Московский Государственный Технический Университет им.Н.Э.Баумана

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

Распределенная система мультимедийного вещания в сетях передачи данных

Афанасьев А.В.

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

Москва, 2007

Цели и задачи

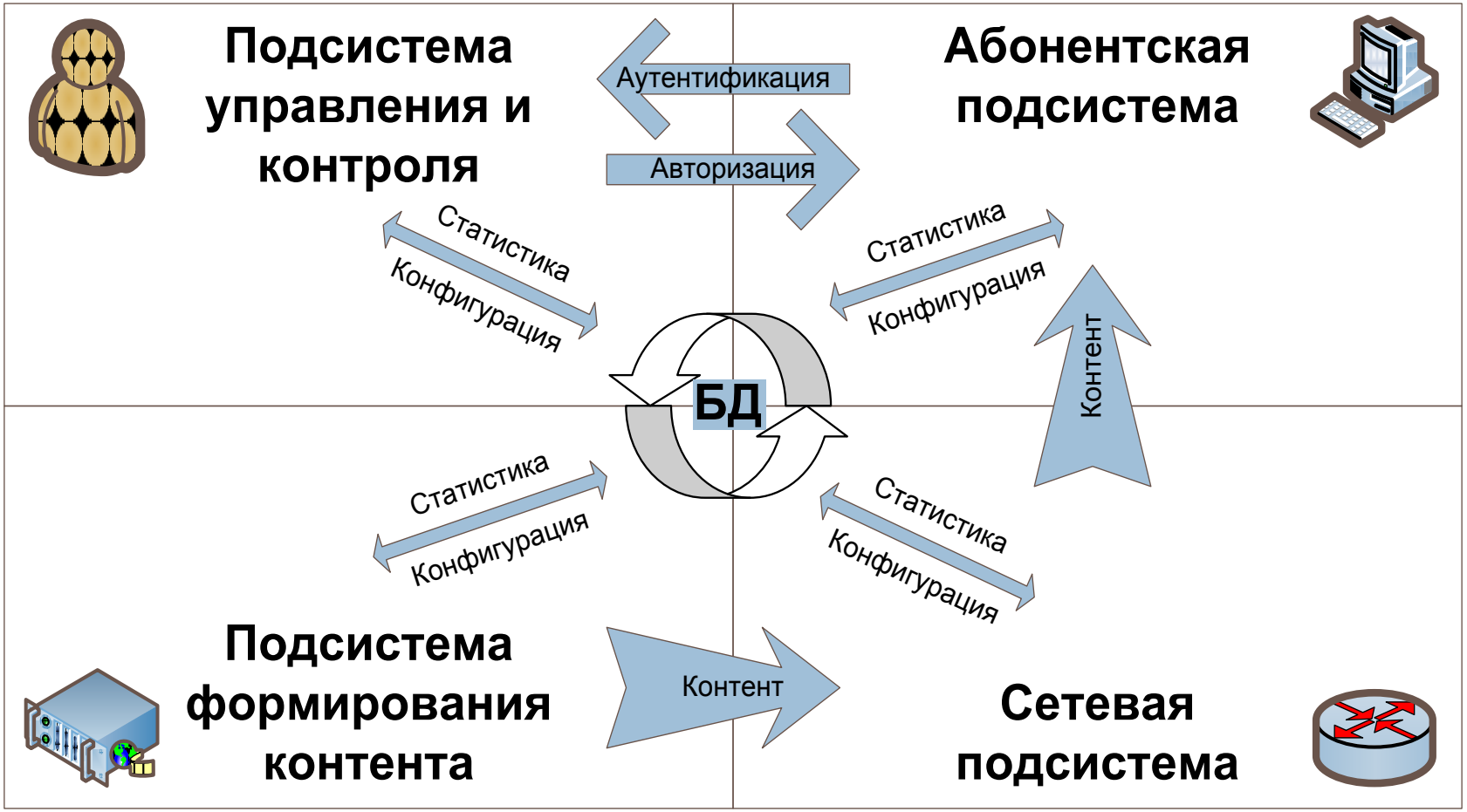
Цель работы:

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.

Структура системы мультимедийного вещания



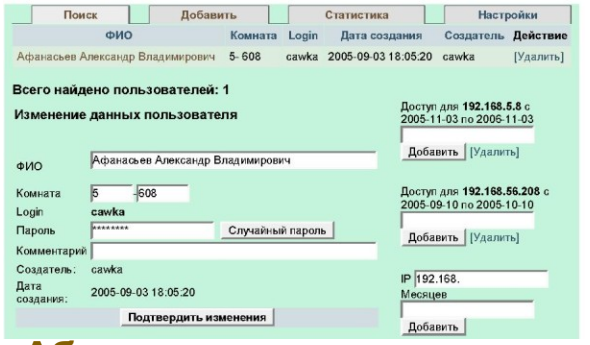
Подсистема контроля и управления

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 необходимый уровень качества работы путем сбора статистической информации на каждом этапе формирования, передачи и получения данных.

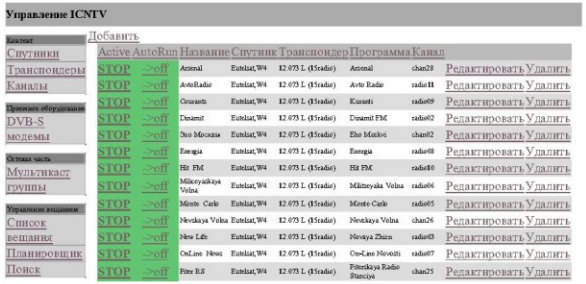
Проблемы:

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



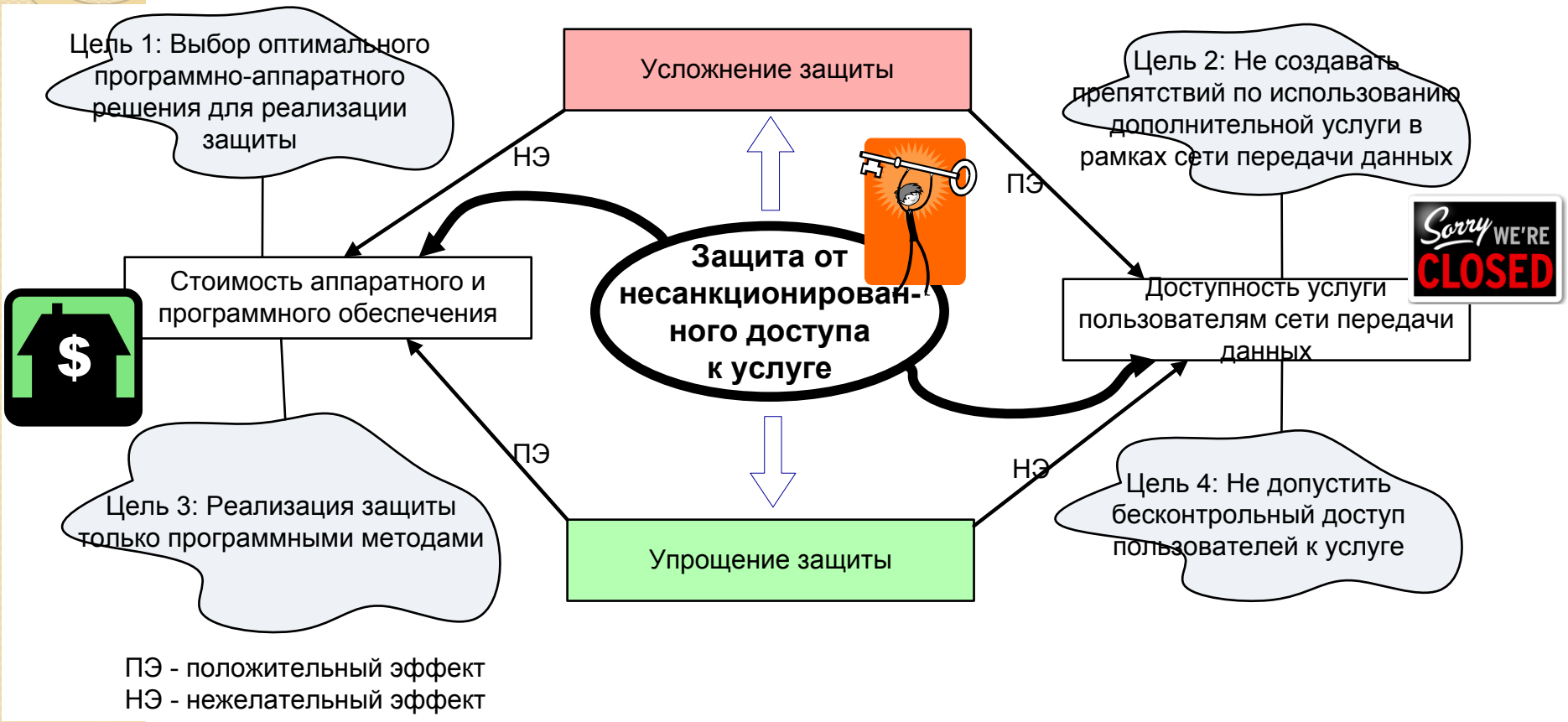
Абонентское управление

Доступ к статистике



Управление вещанием

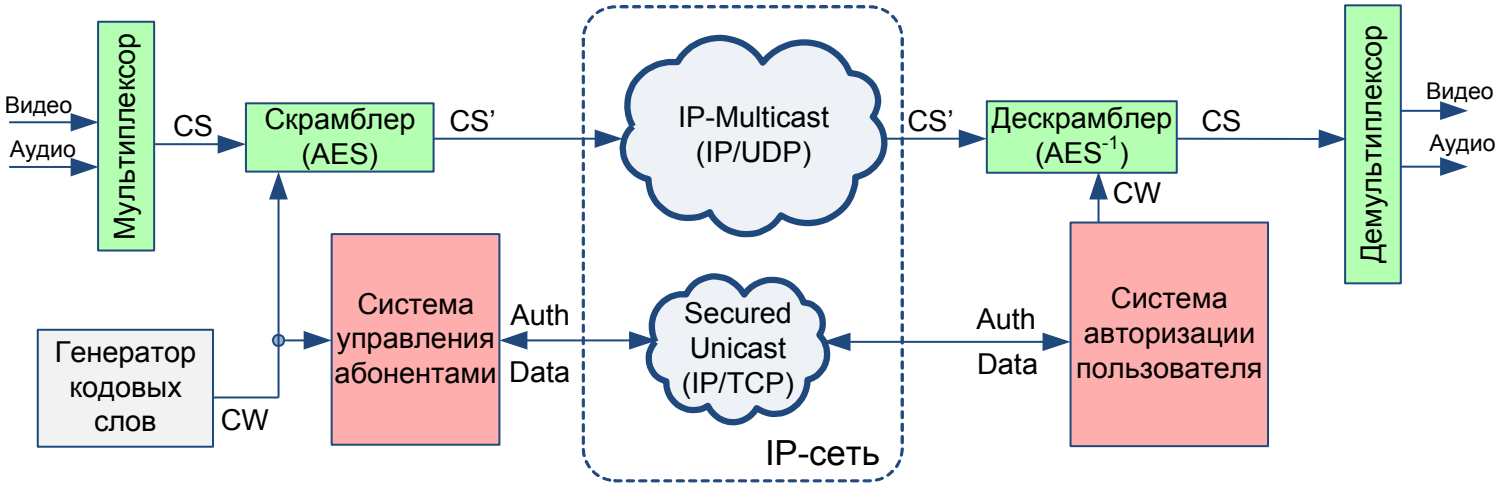
Противоречие: защита от несанкционированного доступа



Разрешение – переход к гибридной модели защиты от НД

DVB-CSA

Гибридная модель



Симметричное шифрование AES

	Длина ключа *(Nk 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

x \ 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	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

ShiftRows – циклический сдвиг

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

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

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

AddRoundKey – наложение итерационного ключа

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

Подсистема формирования контента

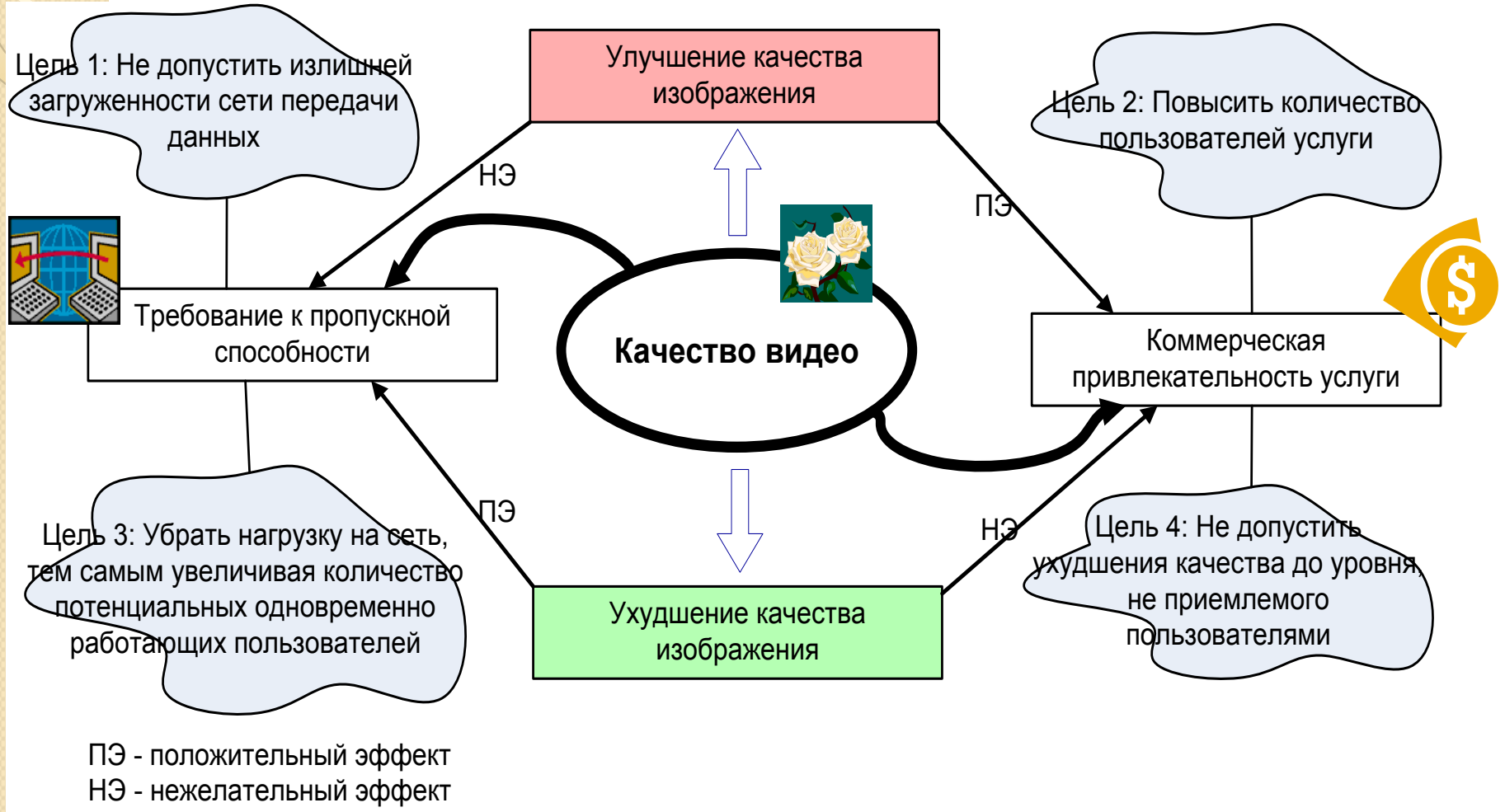
Цель подсистемы:
получение и преобразование получаемого контента из исходной (цифровой или аналоговой) формы в эфективный формат вещания – H.264/RTP

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 большем потерям данных => ухудшение качества видео

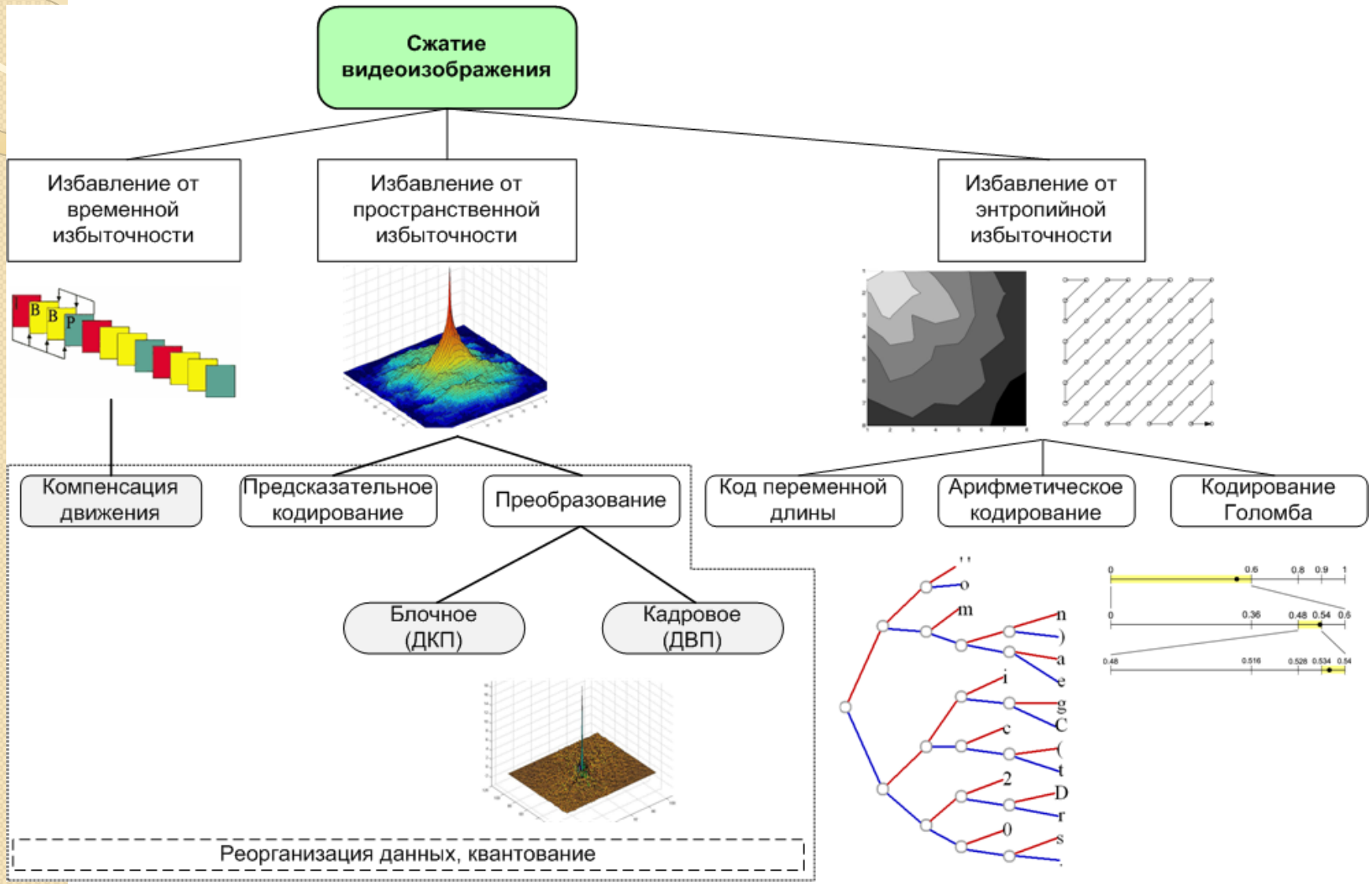
б) Множество различных по типу источников контента:

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

Противоречие: качество вещаемого контента

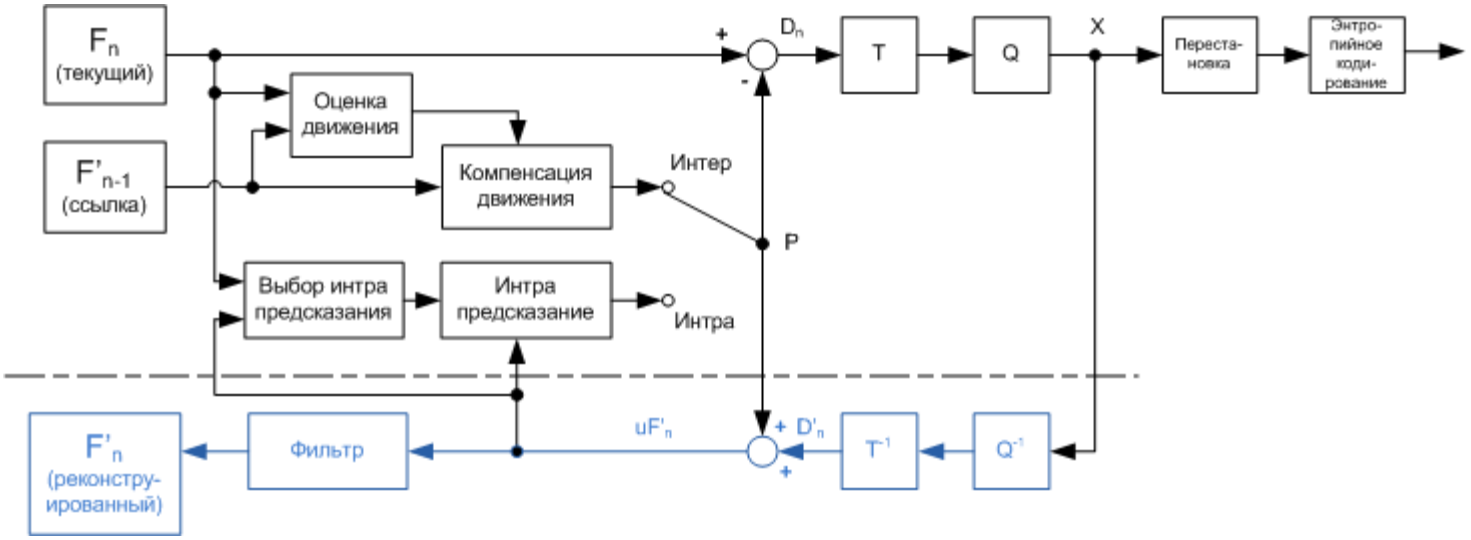


Разрешение (а) – повышение эффективности сжатия

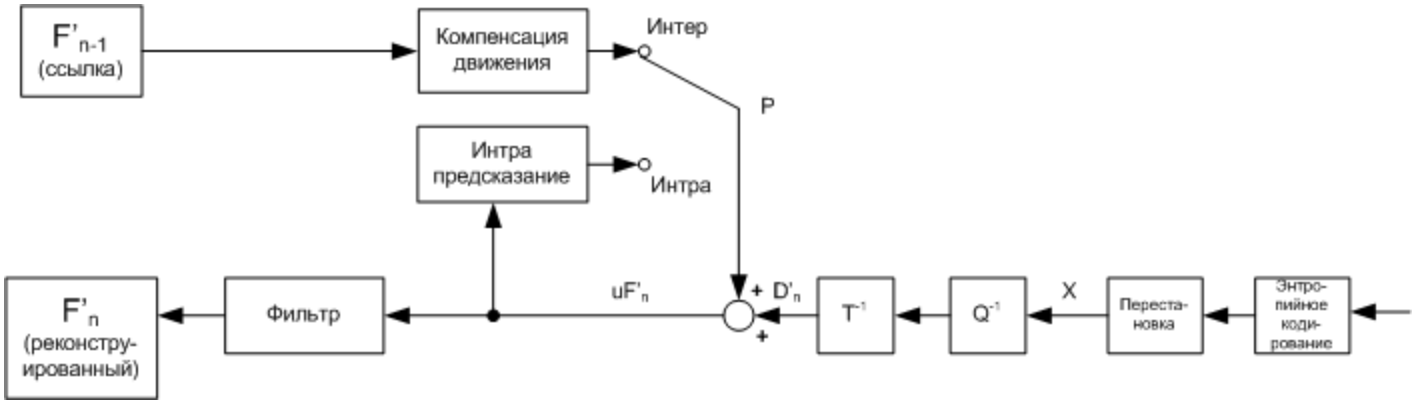


Гибридная модель кодека H.264

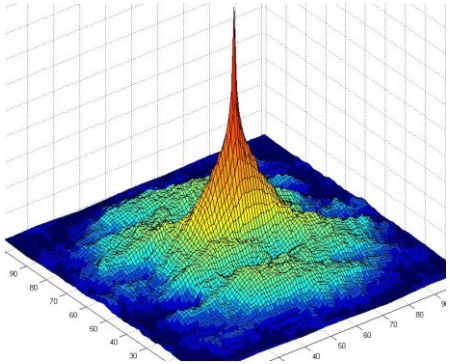
КОДЕР:



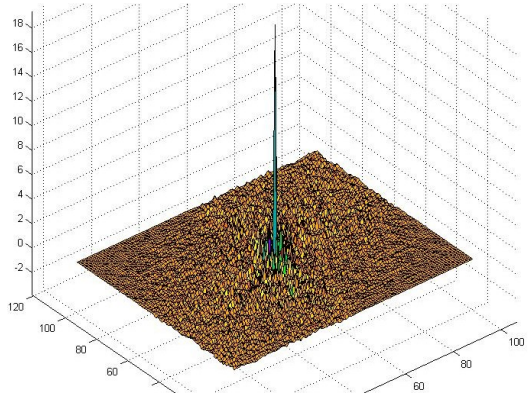
ДЕКОДЕР:



ДКП и H.264 преобразование



ДКП

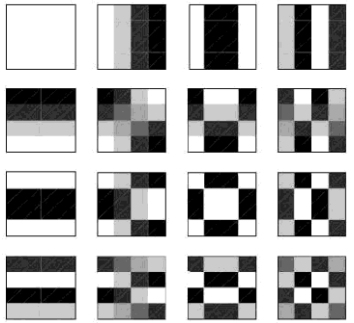


ДКП:

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

ИДКП:

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



H.264 преобразование:

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

Инверсное H.264 преобразование:

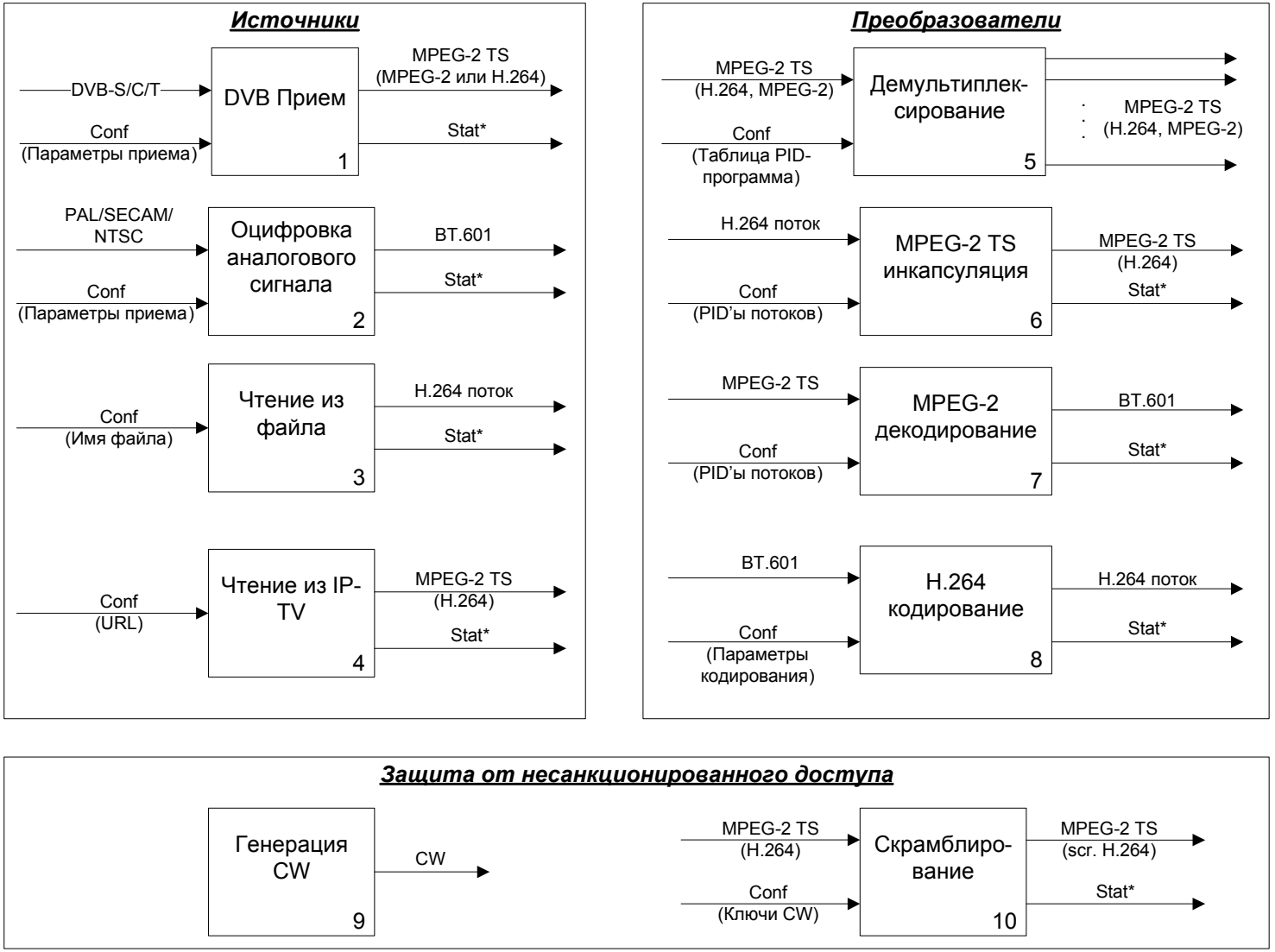
$$\mathbf{X} = C_i^T (\mathbf{Y} \otimes \mathbf{E_i}) C_i = \begin{bmatrix} 1 & 1 & 1 & \frac{1}{2} \\ 1 & \frac{1}{2} & -1 & -1 \\ 1 & -\frac{1}{2} & -1 & 1 \\ 1 & -1 & 1 & -\frac{1}{2} \end{bmatrix} \left(\begin{bmatrix} \mathbf{Y} \end{bmatrix} \otimes \begin{bmatrix} a^2 & ab & a^2 & ab \\ ab &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

Разница между ДКП и H.264 преобразованием

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

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

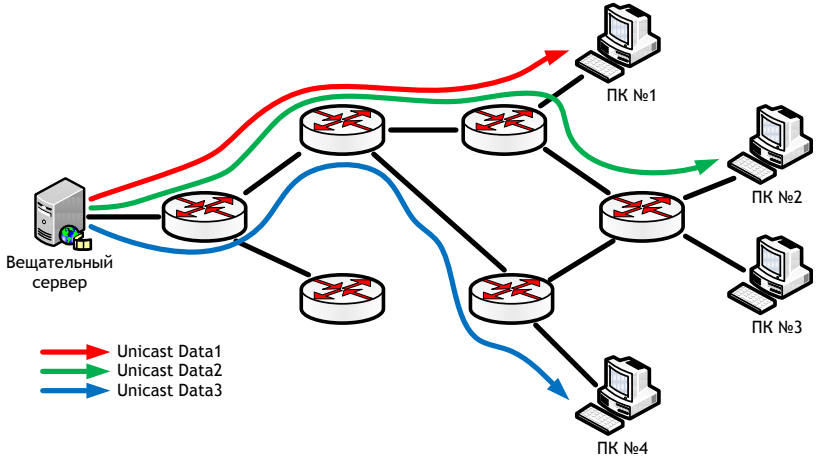
Разрешение (б) – модульное построение подсистемы



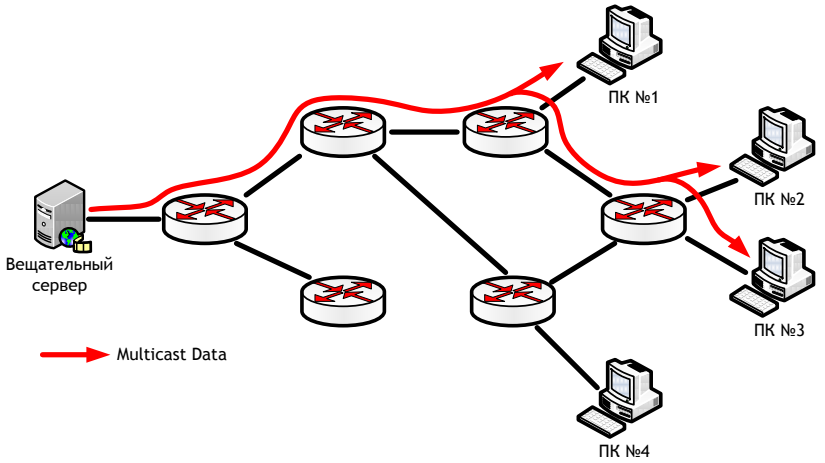
Сетевая подсистема

Цель подсистемы:
данных из подсистемы формирования контента в абонентскую

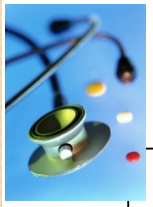
Проблемы:
Использование юникаст (unicast, точка-точка) максимально защищает систему от несанкционированного доступа, но ограничивает либо качество видео, либо количество абонентов



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



Противоречие: количество абонентов



Цель 1: Не допустить экстенсивного роста пропускной способности сети

Увеличение абонентов

Цель 2: Повысить количество потенциальных и реальных пользователей услуги

НЭ

ПЭ

Увеличение требуемой пропускной способности сети

Количество абонентов

Привлечение новых абонентов

ПЭ

НЭ

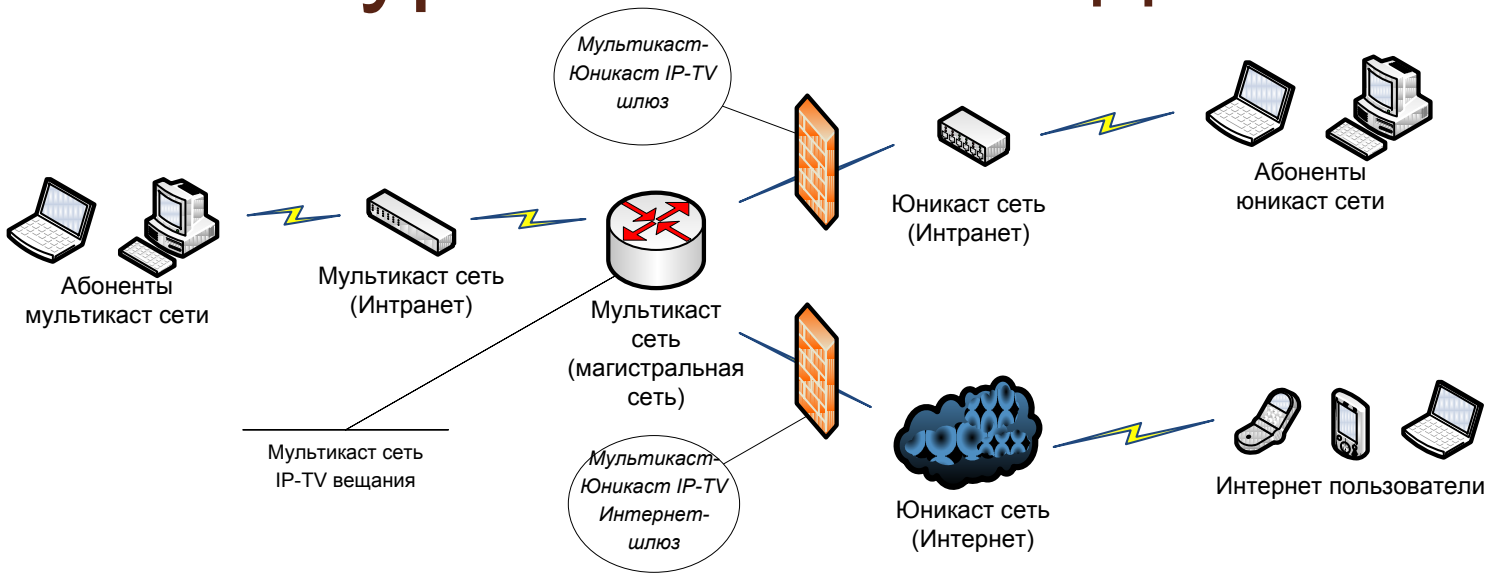
Цель 3: Оптимизация информационной загруженности сети передачи данных

Уменьшение абонентов

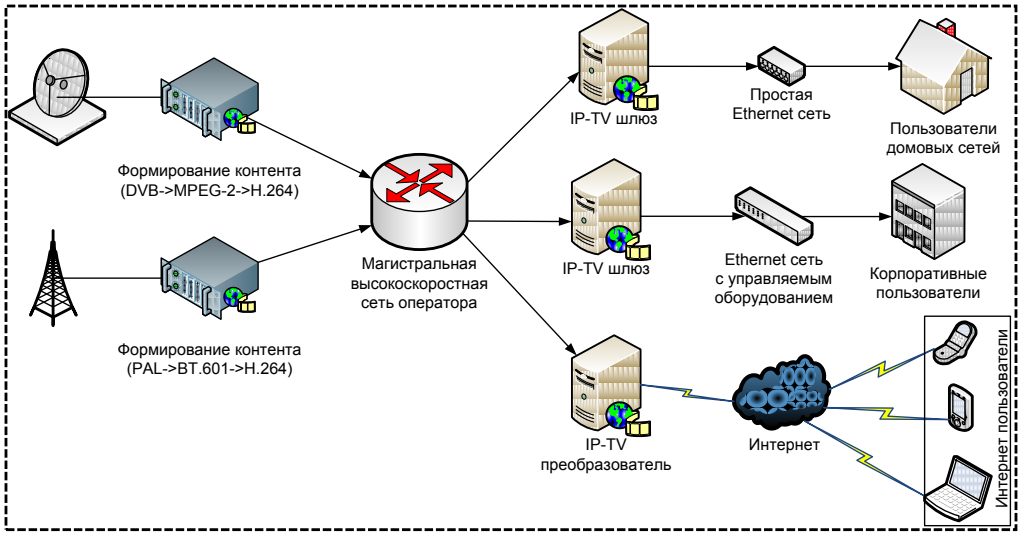
Цель 4: Не создавать неудобства пользователям услуги

ПЭ - положительный эффект
НЭ - нежелательный эффект

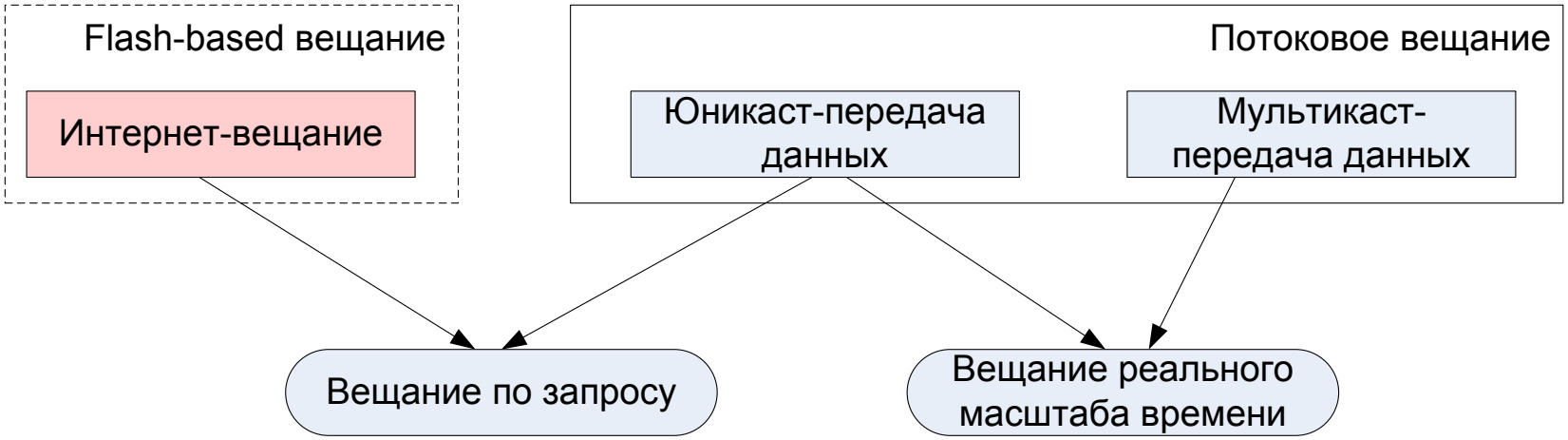
Разрешение – гибридная архитектура сетевой подсистемы



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



Абонентская подсистема

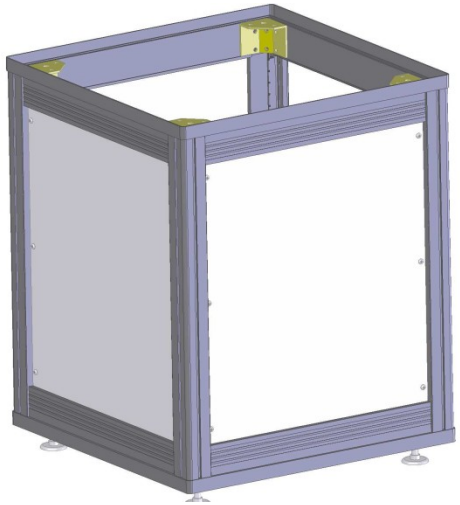


Цель подсистемы:
реализация удобного и понятного (эргономичного) интерфейса пользователя доступа к вещанию

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

Разработка НК сервера вещания

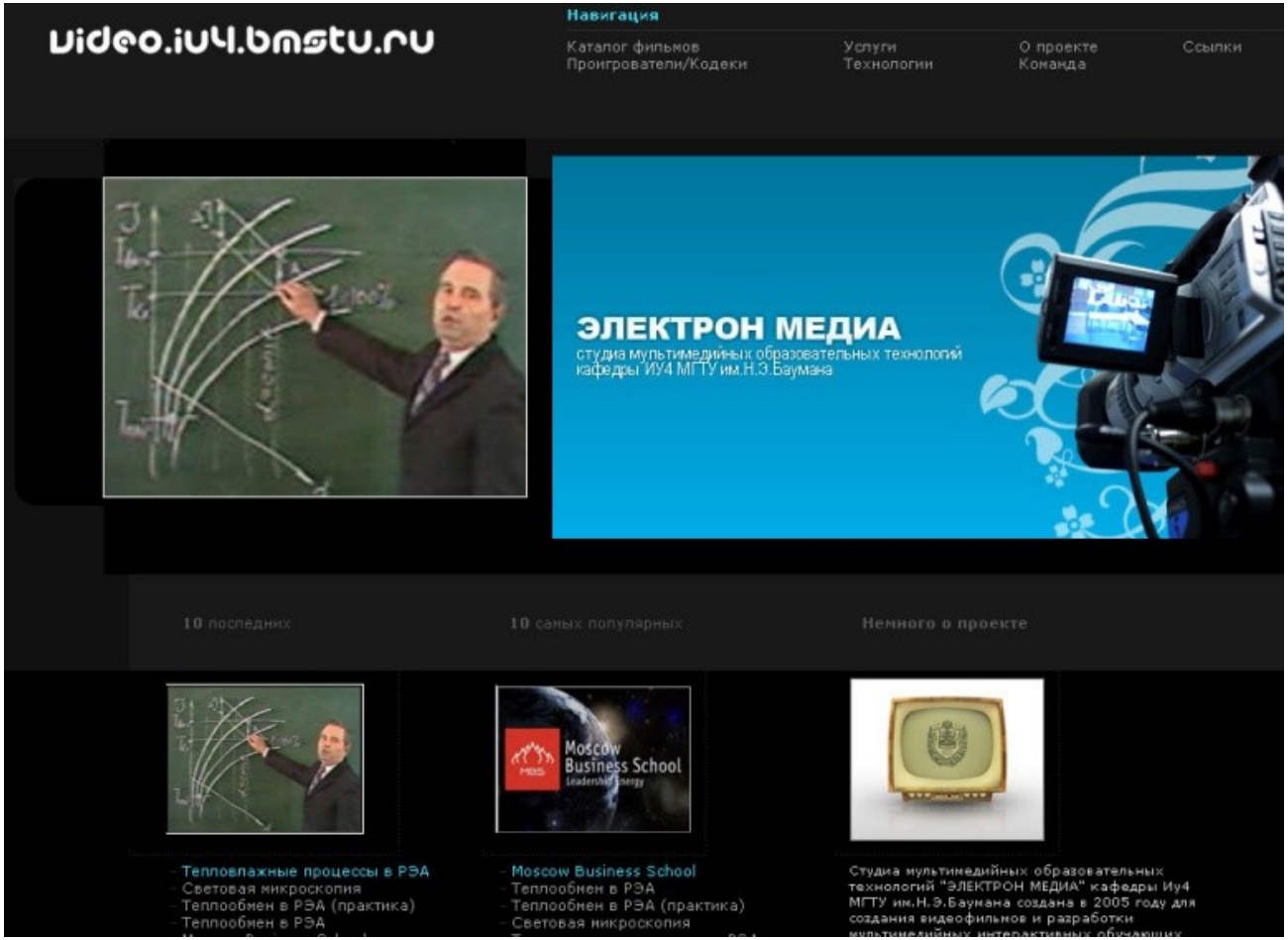


SolidWorks модель тумбы – 14U конструкции сервера вещания

НК сервера вещания

Опытный образец сервера вещания

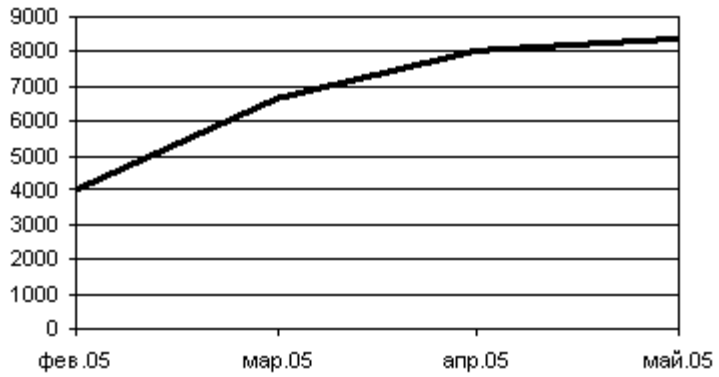
Демонстрация доступа к системе телеобучения «Электрон Медиа»



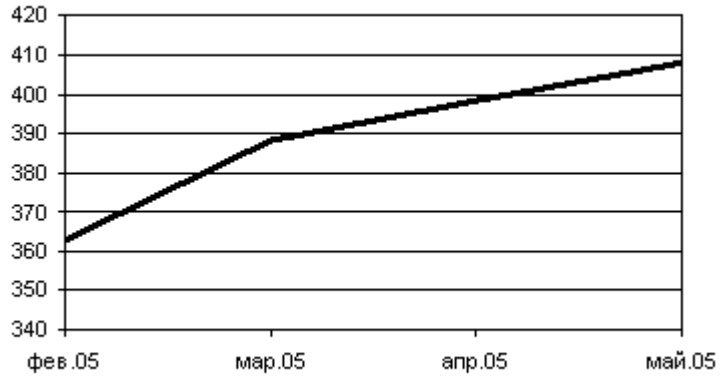
Экспериментальное исследование

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

Исследованы принципы построения мультимедийного вещания: определены возможные источники мультимедийного контента

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 несущей конструкции

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 предоставляения 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 техникик «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 научной-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

Спасибо за внимание

Афанасьев А.В. alex@icn.bmstu.ru

МГТУ им.Н.Э.Баумана, кафедра ИУ4 "Проектирование и технология производства ЭС"