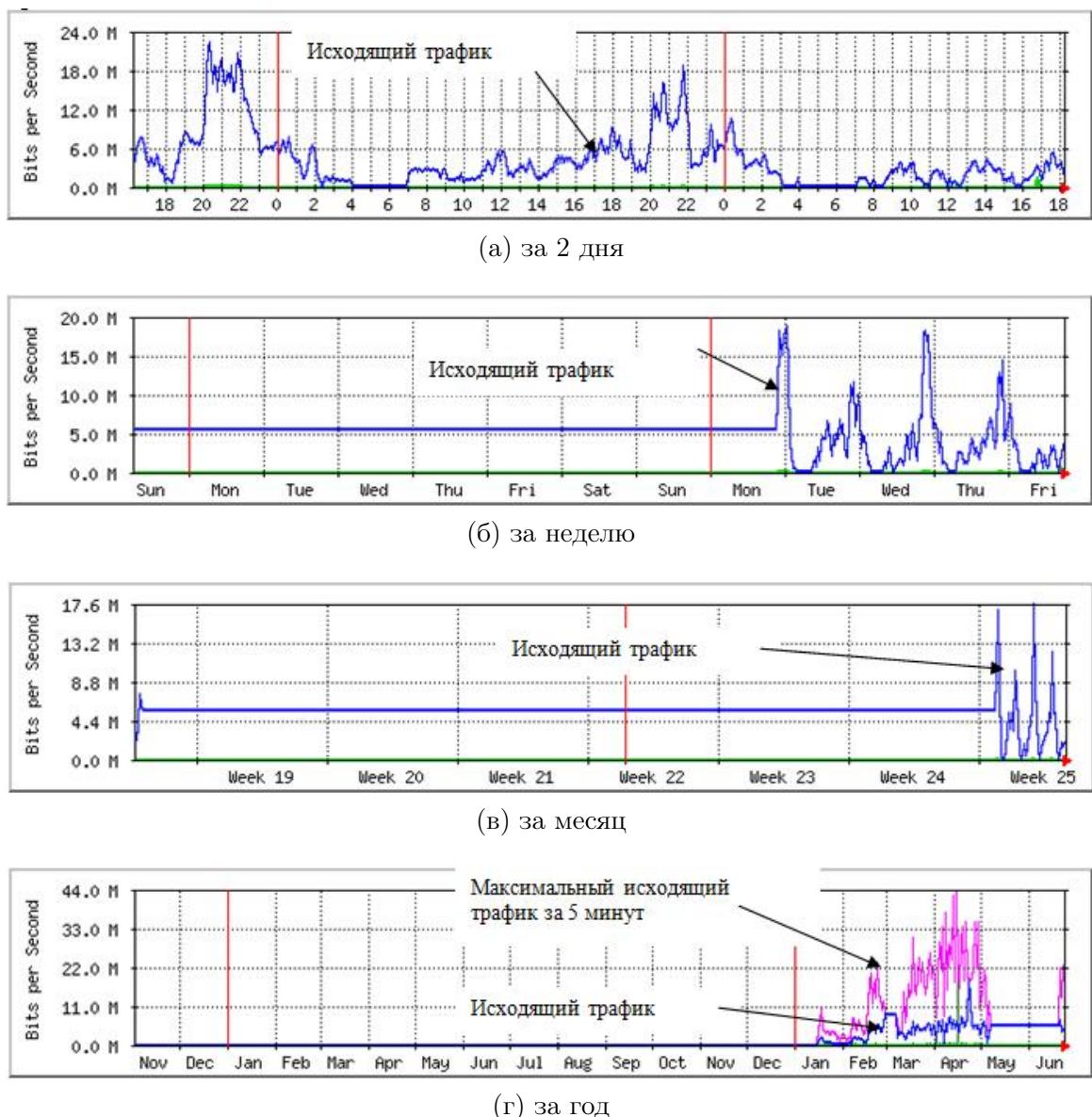


Рисунок 5.8 – Статистика использования каналов передачи данных

На основе статистики за последние 2 дня видно (рис.5.8а), наибольшей популяр-

ностью сервер вещания пользуется в промежуток времени 18:00-23:00 каждого дня, а из статистики за год (рис.5.8г) виден постепенный рост использования сервера мультимедийного вещания.

#### 5.4.2.3 Использования сервера вещания

Статистика использования сервера мультимедийного вещания пользователями сети Измайлловского студгородка представлена на рис.5.9. Первые два графика (5.9а и 5.9б) показывают суммарную статистику запросов мультимедийных потоков (каналов) пользователями (по дням и по месяцам соответственно). В обоих случаях виден постепенный рост использования услуг сервера вещания (на графике рис.5.9б эта тенденция явно прослеживается). В среднем число запросов мультимедийных потоков составляет 250-300 в день, что является показателем достаточной популярности и востребованности ресурса.

При анализе уникальных хостов (компьютеров сети) (рис.5.9в), с которых происходили запросы мультимедийных потоков, также прослеживается тенденция к росту числа потенциальных пользователей будущего коммерческого ресурса сети. В целом можно отметить, что ежемесячно услугами видеосервера пользуется около 400 пользователей, что составляет практически 50% пользователей всей сети, что еще более явно говорит о высокой степени актуальности услуг мультимедийного вещания.

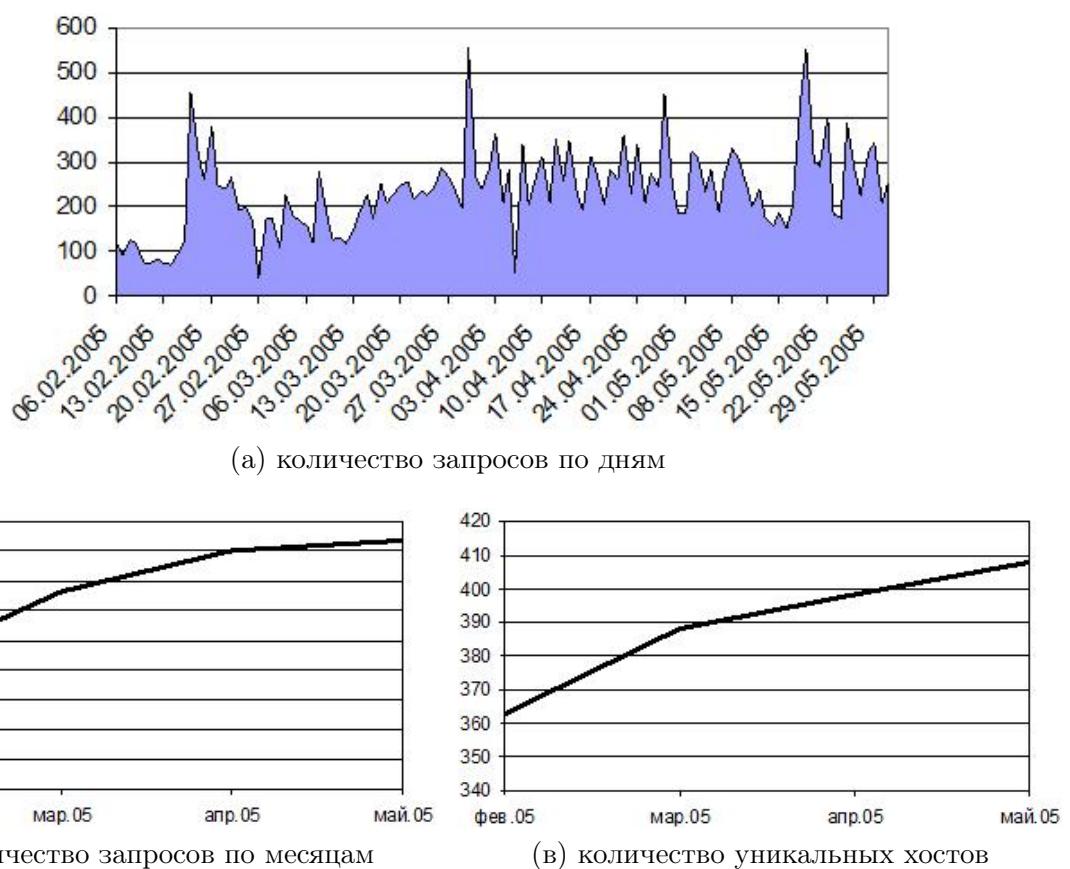


Рисунок 5.9 – Статистика использования IP-TV вещания

В рамках опытной эксплуатации возможно было получение одного из 4 (а из-за нестабильности аппаратного обеспечения - одного из 3) мультимедийных потоков. При переходе на коммерческий режим эксплуатации количество доступных пользователям муль-

тимедийных потоков будет расширено до 12, что может привлечь еще некоторую часть пользователей сети.

## Выводы

Важным этапом разработки системы мультимедийного вещания является построение опытного сервера вещания (т.е. контрольно-управляющей и формировательной подсистемы) и экспериментальное исследование функциональности системы в целом. Благодаря наличию обратной связи в управляемых подсистемах, экспериментальное исследование сводится к накоплению статистических данных работы системы и анализ этих данных. В основе сервера вещания лежит несущая конструкция, обеспечивающая возможность установки необходимого базового оборудования (материнская плата) и специализированных плат расширения (ТВ-тюнеры, DVB-модемы). Кроме того, несущая конструкция обеспечивает лёгкий доступ к разъёмам плат расширения для коммутации и технического обслуживания.

Для экспериментального исследования функциональности системы вещания в различных режимах эксплуатации реализован экспериментальный образец сервера мультимедийного вещания на базе ПК: Pentium 4 2.4G, 512 Мбайт ОЗУ, 40 Гбайт ПЗУ. В качестве аппаратного обеспечения приема мультимедийных потоков используются спутниковые антенны (60 см и 90 см), спутниковые ресиверы и платы аппаратного H.264 кодирования.

Определена методика, а также порядок проведения испытаний комплекса программно-аппаратного обеспечения при вводе его в эксплуатацию.

Приведены результаты испытаний программного и аппаратного обеспечения по дифференциальным оценкам качества программного обеспечения (критерии для серверного ПО: поддержка протокола IP, прием соединений клиентом, передача в сеть мультимедийного потока; критерии для клиентского ПО: поддержка протокола IP и декодирование мультимедийного потока в различных условиях). Результатом оценок явилось принятие комплекса мультимедийного вещания в опытную эксплуатацию в рамках сети передачи данных Измайловского студгородка МГТУ им.Н.Э.Баумана. Произведены интегральные оценки качества ПО: стабильности работы аппаратного (основная нестабильность - ненадежность работы одного из четырех ресиверов - XSAT Simulcrypt DVB) и программного обеспечения комплекса, статистика использования услуг сервера вещания и используемая пропускная способность канала передачи данных осредненная по различным временными промежуткам. В результате анализа статистики прослеживается тенденция к росту числа потенциальных пользователей будущего коммерческого ресурса сети. Ежемесячно к услугам мультимедийного вещания прибегает около 400 пользователей, что составляет 50% пользователей всей сети.

## ЗАКЛЮЧЕНИЕ

В работе исследованы принципы построения мультимедийного вещания: определены возможные источники мультимедийного контента (файлы мультимедиа данных, эфирное телевидение, эфирное радио, кабельное телевидение, спутниковое телевидение и радио, локальные источники мультимедийных данных), получена сравнительная оценка источников, исследованы технологии доставки информации от сервера до клиента: unicast, multicast, сети mbone.

Произведен анализ аналогового и цифрового телевизионного и радиовещания с целью исследования существующих моделей и методов передачи мультимедийных данных: стандарты аналогового телевещания NTSC, PAL, SECAM; цифрового телевещания: DVB, ATSC, ISDB; цифрового радиовещания: DAB, DRM. Практически все цифровые форматы телевещания базируются на стандарте сжатия MPEG-2.

Проанализированы общие концепции представления видеопоследовательностей в цифровом виде — дискретизированный по времени и в пространстве видео поток, — представляющий в чистом виде собой большой массив данных, непригодный для хранения и передачи: порядка 200 Мбит на 1 секунду видео стандартного телевизионного качества. Исследованы механизмы и способы реализация высокой степени сжатия (более 1:50) видеопотока за счет потери части данных (кадр ≠ декодирование[кодирование(кадр)]) при отсутствии влияния или допустимом влиянии на субъективное восприятие видео потока человеком (использование свойств системы чувственного восприятия человека), а также использования высокой коррелированности последовательных кадров и внутри кадра.

Исследована архитектура самого эффективного с точки зрения отношения качества видео к требуемому потоку данных кодека H.264, использующего гибридную модель кодека, в которой происходит избавление как от временной, так и от пространственной и энтропийной избыточности, отличающегося применением технологий переменного размера блока компенсации движения, повышенной точности компенсации движения (до 1/4 пикселя), реализации векторов движения за границы изображения, множественной ссылочности компенсации движения, независимости ссылочности от порядка воспроизведения, взвешенного предсказания, пространственного предсказания в интра-кодировании, встроенного фильтра блочности, контекстнозависимого арифметическое энтропийного кодирования и контекстнозависимого кода переменной длины. Эффективность сжатия (при мерно в два-три раза большая чем для MPEG-2) и возможность аппаратной и программной реализации обуславливает выбор H.264 стандарта в качестве основного варианта представления данных в рамках IP-TV вещания.

Исследованы существующие технологии защиты данных от несанкционированного доступа в рамках мультикаст сетей: многоуровневая модель разграничения доступа к вещанию в стандарте DVB, включающая процесс скрамблирования транспортного потока с помощью симметрично шифрования, ключи которого передаются абонентам в рамках этого же транспортного потока, используя проприetaryные механизмы (Viaccess, Conax,

BISS, Mediaguard и другие) шифрования и управления абонентами (на основе смарт-карт).

Разработана технология защиты от несанкционированного доступа к IP-вещанию, отличающейся применением гибридной модели разграничения доступа, в которой основной поток шифруется эффективным (с точки зрения стойкости, стоимости, аппаратной и программной реализации) алгоритмом симметричного шифрования AES, а ключи для дешифрования передаются, используя безопасное (SSL) двунаправленное соединение абонентского терминала с системой управления пользователями оператора с непосредственной аутентификацией и авторизацией абонента.

Исследована на системном уровне архитектура системы IP-TV вещания и выделены основные подсистемы: управления и контроля IP-вещания, формирования контента, сетевой и абонентской подсистемы. Определены рамки распределенности системы IP-TV в рамках подсистем формирования контента (множество мультимедийного материала доступного в сети формируется с помощью независимых формировательных элементов) и сетевой (доставка контента осуществляется с использованием не только собственно сетевого оборудования, а с задействованием специальных шлюзовых компонентов). Произведена декомпозиция подсистемы формирования и определены базовые блоки (источники данных, блоки преобразования) и варианты реализации компонентов формирования контента, представляющих собой элементы модульной архитектуры системы.

Разрешены противоречия между использованием дешевой структуры сети (неуправляемое оборудование, отсутствие приоритезации трафика внутри сети) и желанием использовать качественное мультимедийное вещание в рамках этой сети путем использования гибридной схемы доставки данных в рамках сети передачи данных в рамках разработанных протоколов: установления соединения, запросов и получения мультимедийных данных, запросов и получения ключей дескрамблирования и сопутствующей информации по программе.

В абонентской подсистеме выделены два компонента: подсистема доступа к потоковому вещанию и подсистема доступа к Интернет вещанию. В первом случае организуется доступ абонентов сети оператора в рамках мультикаст и/или юникаст сетей к набору сервисов вещания (потоковое, вещание по запросу). В случае Интернет вещания (посредством IP-TV Интернет шлюза, обеспечивающим необходимый уровень перекодирования исходных данных) осуществляется доступ авторизованных Интернет пользователей к подмножеству мультимедийных ресурсов сети оператора.

На базе сети передачи данных Измайловского студгородка МГТУ им.Н.Э.Баумана построен экспериментальный стенд мультимедийного вещания и получены результаты качественных и количественных оценок работы комплекса программного и аппаратного обеспечения (непрерывное бесшлейфное функционирование серверной части более 30 дней без вмешательства оператора, усредненное ежедневное число запросов мультимедийных потоков-каналов 250-300, количество уникальных IP адресов, с которых происходило подключение к серверу вещания в месяц имеет тенденцию к росту и составляет порядка 400 - около 50% всех пользователей сети).

## СПИСОК ЛИТЕРАТУРЫ

1. Minerva Networks // <http://www.minervanetworks.com/> 10
2. SecNews.Ru. CTI готов к Video по IP //  
<http://www.secnews.ru/events/110116280813.htm> 10
3. Cisco Press. Quality of Service //  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/qos.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm) 10, 105
4. Семёнов Ю.А. Telecommunication technologies - телекоммуникационные технологии // <http://book.itep.ru> 18
5. D.D.Clark, D.L.Tennenhouse, «Architectural considerations for a new generation of protocols» // SIGCOMM Symposium on Communications Architectures и Protocols, (Philadelphia, Pennsylvania), pp. 200–208, IEEE, Sept. 1990. Computer Communications Review, Vol. 20(4), Sept. 1990 16
6. Cisco Press. Internet Protocol Multicast //  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/ipmulti.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm) 18
7. Kramer AV Academy. Стандарты цифрового телевизионного вещания, Журнал 625, выпуск 5, 2006 г. 26
8. The World DAB Forum // <http://www.worlddab.org> 27
9. Digital Radio Mondiale // <http://www.drm.org> 27
10. Локшин Б.А. Цифровое вещание: от студии к телезрителю. - М.: Сайрус системс, 2001 29
11. VideoLAN, École Centrale Paris // <http://www.videolan.org> 31
12. Iain E.G.Richardson, H.264 and MPEG-4 Video Compression. Video Coding for Next-generation Multimedia, Willey, 2003. 38, 39, 40, 41, 42, 43, 50, 61
13. Recommendation ITU-R BT.601-5, Studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios, ITU-T, 1995. 36, 38
14. Recommendation ITU-T BT.500-11, Methodology for the subjective assessment of the quality of television pictures, ITU-T, 2002. 38
15. Mallat, A Wavelet Tour of Signal Processing, Academic Press, 1999. 42, 45
16. ISO/IEC 14496-10 and ITU-T Rec.H.264, Advanced Video Coding For Generic Audiovisual Services, ITU, 2005 41, 50, 51, 54, 55
17. ISO/IEC 14496-10 and ITU-T Rec.H.264, H.264/MPEG-4 AVC Reference Software Manual, ITU, 2005 58, 59, 60
18. Национальная спутниковая компания, ТРИКОЛОР ТВ //  
<http://www.tricolor.tv/> 64
19. ЗАО «КОМСТАР-Директ», СТРИМ // <http://www.stream.ru/> 10, 65
20. DVB Project, DVB - Digital Video Broadcasting // <http://www.dvb.org/> 26, 65
21. DVB Project Office, DVB Common Scrambling Algorithm. Distribution Agreements, 1996 67
22. Берд Киви. О процессе принятия AES. «Компьютерра», декабрь 1999, N 49 71

23. NIST, AES - Advanced Encryption Standard //  
<http://csrc.nist.gov/CryptoToolkit/aes/> 68
24. Joan Daemen, Vincent Rijmen, The Rijndael Block Cipher, AES Proposal, 1999 73
25. Federal Information Processing Standards Publication 197, Advanced Encryption Standard, 2001 73, 74, 75, 76
26. William Stallings, Cryptography and Network Security Principles and Practices, 4th Ed, Prentice Hall, 2005 - 592 pages 68, 77, 78, 79, 82
27. Семенов Ю.А. Протокол SSL. Безопасный уровень соединителей //  
[http://book.itep.ru/6/ssl\\_65.htm](http://book.itep.ru/6/ssl_65.htm) 68
28. Alan O. Freier, Philip Karlton, Paul C. Kocher, The SSL Protocol Version 3.0, Netscape Communications, Internet Draft, 1996 80
29. Ralf S. Engelschall, OpenSSL: The Open Source toolkit for SSL/TLS //  
<http://www.openssl.org/> 81
30. Philips Semiconductors. THE I2C-BUS SPECIFICATION // [www.nxp.com](http://www.nxp.com) 99
31. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. RTP: A Transport Protocol for Real-Time Applications / Network Working Group, Audio-Video Transport Working Group, Request for Comments: 1889. - 1996 108

ПРИЛОЖЕНИЕ А  
Несущая конструкция сервера вещания

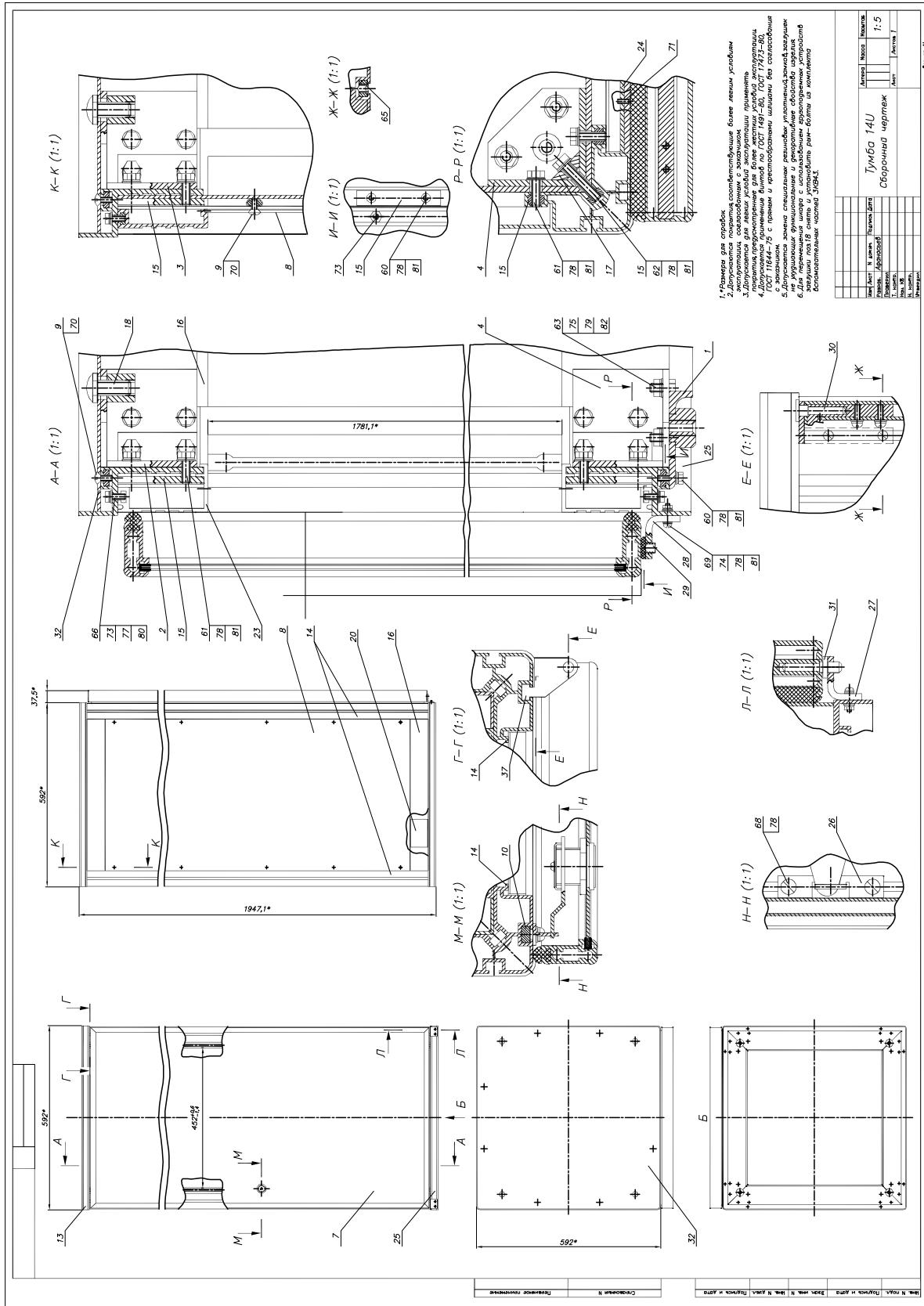


Рисунок А.1 – Сборочный чертеж тумбы 14U

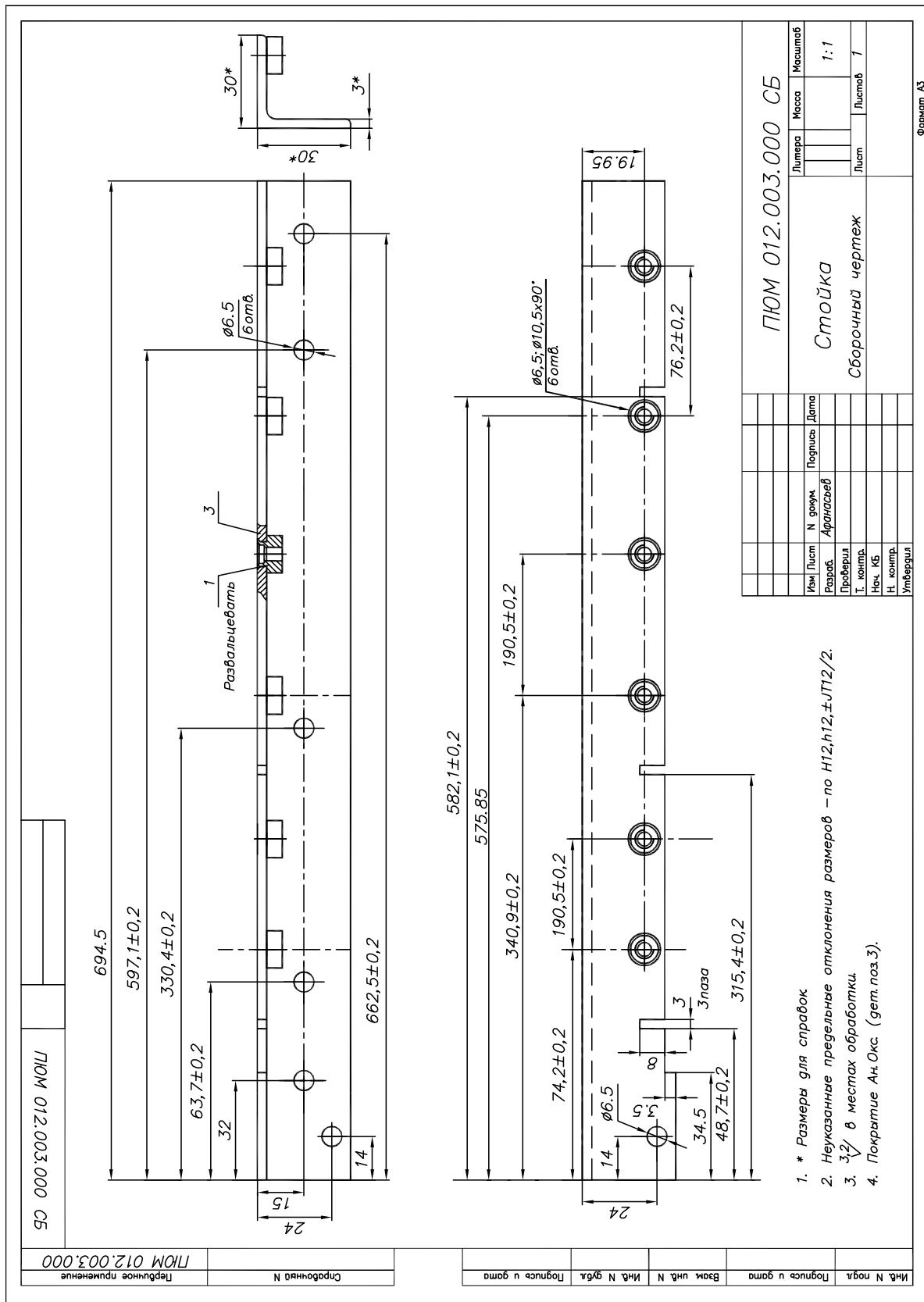


Рисунок А.2 – Сборочный чертеж стойки

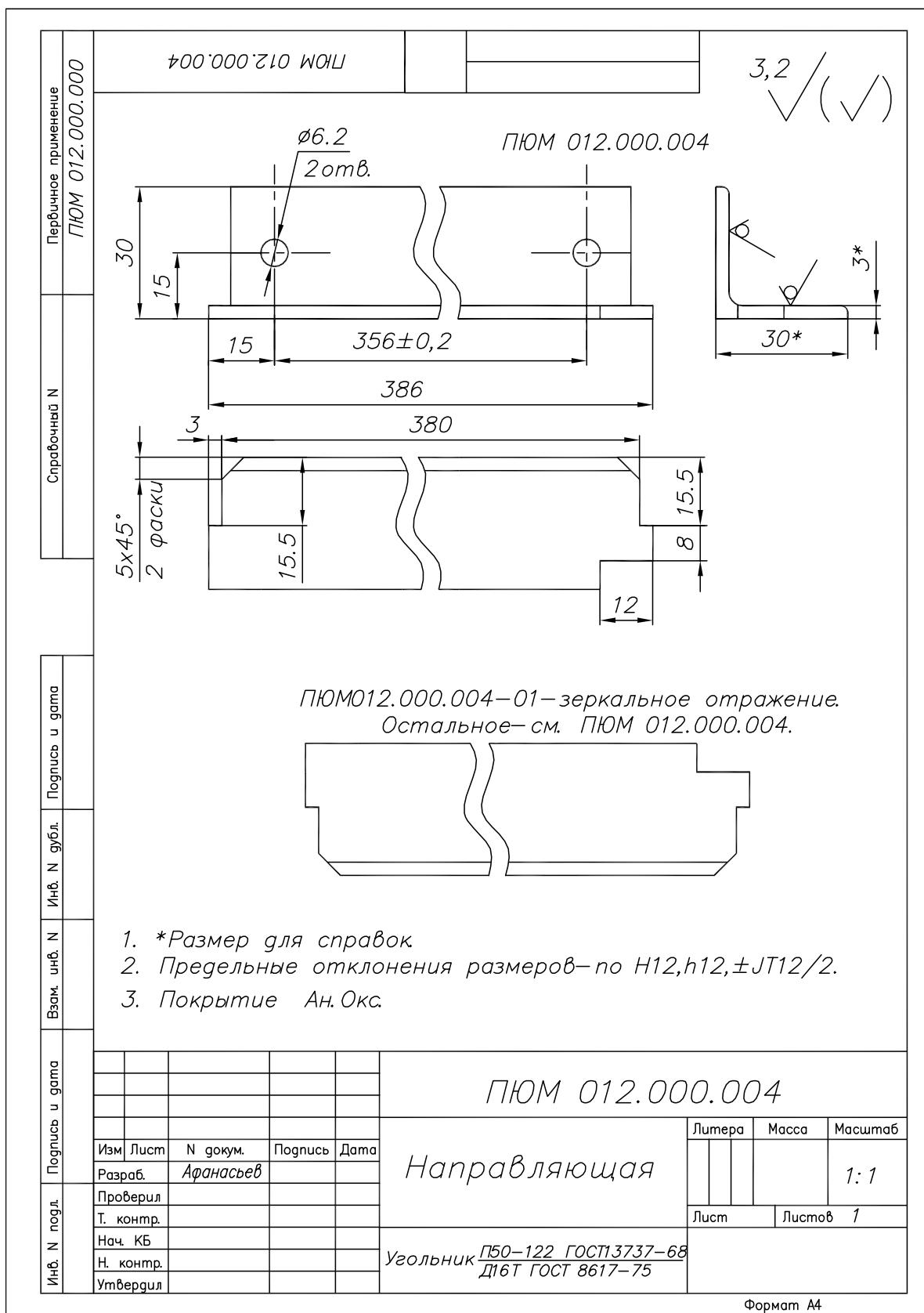


Рисунок А.3 – Чертеж направляющей

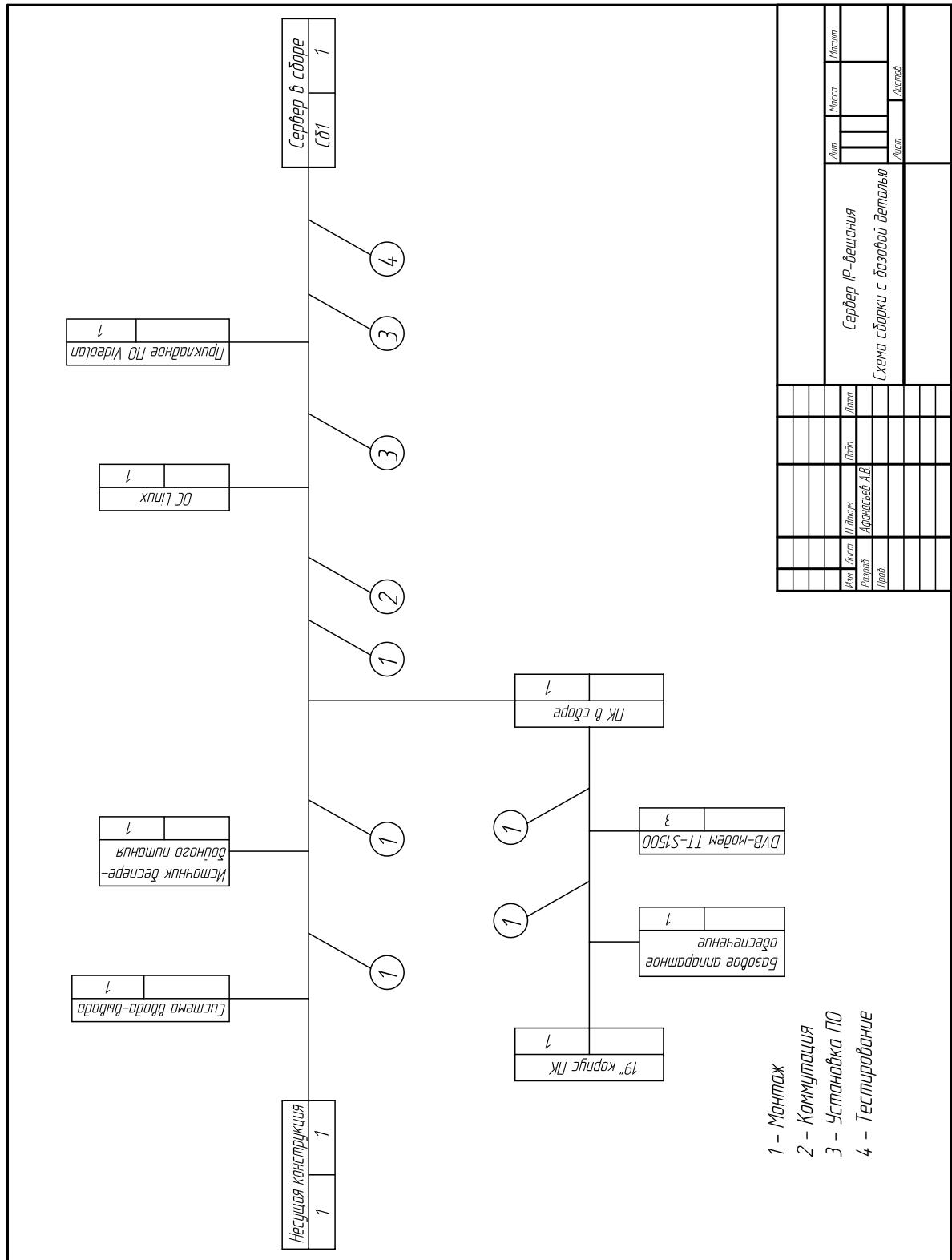


Рисунок А.4 – Схема сборки сервера вещания

ПРИЛОЖЕНИЕ Б  
Графический материал

# ИНФОРМАЦИОННЫЙ РАЗДЕЛ. Не входит в состав РПЗ

## Список иллюстраций

1.1 Классификация услуг сетей передачи данных . . . . .	13
1.2 Классификация источников мультимедийного контента . . . . .	16
1.3 Схемы доставки цифрового потока от сервера до клиента . . . . .	17
1.4 Противоречия в реализации системы IP-вещания . . . . .	20
1.5 Классификация форматов представления мультимедиа данных . . . . .	23
1.6 Структура мультимедийного вещания с помощью проекта VideoLAN . . . . .	32
1.7 Структура мультимедийного вещания с помощью продуктов Microsoft . . . . .	33
2.1 Распределение компонент цветности в 4:2:0, 4:2:2 и 4:4:4 представлении YCbCk . . . . .	37
2.2 Примеры расчета PSNR: а) исходный кадр, б) $PSNR = 30.6 \text{ dB}$ , в) $PSNR = 28.3 \text{ dB}$ . . . . .	39
2.3 Кадр с $PSNR = 27.7 \text{ dB}$ (размыт фон) . . . . .	40
2.4 Структурная схема кодировщика видео . . . . .	41
2.5 Порядок работы DPCM . . . . .	42
2.6 Функция 2D автокорреляции для исходного изображения в пространственной области . . . . .	43
2.7 Функция 2D автокорреляции для исходного изображения в частотной области . . . . .	43
2.8 Базисные шаблоны ДКП размерности $4 \times 4$ . . . . .	44
2.9 Блок $4 \times 4$ яркостной составляющей изображения . . . . .	44
2.10 Результат инверсного ДКП: а) полного; б) 1 коэффициент матрицы ДКП; в) 2 коэффициента матрицы ДКП; г) 3 коэффициента матрицы ДКП; д) 4 коэффициента матрицы ДКП; е) 5 коэффициентов матрицы ДКП; ж) 6 коэффициентов матрицы ДКП; з) 7 коэффициентов матрицы ДКП . . . . .	45
2.11 Пример двумерного вейвлет-преобразования . . . . .	46
2.12 Типовое распределение вероятности нахождения ненулевых коэффициентов в квантованной матрице ДКП преобразования . . . . .	47
2.13 Схема работы зиг-заг преобразования . . . . .	47
2.14 Коэффициент вейвлет-преобразования и его «дети» . . . . .	48
2.15 Процесс декодирования данных, закодированных с помощью арифметического кодирования . . . . .	49
2.16 Структурная схема кодировщика H.264 . . . . .	52
2.17 Структурная схема декодера H.264 . . . . .	52
2.18 Возможные комбинации разделения макроблока на субблоки . . . . .	53
2.19 Выбор размера блоков для операции предсказания движения . . . . .	54
2.20 Схема интерполяции яркостной составляющей макроблока . . . . .	54
2.21 Схема интерполяции цветностных составляющих макроблока . . . . .	55

2.22	Варианты интра-предсказания для блоков $4 \times 4$	56
2.23	Границы макроблоков, подвергающиеся фильтрации	57
2.24	Последовательность сканирования блоков внутри макроблока	58
3.1	Классификация способов защиты телевещания от несанкционированного доступа	65
3.2	Классификация методов идентификации абонентов	66
3.3	Многоуровневая модель разграничения доступа стандарта DVB-CSA	67
3.4	Структурная схема работы защиты контента в IP вещания	68
3.5	Диаграмма вариантов использования защищенной системы IP-вещания	72
3.6	S-box - таблица замены для байта <b>xy</b> (в шестнадцатеричном формате)	75
3.7	Алгоритм установления сессии SSL	80
4.1	Структурная схема системы IP-вещания	84
4.2	Диграмма вариантов использования подсистемы управления пользователей	85
4.3	Разработанные интерфейсы подсистемы абонентского управления	88
4.4	Разработанные интерфейсы подсистемы управление вещанием	88
4.5	Логическая модель базы данных управления пользователями	89
4.6	Логическая модель базы данных управления вещанием	91
4.7	Базовые компоненты подсистемы формирования контента IP-вещания	94
4.8	Варианты реализации формирования и доставки контента до абонентов	95
4.9	Пример построения подсистемы формирования контента	96
4.10	Диаграмма взаимодействий подсистемы формирования контента	96
4.11	Функциональная схема аналогового ТВ тюнера	99
4.12	Функциональная схема платы захвата с аппаратным MPEG кодированием	100
4.13	Функциональная схема спутникового приемника DVB-S	102
4.14	Варианты реализации формирования контента на основе аналогового вещания	103
4.15	Варианты реализации формирования контента на основе цифрового вещания в формате H.264	104
4.16	Варианты реализации формирования контента на основе цифрового вещания в формате MPEG-2	104
4.17	Вариант реализации формирования контента на основе IP-TV вещания	105
4.18	Гибридная архитектура сетевой подсистемы мультимедийного вещания	107
4.19	Формат заголовка RTP пакета	108
4.20	Диаграмма состояния протокола взаимодействия клиента с сервером	111
4.21	Диаграмма вариантов использования подсистемы доступа к потоковому вещанию	115
4.22	Внешний вид и компоненты управления ПО доступа к потоковому вещанию	116
4.23	Окно общей настройки программы	117
4.24	Окно записи принимаемых мультимедийных данных на диск	117
4.25	Окно создания и редактирования элементов планировщика заданий	117

4.26	Домашняя страница студии мультимедийных образовательных технологий кафедры ИУ4 МГТУ им.Н.Э.Баумана . . . . .	118
5.1	Модель SolidWorks НК сервера вещания . . . . .	121
5.2	Реализованная НК сервера вещания . . . . .	121
5.3	Блок схема испытания на обнаружение результатов . . . . .	122
5.4	Блок схема испытания на устойчивость к синусоидальной вибрации . . . . .	122
5.5	Расположение спутниковых тарелок приема сигнала со спутников . . . . .	123
5.6	Экспериментальный вещательный сервер . . . . .	123
5.7	Опытный образец блока сервера вещания . . . . .	123
5.8	Статистика использования каналов передачи данных . . . . .	127
5.9	Статистика использования IP-TV вещания . . . . .	128
A.1	Сборочный чертеж тумбы 14U . . . . .	135
A.2	Сборочный чертеж стойки . . . . .	136
A.3	Чертеж направляющей . . . . .	137
A.4	Схема сборки сервера вещания . . . . .	138

### Список таблиц

1.1	Сравнительные характеристики требований к мультимедийному вещанию . . . . .	15
1.2	Оценка источников мультимедийного контента . . . . .	16
1.3	Оценка параметров unicast и multicast . . . . .	18
1.4	Достоинства и недостатки NTSC . . . . .	24
1.5	Достоинства и недостатки PAL . . . . .	25
1.6	Достоинства и недостатки SECAM . . . . .	26
1.7	Сравнительные характеристики форматов представления мультимедийного контента . . . . .	30
1.8	Сравнительные характеристики организации мультимедийного вещания . . . . .	31
2.1	Режимы интра-предсказаний $4 \times 4$ блоков . . . . .	56
2.2	Режимы интра-предсказаний $16 \times 16$ блоков . . . . .	57
3.1	Спецификация диаграммы вариантов использования защищенной системы IP-вещания . . . . .	69
3.2	Комбинации длин ключа, шифруемого блока и числа раундов AES . . . . .	73
3.3	Результат тестирования работы симметричного шифрования с помощью библиотеки OpenSSL . . . . .	82
3.4	Результат тестирования работы асимметричного шифрования с помощью библиотеки OpenSSL . . . . .	82
4.1	Спецификация диаграммы вариантов использования подсистемы управления пользователями . . . . .	86
4.2	Спецификация логической модели базы данных управления пользователями . . . . .	89
4.3	Спецификация логической модели базы данных управления вещанием . . . . .	91

4.4	Спецификация диаграммы взаимодействий подсистемы формирования контента . . . . .	97
4.5	Спецификация диаграммы состояния протокола установления соединения для доступа абонентов к ресурсам вещания . . . . .	111
4.6	Спецификация для диаграммы вариантов использования подсистемы доступа к потоковому вещанию . . . . .	115
5.1	Перечень тестовых заданий для определения дифференциальных оценок качества программного обеспечения . . . . .	125
5.2	Результаты испытаний программного обеспечения . . . . .	126

### **Перечень листингов**

3.1	Псевдокод алгоритма AES . . . . .	74
3.2	Псевдокод алгоритма выработки итерационных ключей AES . . . . .	76
4.1	Фрагмент выборочной отправки данных клиенту на основании заголовка RTP пакета . . . . .	110
4.2	Спецификация формата получаемых данных во время установления соединения . . . . .	113
4.3	Спецификация протокола запросов мультимедийных данных и получения ключей декрамблирования . . . . .	114