

Московский Государственный Технический Университет
им.Н.Э.Баумана

Магистерская диссертация по направлению 220500:
«Проектирование и технология производства ЭС»

Распределённая система мультимедийного вещания в сетях передачи данных

Афанасьев А.В.

научный руководитель:
доцент, к.т.н. Власов А.И

Москва, 2007

Цели и задачи

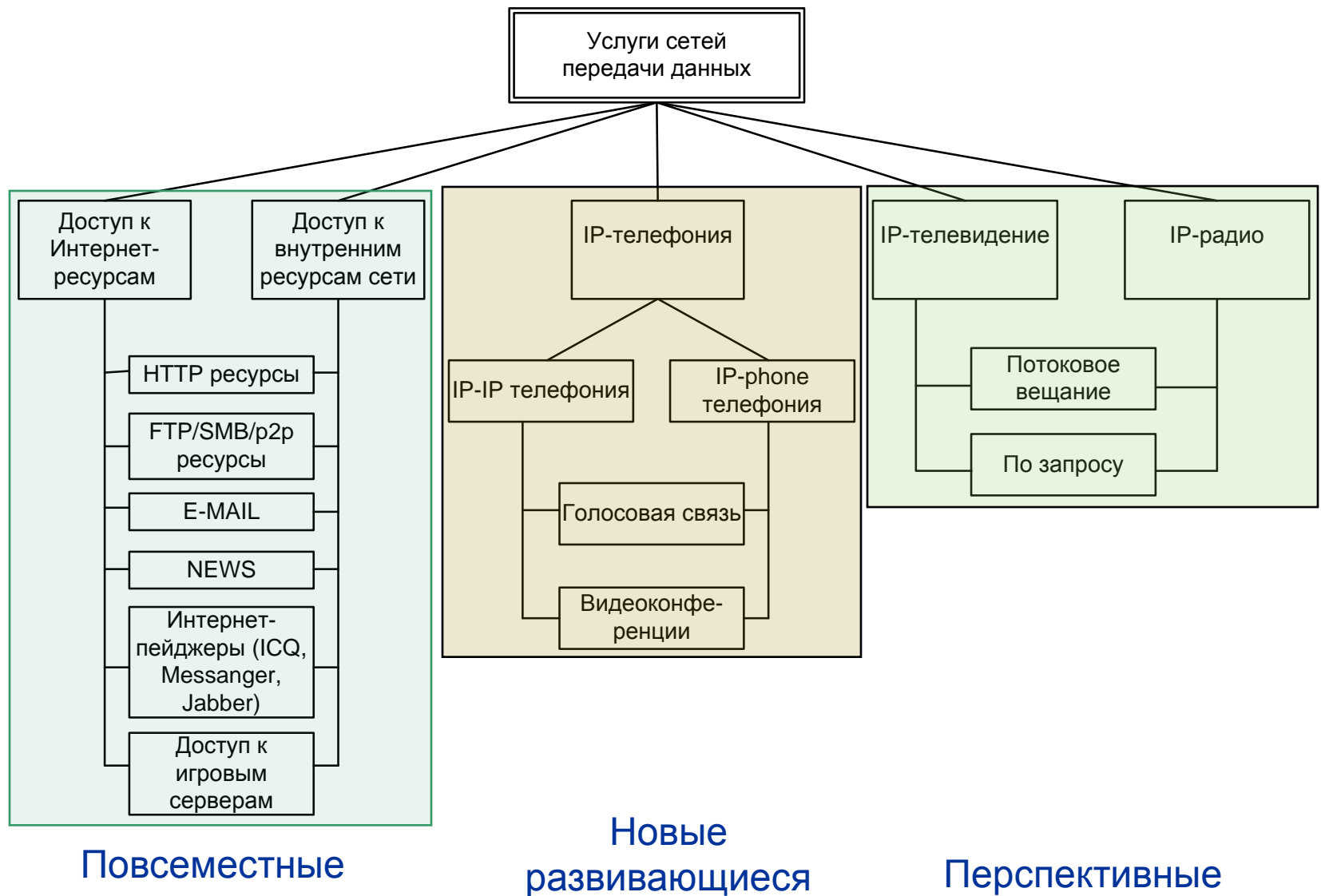
Цель работы:

Разрешение противоречий между возможностями и желаниями со стороны провайдеров IP-TV, так и между ожиданиями и предложениями услуг для пользователей системы

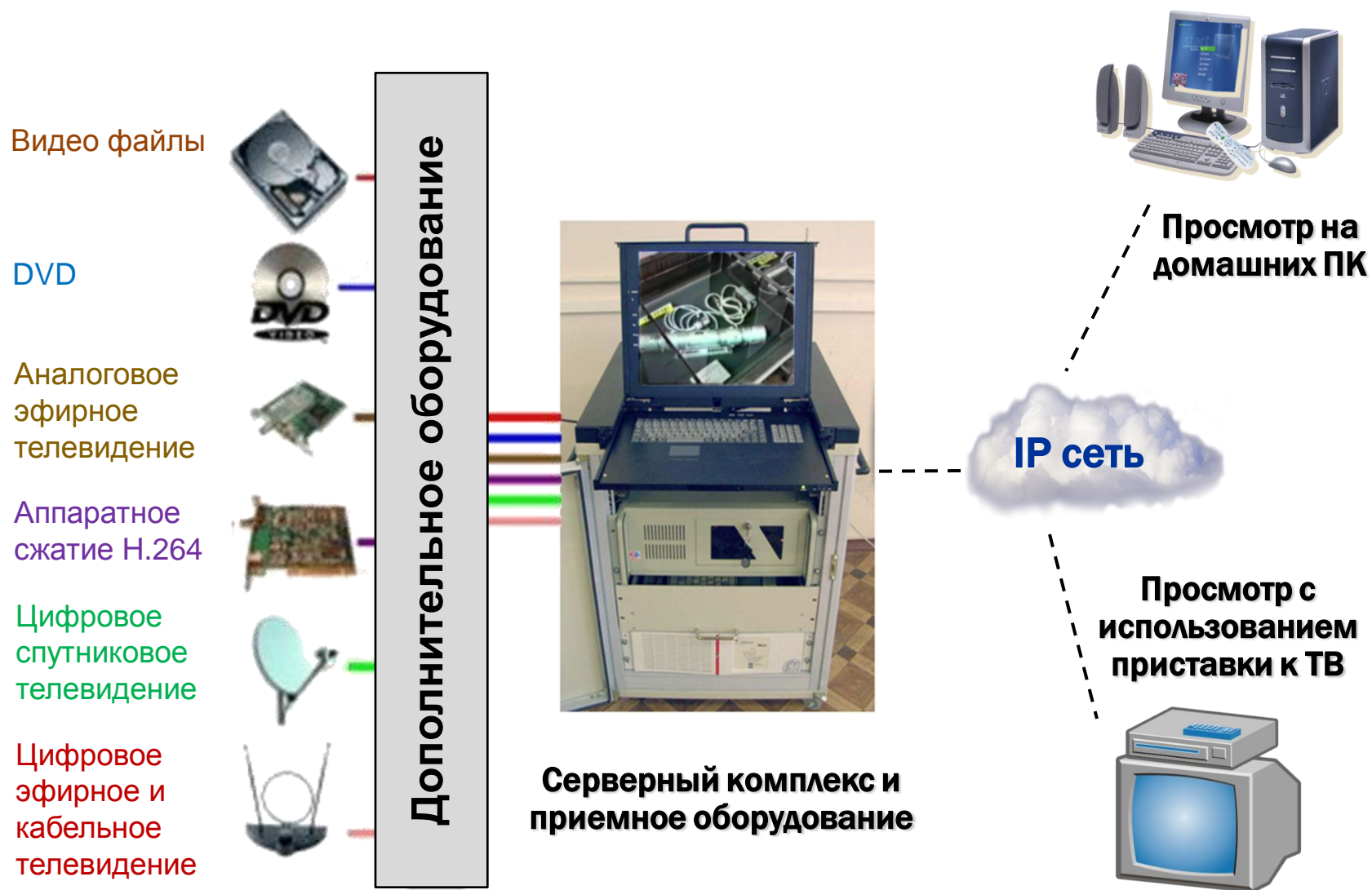
Решаемые задачи:

- Исследование принципов мультимедийного вещания в сетях передачи данных с классификацией технологий доставки информации от сервера до клиента и форматов представления мультимедийного контента.
- Изучение возможностей стандартизованных технологий представления и передачи мультимедийной информации в сетях передачи данных и математического аппарата применяемого в форматах представления мультимедийных данных в цифровом виде.
- Исследование способов защиты мультимедийной информации в DVB сетях и разработка схемы защиты мультимедийного вещания от несанкционированного доступа в рамках сетей передачи данных.
- Разработка серверного и клиентского программного обеспечения системы мультимедийного вещания.
- Построение опытного образца сервера вещания и его внедрение в эксплуатацию.

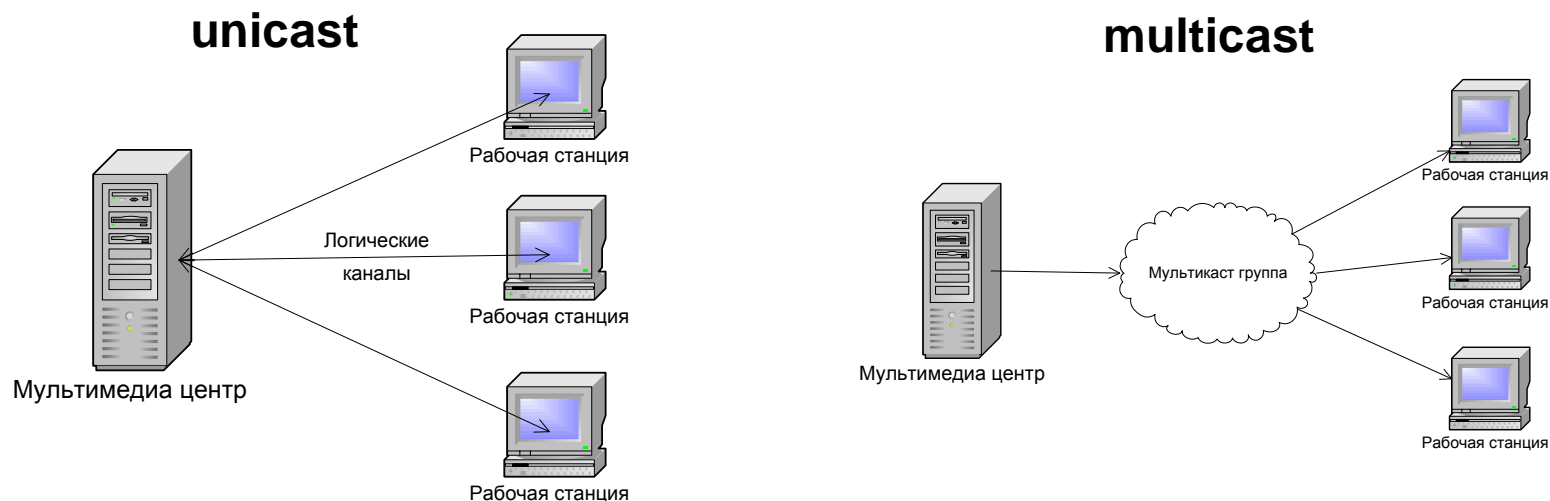
Услуги в сетях передачи данных



Структура вещания в сетях передачи данных



Схемы предоставления мультимедийных услуг



<i>Особенности</i>	
<p>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.</p>	<p>Опосредованная передача данных от сервера клиенту, осуществляемая с помощью входа сервера и клиентов в т.н. multicast группы []. 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</p>
<i>Используемые протоколы</i>	
<p>передачи: TCP, UDP, RTP, HTTP маршрутизации: RIP, BGP, OSPF</p>	<p>UDP, RTP IGMP</p>
<i>Каналообразующее оборудование, поддерживающее передачу по схемам</i>	
<p>Все оборудование, поддерживающее передачу данных по протоколу IP</p>	<p>Маршрутизаторы, поддерживающие протокол маршрутизации IGMP Коммутаторы с поддержкой IGMP Snooping Прочие коммутаторы и концентраторы с передачей multicast пакетов в широковещательном режиме</p>

Структура системы мультимедийного вещания



Подсистема контроля и управления

Цели подсистемы:

- задание нужного режима работы системы в целом, т.е. формирование и контроль передачи данных из подсистемы формирования контента в абонентскую подсистему посредством сетевой подсистемы;
- обеспечение необходимого уровня качества работы путем сбора статистической информации на каждом этапе формирования, передачи и получения данных.

Проблемы:

трудность реализации разграничения доступа абонентов и защиты от несанкционированного доступа к услугам IP-вещания

Поиск Добавить Статистика Настройки

ФИО	Комната	Login	Дата создания	Создатель	Действие
Афанасьев Александр Владимирович	5-608	sawka	2005-09-03 18:05:20	sawka	[Удалить]

Всего найдено пользователей: 1

Изменение данных пользователя

Доступ для 192.168.5.8 с 2005-11-03 по 2006-11-03

ФИО:

Комната:

Доступ для 192.168.56.208 с 2005-09-10 по 2005-10-10

Login:

Пароль:

Комментарий:

Создатель: sawka IP: 192.168.

Дата создания: 2005-09-03 18:05:20 Месяцев:

Абонентское управление



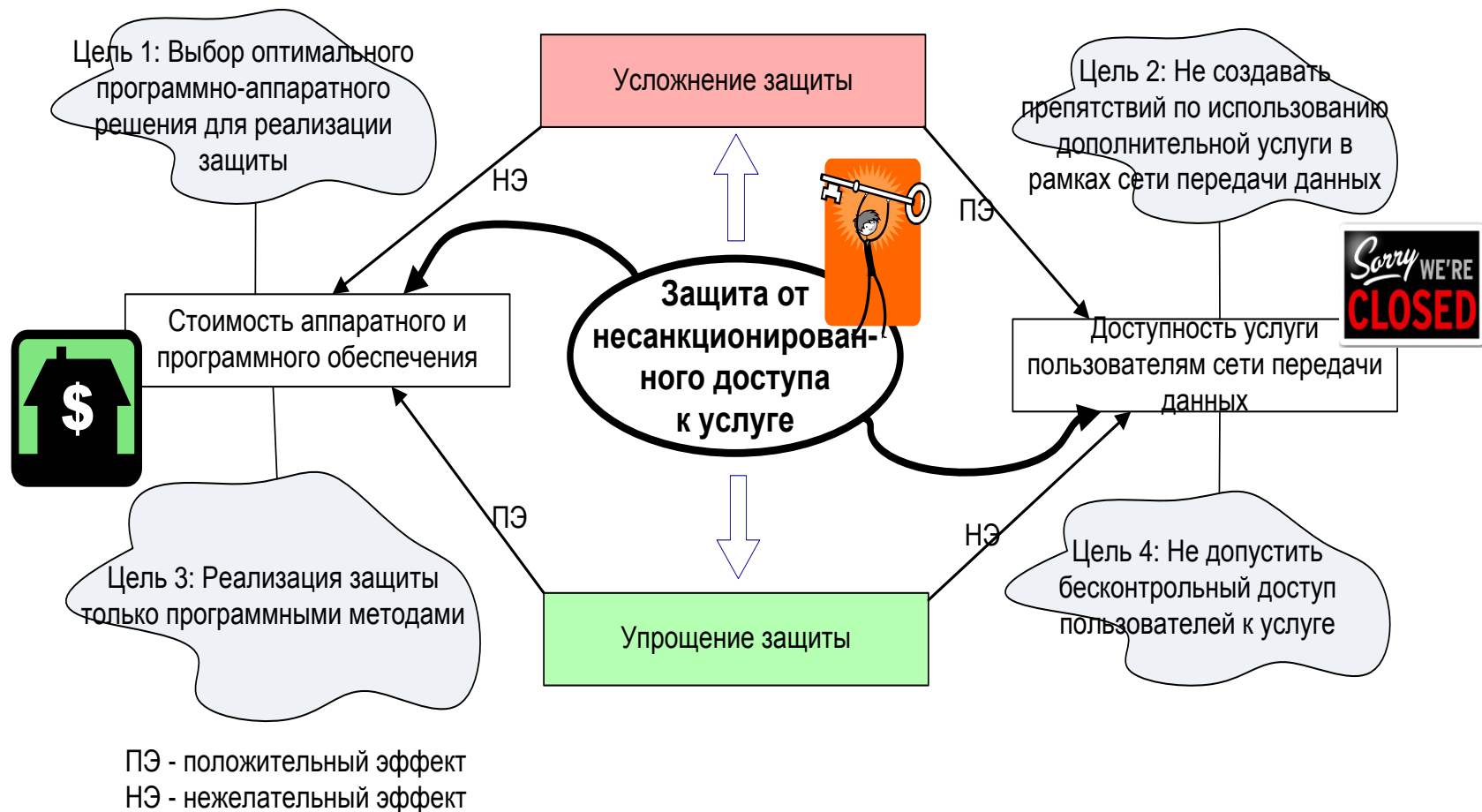
Доступ к статистике

Управление ICNV

Категория	Действие	АвтоRun	Название	Спутник	Транспортер	Программа	Канал	
Спутники	STOP	>>>	Armal	Eutelsat_W4	12 075 L (Q-Star)	Armal	chac29	Редактировать Удалить
Транспортеры	STOP	>>>	ArvoRadio	Eutelsat_W4	12 075 L (Q-Star)	Arvo Radio	radio11	Редактировать Удалить
Каналы	STOP	>>>	Chavari	Eutelsat_W4	12 075 L (Q-Star)	Chavari	radio09	Редактировать Удалить
Наличие оборудования	STOP	>>>	Dream1	Eutelsat_W4	12 075 L (Q-Star)	Dream1 FM	radio02	Редактировать Удалить
DVB-S модемы	STOP	>>>	Sao Marcos	Eutelsat_W4	12 075 L (Q-Star)	Eho Melros	chac02	Редактировать Удалить
Мульти-канал	STOP	>>>	Enigma	Eutelsat_W4	12 075 L (Q-Star)	Enigma	radio08	Редактировать Удалить
Мульти-канал группы	STOP	>>>	HR FM	Eutelsat_W4	12 075 L (Q-Star)	HR FM	radio03	Редактировать Удалить
Мульти-канал группы	STOP	>>>	Melody Volna	Eutelsat_W4	12 075 L (Q-Star)	Melody Volna	radio06	Редактировать Удалить
Мульти-канал группы	STOP	>>>	Melody Caribe	Eutelsat_W4	12 075 L (Q-Star)	Melody Caribe	radio05	Редактировать Удалить
Мульти-канал группы	STOP	>>>	Melody Yoho	Eutelsat_W4	12 075 L (Q-Star)	Melody Yoho	chac26	Редактировать Удалить
Мульти-канал группы	STOP	>>>	Nov L&O	Eutelsat_W4	12 075 L (Q-Star)	Novaya Zhizn	radio03	Редактировать Удалить
Мульти-канал группы	STOP	>>>	OnLine News	Eutelsat_W4	12 075 L (Q-Star)	On-Line News	radio07	Редактировать Удалить
Мульти-канал группы	STOP	>>>	Radio R&R	Eutelsat_W4	12 075 L (Q-Star)	Ritonskaya Radio	chac25	Редактировать Удалить

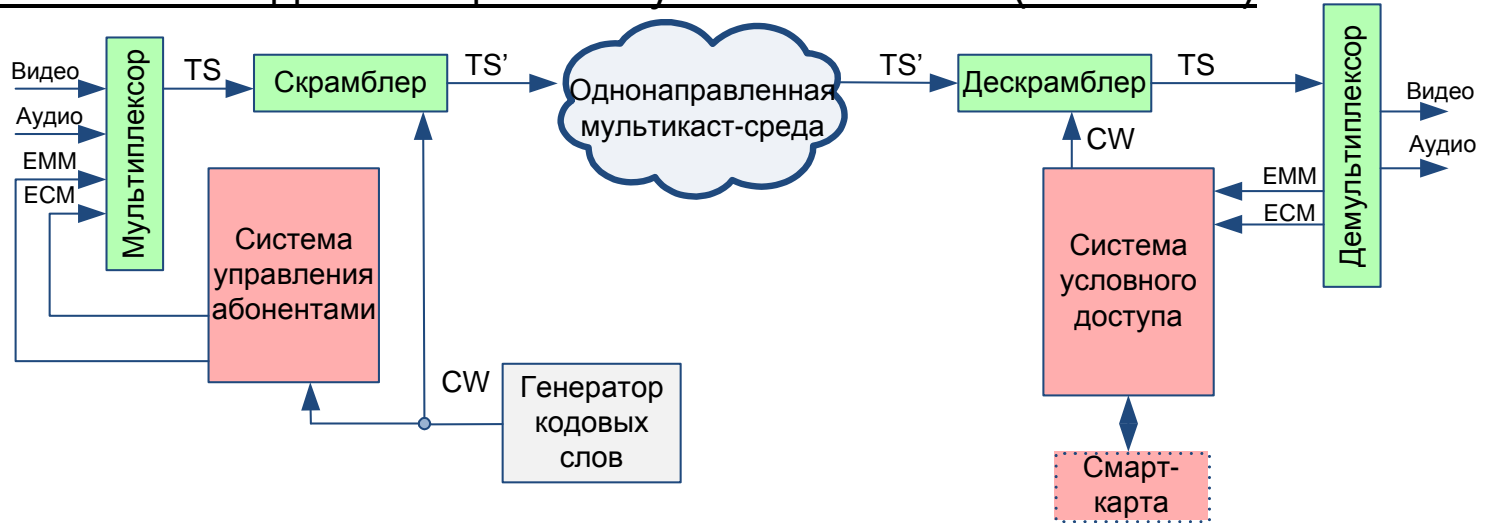
Управление вещанием

Противоречие, связанное с защитой от несанкционированного доступа

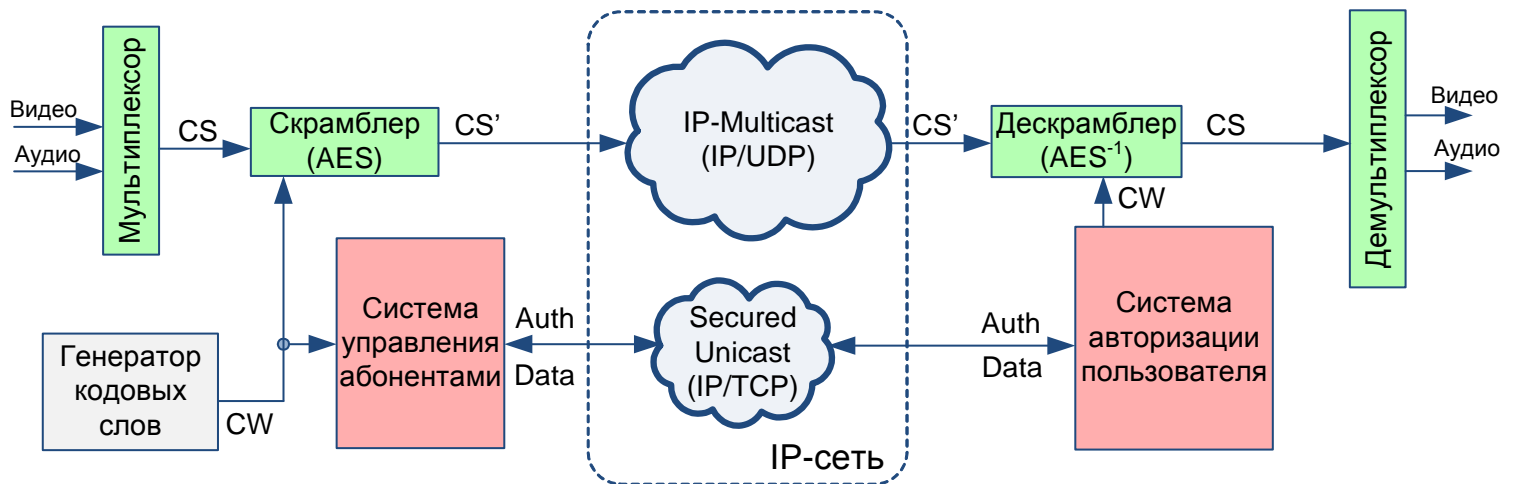


Разрешение противоречия – переход к гибридной модели защиты от несанкционированного доступа

Классическая модель защиты в мультикаст сетях (DVB-CSA)



Предлагаемая модель защиты в сетях передачи данных



Подсистема формирования контента

Цель подсистемы:

получение и преобразование получаемого контента из исходной (цифровой или аналоговой) формы в эффективный формат вещания – H.264/RTP

Проблемы:

а) Оцифрованное несжатое видео требует порядка 200 Mibit на 1 секунду видео (ТВ качество). Частично решает проблему сжатие с потерями, но больший уровень сжатия приводит к большим потерям данных => ухудшение качества видео

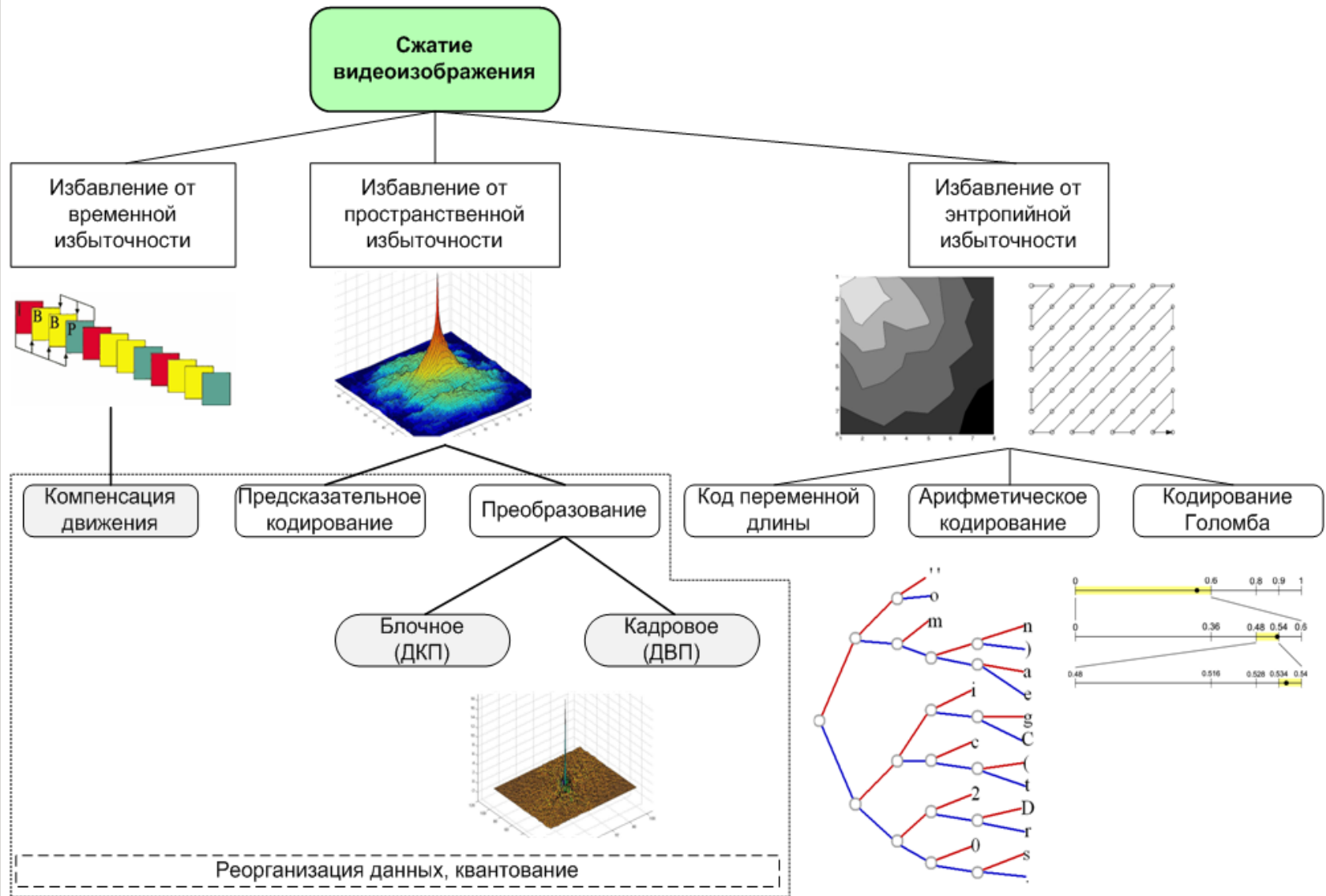
б) Множество различных по типу источников контента:

- Цифровое спутниковое/кабельное/эфирное вещание в формате DVB-S/C/T
- Аналоговое вещание, либо аналоговые источники мультимедийных данных (видеокамеры, видеомэгафоны) в формате PAL/SECAM/NTSC
- Файловые источники мультимедийных данных (DVD, AVI и MP4 файлы)
- Данные IP-TV вещания

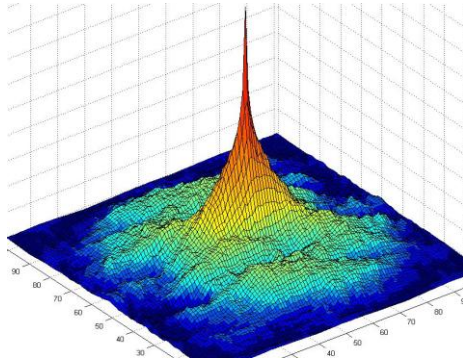
Противоречие, связанное с качеством вещаемого контента



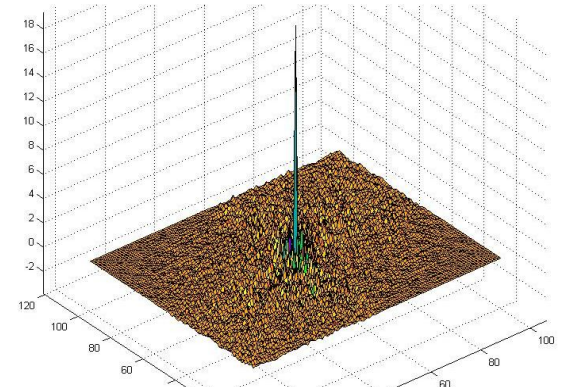
Разрешение противоречия **a** – повышение эффективности сжатия



Дискретное косинусное преобразование (ДКП) и H.264 преобразование



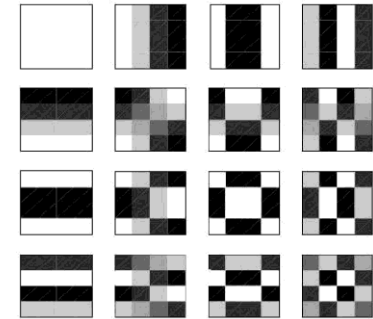
Автокорреляция внутри исходного блока



Автокорреляция внутри преобразованного блока

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

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



Базисные шаблоны

Н.264 преобразование:

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

Инверсное Н.264 преобразование:

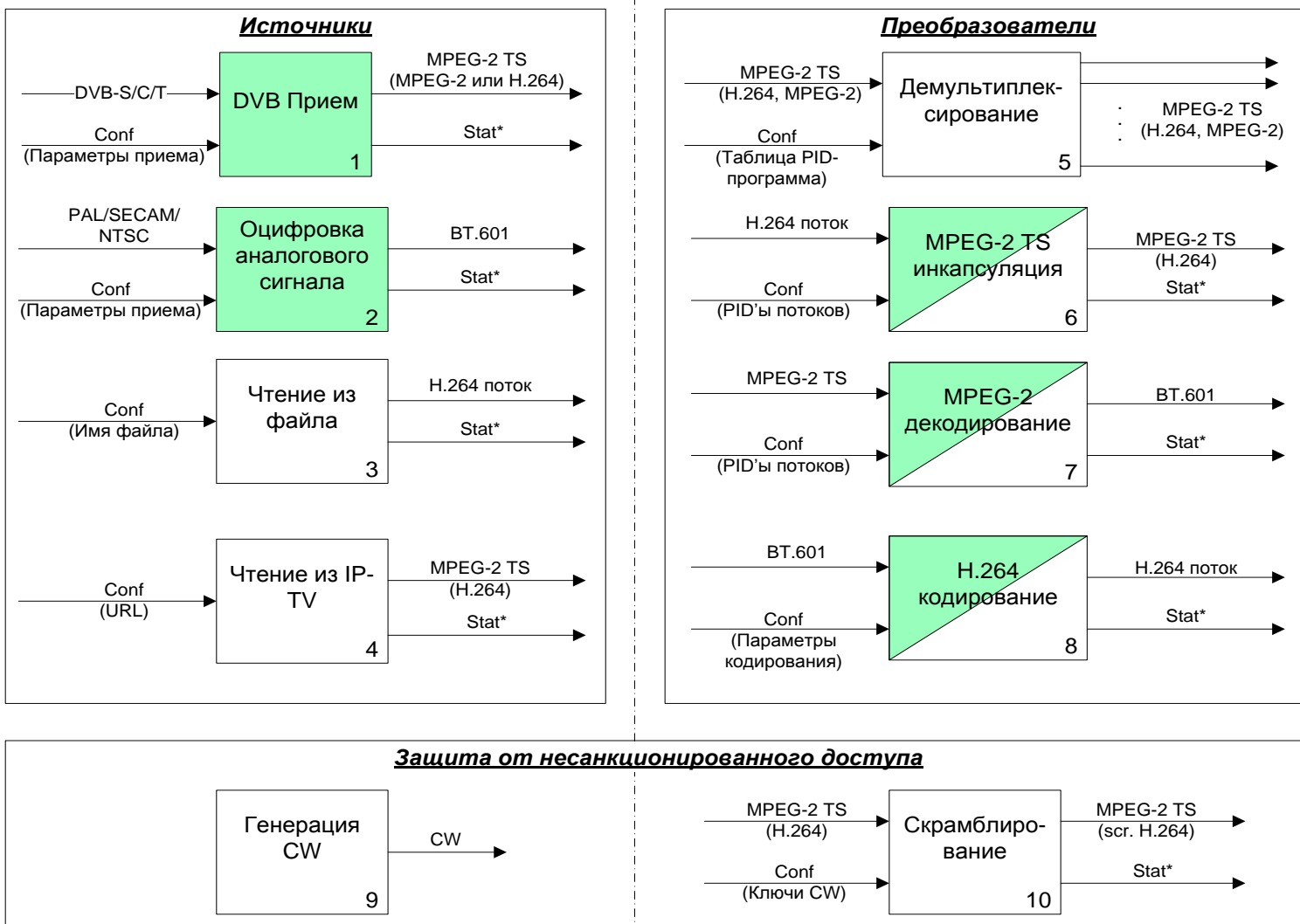
$$X = C_i^T (Y \otimes E_i) C_i = \begin{bmatrix} 1 & 1 & 1 & \frac{1}{2} \\ 1 & \frac{1}{2} & -1 & -1 \\ 1 & -\frac{1}{2} & -1 & 1 \\ 1 & -1 & 1 & -\frac{1}{2} \end{bmatrix} \left(\begin{bmatrix} Y \\ \end{bmatrix} \otimes \begin{bmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2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

Разница между ДКП и Н.264 преобразованием

5	11	8	10
9	8	4	12
1	10	11	4
19	6	15	7

$$Y - Y' = \begin{bmatrix} 0 & 0.079 & 0 & 0.008 \\ -0.295 & -0.868 & -0.664 & 0.190 \\ 0 & 0.341 & 0 & -0.203 \\ 0.224 & 0.190 & -0.055 & 0.868 \end{bmatrix}$$

Разрешение противоречия **Б** – модульное построение подсистемы



Использование для реализации блока специализированного аппаратного обеспечения

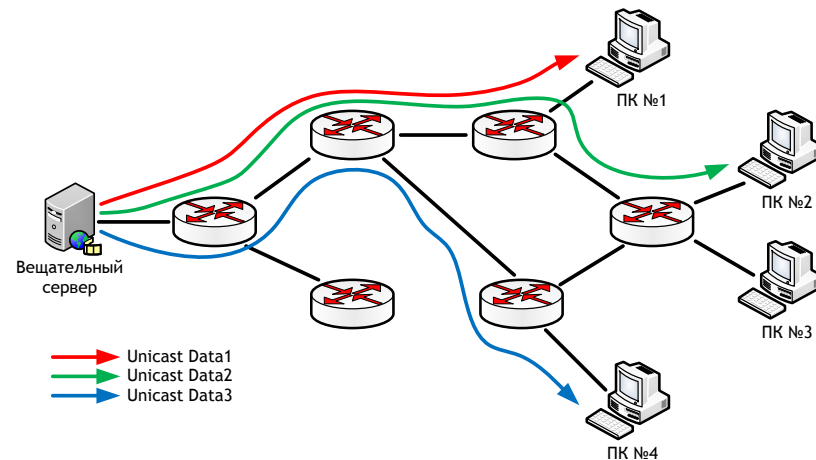
Сетевая подсистема

Цель подсистемы:

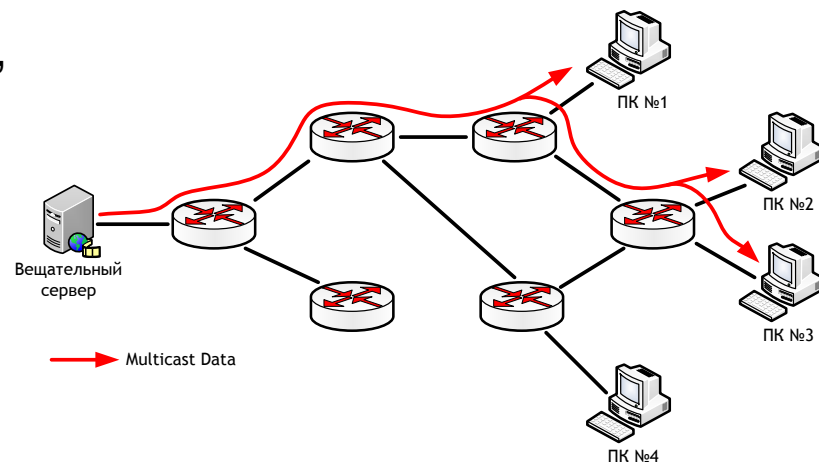
данных из подсистемы формирования контента в абонентскую

Проблемы:

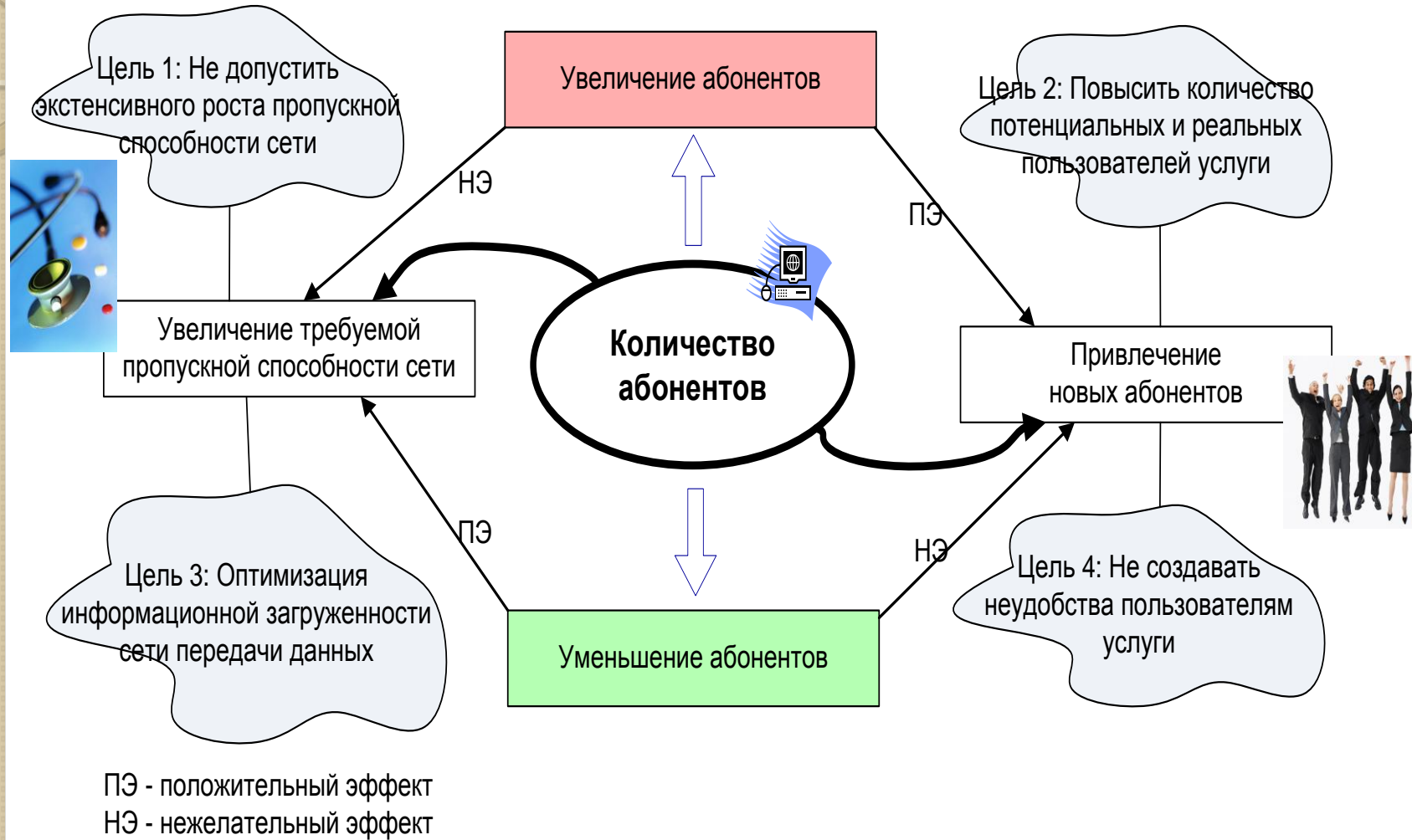
Использование юникаст (unicast, точка-точка) максимально защищает систему от несанкционированного доступа, но ограничивает либо качество видео, либо количество абонентов



Использование мультикаст (multicast, точка-многоточка) решая проблемы юникаст, требует наличия специального каналобразующего оборудования и создает сложности реализации системы защиты вещания от несанкционированного доступа



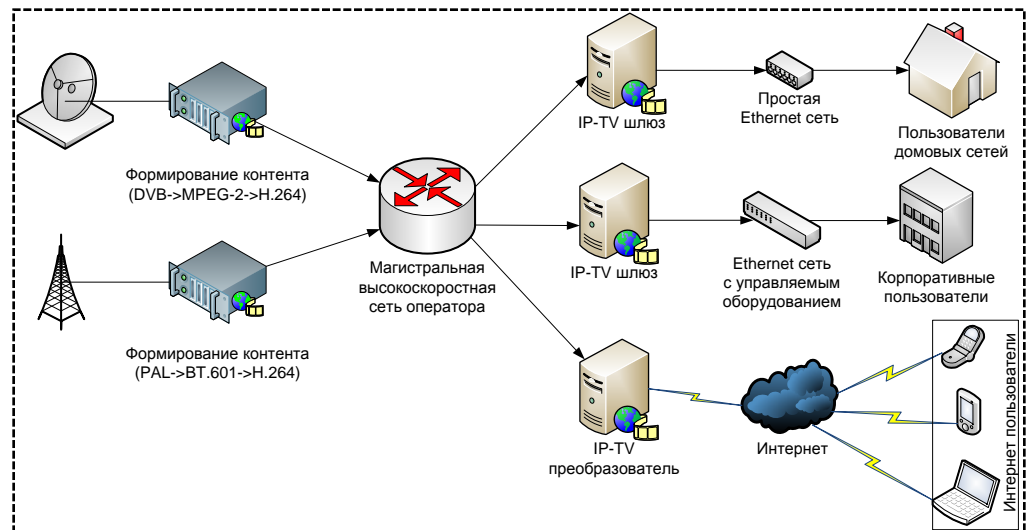
Противоречие, связанное с количеством абонентов



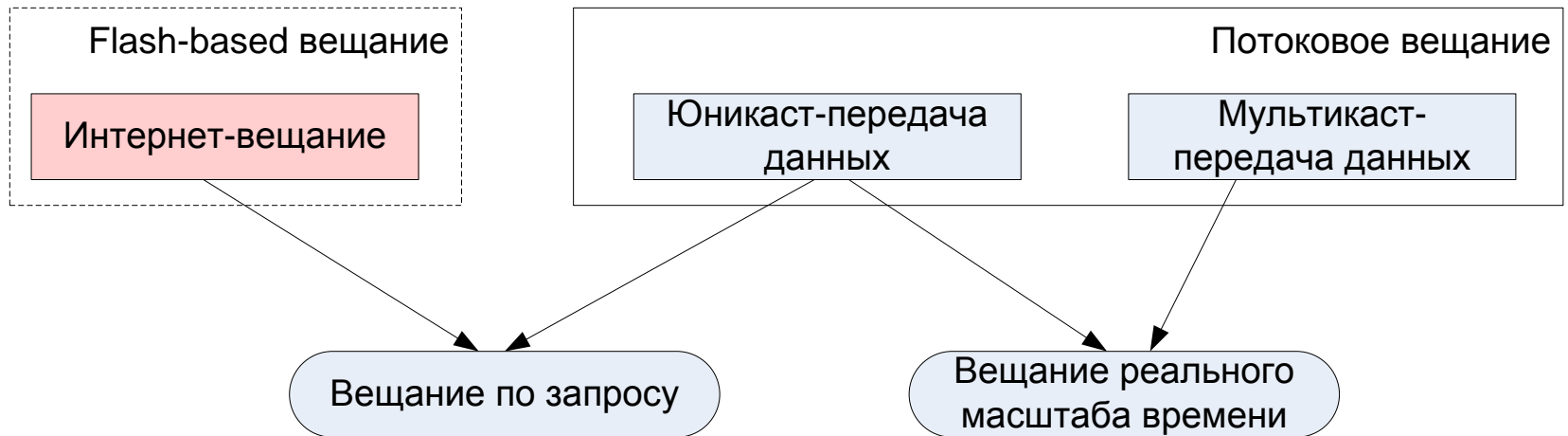
Разрешение противоречия – гибридная архитектура сетевой подсистемы



Пример гибридной архитектуры: магистральная сеть оператора, наполненная сформированным контентом, доставка абонентам по юникаст сетям через IP-TV шлюзы



Абонентская подсистема



Цель подсистемы:

реализация удобного и понятного (эргономичного) интерфейса пользователя доступа к вещанию

В рамках потокового вещания:

Разработка прикладного ПО получения и отображения мультимедийных данных и сопроводительной информации (название канала, информационное сопровождение)

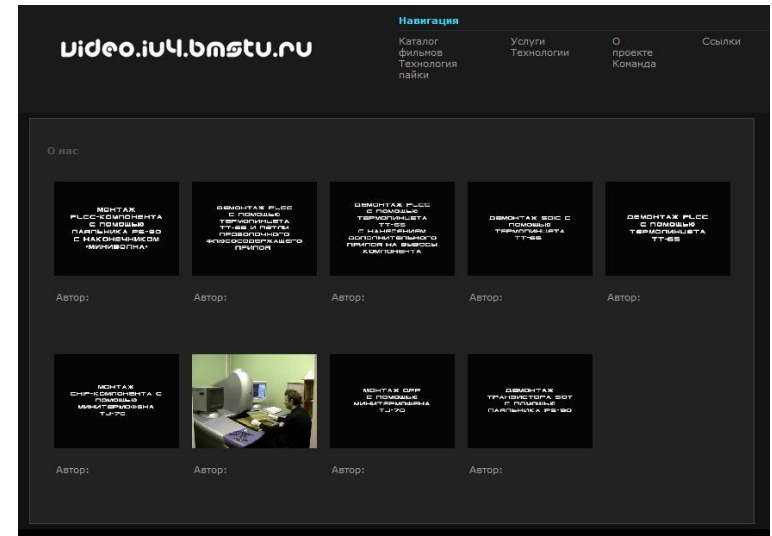
В рамках Интернет-вещания:

Разработка H.264->FlashVideo автоматизированного конвертера и WEB-портала доступа к вещанию

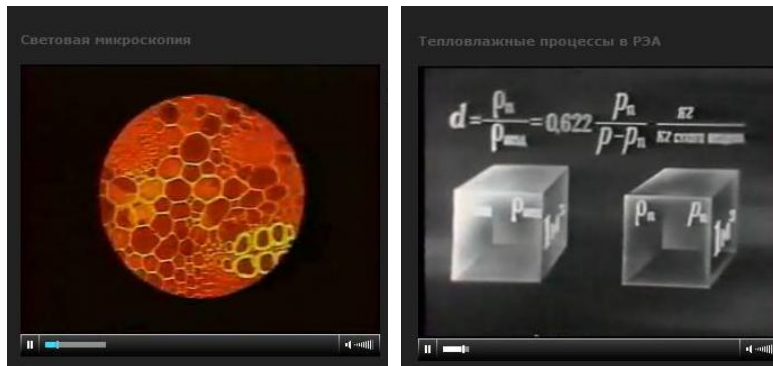
Доступ к Интернет-вещанию системы телеобучения «Электрон Медиа»



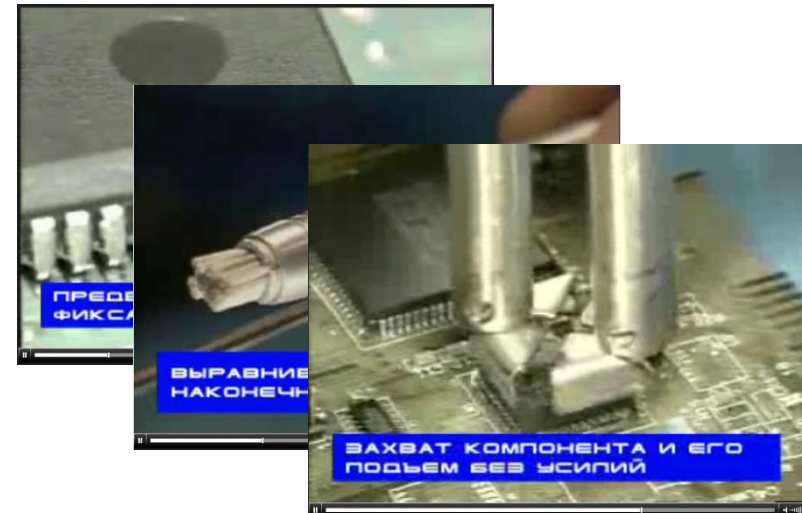
Заглавная страница – новый обучающий материал



Тематическое видео - технология пайки



Тематическое видео – световая микроскопия и тепловлажные процессы в РЭА



Разработка сервера вещания



Разработка 3D НК в стандарте Евромеханика

Разработка оптимальной комплектации (19" исполнение, компактность, расширяемость, мин стоимость)

Разработка ПО Videolan

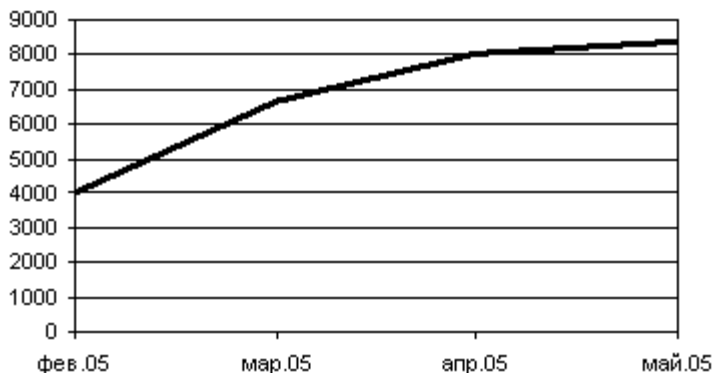
Экспериментальное исследование



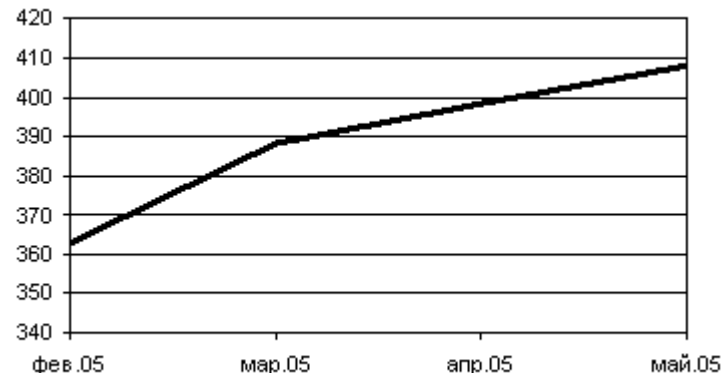
Антенны приема сигнала со спутника Eutelsat W4 (36° в.д.) и Sirius 2/3 (5° в.д.)



Блок ресиверов приема и декодирования мультимедийного контента со спутников и сервер вещания



Ежемесячное число запросов мультимедийных потоков (каналов)



Ежемесячное число уникальных IP адресов, с которых осуществлялся доступ

Выводы

Исследована архитектура самого эффективного с точки зрения отношения качества видео к требуемому потоку данных: кодека H.264

Разработана технология защиты от несанкционированного доступа к IP-вещанию, отличающейся применением гибридной модели разграничения доступа

Разрешены противоречия между использованием дешевой структуры сети (неуправляемое оборудование, отсутствие приоритезации трафика внутри сети) и желанием использовать качественное мультимедийное вещание в рамках этой сети

Создан опытный образец сервера вещания на основе спроектированной по стандартам Евромеханика несущей конструкции в рамках работы по гранту фирмы **Lucent**

Реализована система Интернет-вещания в рамках проекта телеобучения «Электрон Медиа»



Опытный образец



Электрон Медиа

Апробация работы

Положения работы докладывались

- на IV, V, VII Молодежной научно-технической конференции «Наукоемкие технологии и интеллектуальные системы» (2002, 2003, 2005 г.г.),
- на «Федеральная итоговая научно-техническая конференции творческой молодежи России по естественным, техническим, гуманитарным наукам» (2003) – диплом победителя, грант,
- на открытом конкурсе ОАО «Мосэнерго» на лучший дипломный и курсовой проекты студентов вузов России (2004) - диплом,
- на Международном научно-техническом симпозиуме «Образование через науку» (2005),
- Всероссийском конкурсе инновационных проектов аспирантов и студентов по приоритетному направлению развития науки и техники «Информационно-телекоммуникационные системы» (2005) – диплом I степени, грант

Результаты работ отмечены :

- стипендиями правительства РФ (2004,2006 год)
- стипендиями АФК«Система» (2004,2005,2006 год)
- стипендией клуба «Императорского Технического Училища» (2005 год)
- премией АФК «Система» молодым ученым и специалистам (2007 год)



Печатные работы по теме

1. Афанасьев А.В., Анализ аппаратных средств получения мультимедийных данных для использования в IP вещании // Сборник научных трудов студенческой научной конференции «Наукоемкие технологии и интеллектуальные системы 2006», 19-20 апреля 2006 года М.: МГТУ им. Н.Э.Баумана
2. Афанасьев А.В., Аппаратно-программный комплекс для предоставления мультимедиа контента в IP сетях // Материалы 7-ой Молодежной научно-технической конференции «Наукоемкие технологии и интеллектуальные системы 2005», 20-21 апреля 2005 г., М.: МГТУ им.Н.Э.Баумана - С.123-129
3. Афанасьев А.В. Программно-аппаратный комплекс мультимедийного вещания в сетях передачи данных // Сборник материалов Всероссийского конкурса инновационных проектов аспирантов и студентов по приоритетному направлению развития науки и техники «информационно-телекоммуникационные системы» / Под. ред. А.О. Сергеева. - М.: ГНИИ ИТТ «Информика», 2005
4. Афанасьев А.В., Разработка программно-аппаратного комплекса потокового мультимедийного вещания в научно-образовательных сетях передачи данных // Всероссийская научная конференция «Информационные технологии в науке, образовании и экономике»; Тез. докл. Часть II. / Якутск: РИЦ «Офсет», 2005
5. Афанасьев А.В., MSTU - многофункциональный измерительный комплекс // Сборник научных трудов молодежной научно-технической конференции «Наукоемкие технологии и интеллектуальные системы 2003», 16-17 апреля 2003 года М.: МГТУ им. Н.Э.Баумана
6. Предложения по созданию программно-аппаратного комплекса для исследования активной виброзащиты / Под. ред. Шахнова В.А. Отчет о научно исследовательской работе «Разработка математических моделей и программно-технических средств экспериментальных исследований систем активной виброзащиты», по заказу Научного Центра Нейрокомпьютеров РАСУ, 2002

Внимание!

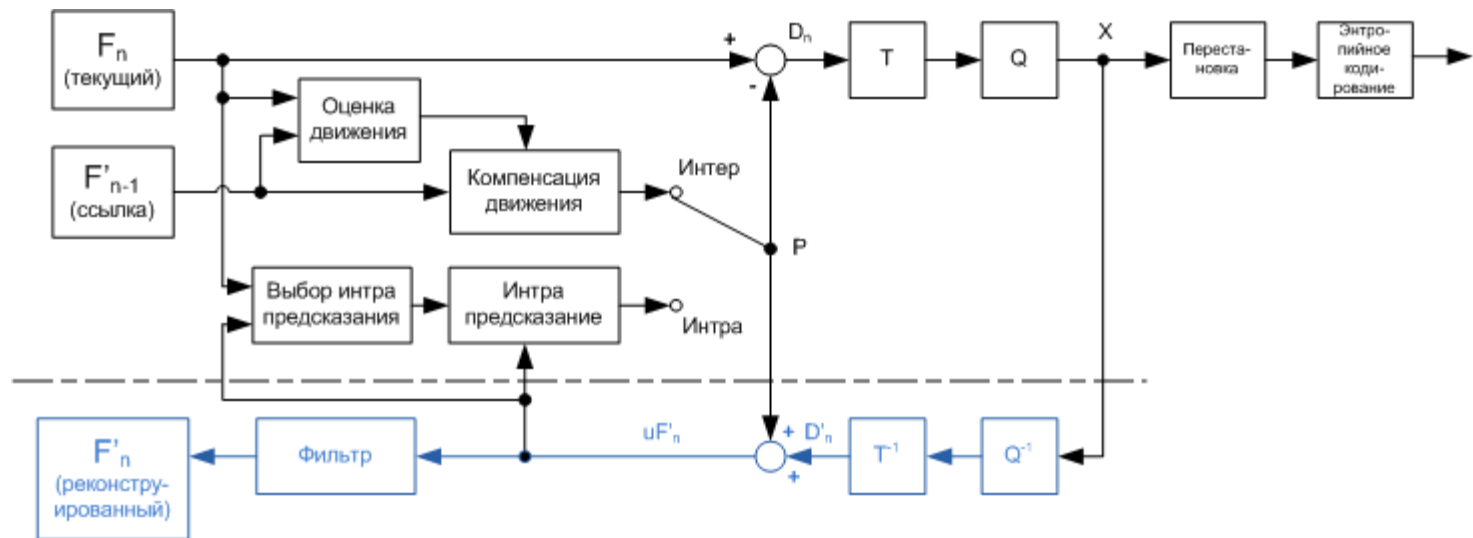
Демонстрация комплекса

Афанасьев А.В.

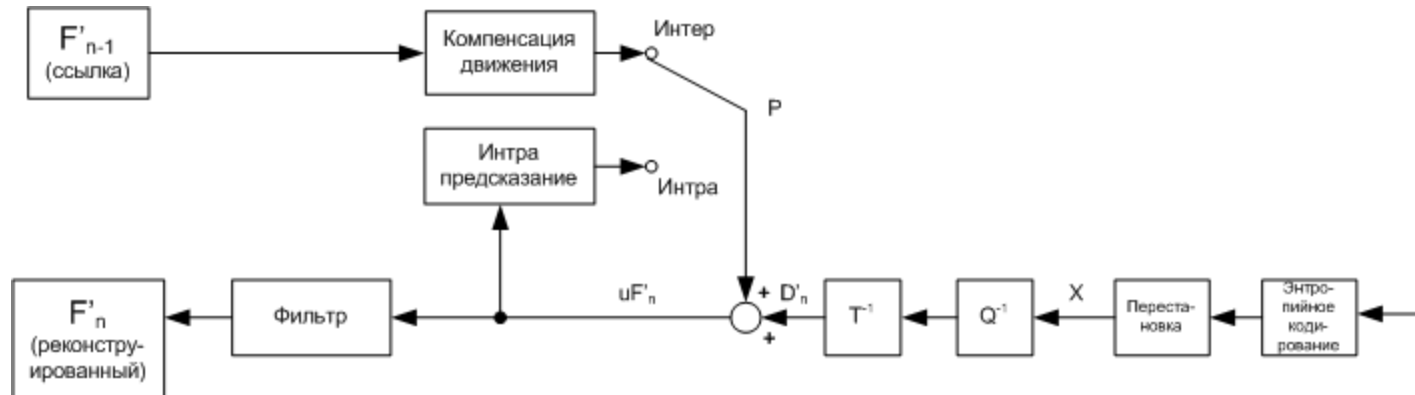
alex@icn.bmstu.ru

Гибридная модель кодека H.264

КОДЕР:



ДЕКОДЕР:



Симметричное шифрование AES

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

SubBytes - нелинейная замена байт

S-box

	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	45	4e	a9	6c	56	fa	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	00	54	bb	16

ShiftRows – циклический сдвиг

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

MixColumns – домножение столбцов (как многочлены над $GF[2^8]$) по модулю x^4+1 на многочлен $a(x)$

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

AddRoundKey – наложение итерационного ключа

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

Научная новизна работы

- Исследована и реализована архитектура системы мультимедийного вещания в сетях передачи данных, отличающаяся тем, что с целью эффективного использования каналов связи и расширения спектра услуг при сохранении как качества самой услуги мультимедийного вещания, так и ранее предоставляемых услуг передач данных, сервер вещания представляет собой набор размещенных в критических узлах сети передачи данных вспомогательных серверов, объединенных высокоскоростными каналами данных и соединенных с центральным координационным сервером, а пользователи используют механизм авторизации и аутентификации на вспомогательных серверах, получая при этом доступ ко всем ресурсам распределенной системы.
- Разработана технология защиты мультимедийных данных от несанкционированного доступа в рамках локальных вычислительных сетей, представляющая собой объединение мультикаст и юникаст технологий.

Достоверность полученных научных результатов подтверждена:

- 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.
- 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.