

NTU-RG-1421G-Wac

NTU-RG-1431G-Wac

Руководство по эксплуатации, версия 1.1 (21.12.2016)

Абонентские оптические терминалы

IP-адрес: 192.168.1.1

имя пользователя: user

пароль: user

<http://eltex.nsk.ru/support/downloads>

Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 1.1	3.28.1	21.12.2016	Вторая публикация
Версия 1.0	3.28.0	29.08.2016	Первая публикация

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ



Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.



Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ	5
2 ОПИСАНИЕ ИЗДЕЛИЯ	6
2.1 Назначение	6
2.2 Варианты исполнения	7
2.3 Характеристика устройства	7
2.4 Основные технические параметры	9
2.5 Конструктивное исполнение	11
2.5.1 NTU-RG-1421G-Wac/NTU-RG-1431G-Wac	11
2.5.2 NTU-RG-1421G-Wac, NTU-RG-1431G-Wac	13
2.5.3 Индикация интерфейсов LAN	14
2.6 Перезагрузка/сброс к заводским настройкам	15
2.7 Комплект поставки	15
3 АРХИТЕКТУРА УСТРОЙСТВ	16
3.1 Архитектура NTU-RG	16
4 НАСТРОЙКА NTU-RG-1421G-W, NTU-RG-1431G-W ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ	18
4.1 Меню «Информация об устройстве»	19
4.1.1 Подменю Общее.	19
4.1.2 Подменю WAN. Информация о состоянии сервисов	19
4.1.2.1 Подменю Подробно. Подробная информация	19
4.1.3 Подменю LAN. Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса	20
4.1.4 Подменю Статистика. Информация о прохождении трафика на портах устройства	20
4.1.5 Подменю Маршрутизация. Просмотр таблицы маршрутизации	21
4.1.6 Подменю ARP. Просмотр кэша протокола ARP	21
4.1.7 Подменю DHCP. Активные аренды DHCP	22
4.1.8 Подменю Беспроводные станции. Подключенные беспроводные устройства	22
4.1.9 Подменю Беспроводной монитор Обнаруженные беспроводные сети	23
4.1.10 Подменю Телефония. Мониторинг состояния телефонного порта	23
4.2 Меню «Расширенные настройки». Расширенные настройки конфигурации	24
4.2.1 Подменю LAN. Настройка основных параметров	24
4.2.2 Подменю «NAT». Настройки NAT	25
4.2.2.1 Подменю Виртуальные серверы. Настройки виртуальных серверов	25
4.2.2.2 Подменю Перенаправление портов. Настройки запуска портов	26
4.2.2.3 Подменю DMZ-хост. Настройки демилитаризованной зоны	27
4.2.3 Подменю «Безопасность». Настройки безопасности	27
4.2.3.1 Подменю IP фильтрация. Настройки фильтрации адресов	27
4.2.3.2 Подменю MAC фильтрация. Настройки фильтрации по MAC-адресам	29
4.2.4 Подменю «Родительский контроль» – настройки ограничения	30
4.2.4.1 Подменю Ограничение по времени. Настройки ограничения продолжительности сеансов ...	30
4.2.4.2 Подменю Фильтр Url. Настройки ограничения доступа в интернет	31
4.2.5 Меню «Динамическая DNS». Настройки динамической системы доменных имен	32
4.2.6 Меню Принт-сервер. Настройки сервера печати	34
4.2.7 Меню DLNA. Настройки сервера DLNA	34
4.2.8 Меню «UPnP». Автоматическая настройка сетевых устройств	35
4.3 Меню «Беспроводная связь». Настройка беспроводной сети	36
4.3.1 Подменю Основные настройки. Общая информация	36
4.3.2 Подменю Безопасность. Настройка параметров безопасности	37
4.3.3 Подменю MAC-Фильтрация. Настройки фильтрации MAC-адресов	40
4.3.4 Подменю Беспроводной мост. Настройки беспроводного соединения в режиме моста	40
4.3.5 Подменю Расширенные настройки	41
4.4 Меню «Хранилища». Службы файловых хранилищ	44
4.4.1 Подменю Информация по устройству хранения. Информация о подключенных USB-устройствах	44

4.4.2	Подменю Пользовательские аккаунты. Настройка пользователей Samba.....	44
4.5	Меню «Управление». Управление устройством	45
4.5.1	Подменю Настройки	45
4.5.1.1	Подменю Резервное копирование.....	45
4.5.1.2	Подменю Заводские настройки. Возврат к настройкам по умолчанию	45
4.5.2	Подменю Дата и время. Настройки системного времени.....	45
4.5.3	Подменю Ping. Проверка доступности сетевых устройств.....	46
4.5.4	Подменю Пароли. Настройка контроля доступа (установление паролей).....	46
4.5.5	Подменю Системный журнал. Просмотр и настройка системного журнала	47
4.5.5.1	Подменю Конфигурация. Настройка системного журнала	47
4.5.5.2	Подменю Просмотр. Просмотр системного журнала.....	48
4.5.6	Подменю Обновить ПО. Обновление ПО	48
4.5.7	Подменю Перезагрузка. Перезагрузка устройства	48
ПРИЛОЖЕНИЕ А. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ		49
СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ NTU-RG.....		50

1 ВВЕДЕНИЕ

Сеть GPON относится к одной из разновидностей пассивных оптических сетей PON. Это одно из самых современных и эффективных решений задач «последней мили», позволяющее существенно экономить на кабельной инфраструктуре и обеспечивающее скорость передачи информации до 2.5 Gbps в направлении downlink и 1.25 Gbps в направлении uplink. Использование в сетях доступа решений на базе технологии GPON дает возможность предоставлять конечному пользователю доступ к новым услугам на базе протокола IP совместно с традиционными сервисами.

Основным преимуществом GPON является использование одного станционного терминала (OLT) для нескольких абонентских устройств (ONT). OLT является конвертором интерфейсов Gigabit Ethernet и GPON, служащим для связи сети PON с сетями передачи данных более высокого уровня. ONT предназначено для подключения к услугам широкополосного доступа оконечного оборудования клиентов. Может применяться в жилых комплексах и бизнес-центрах.

Линейка оборудования ONT NTU производства «ЭЛТЕКС» представлена терминалами:

- NTU-RG-1421G-Wac, NTU-RG-1431G-Wac, которые рассчитаны на четыре UNI интерфейса 10/100/1000Base-T и поддержку интерфейсов FXS, Wi-Fi, USB.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения оптических терминалов серии *NTU-RG*.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства *NTU-RG GPON ONT* (Gigabit Ethernet Passive Optical Network) – высокопроизводительные абонентские терминалы, предназначенные для связи с вышестоящим оборудованием пассивных оптических сетей и предоставления услуг широкополосного доступа конечному пользователю. Связь с сетями GPON реализуется посредством PON интерфейса, для подключения оконечного оборудования клиентов служат интерфейсы Ethernet.

Преимуществом технологии GPON является оптимальное использование полосы пропускания. Эта технология является следующим шагом для обеспечения новых высокоскоростных интернет-приложений дома и в офисе. Разработанные для развертывания сети внутри дома или здания, данные устройства ONT обеспечивают надежное соединение с высокой пропускной способностью на дальние расстояния для пользователей, живущих и работающих в удаленных многоквартирных зданиях и бизнес-центрах.

Благодаря встроенному маршрутизатору, устройства обеспечивают возможность подключения оборудования локальной сети к сети широкополосного доступа. Терминалы обеспечивают защиту межсетевым экраном для компьютеров в сети от атак DoS и вирусных атак, осуществляют фильтрацию пакетов для осуществления управления доступом на основе портов и MAC/IP-адресов источника/назначения. Пользователи могут настроить домашний или офисный Web-сайт, добавив один из LAN-портов в зону DMZ. Функция Родительский контроль обеспечивает фильтрацию Web-сайтов с нежелательным содержанием, блокировку доменов и позволяет задавать расписание использования Интернета. Виртуальная частная сеть (VPN) предоставляет мобильным пользователям и филиалам защищенный канал связи для подключения к корпоративной сети.

Порт FXS позволяет пользоваться услугами IP-телефонии, предоставляя множество полезных функций, таких как отображение идентификатора звонящего, трехстороннюю конференцию, телефонную книгу, ускоренный набор. Все это обеспечивает удобство пользователя при наборе номера и приеме телефонных звонков.

Порты USB могут использоваться для подключения USB-устройств (USB-флеш-накопитель, внешний HDD).

Абонентские маршрутизаторы *NTU-RG-1421G-Wac*, *NTU-RG-1431G-Wac* позволяют подключать клиентов Wi-Fi по стандарту IEEE 802.11a/b/g/n/ac. Поддержка стандарта 802.11ac обеспечивает скорость передачи данных до 1,3 Гбит/с и позволяет доставлять современные высокоскоростные сервисы клиентскому оборудованию по беспроводной сети. Два встроенных контроллера Wi-Fi сети позволяют обеспечить работу устройства одновременно в двух частотных диапазонах – 2,4 ГГц и 5 ГГц.

2.2 Варианты исполнения

Устройства серий *NTU-RG* отличаются набором интерфейсов и функциональными возможностями, Таблица 1.

Таблица 1 – Варианты исполнения

Наименование модели	WAN	LAN	FXS	Wi-Fi 802.11 b/g/n	Wi-Fi 802.11 b/g/n/ac	USB
<i>NTU-RG-1421G-Wac</i>	1xGPON	4x1Gigabit	1	+	802.11n, 2*2 -300Mbps –2,4GHz 802.11ac, 3*3 -1.3Gbps – 5 GHz+	2
<i>NTU-RG-1431G-Wac</i>	1xGPON	4x1Gigabit	1	+	802.11n, 3*3 -450Mbps - 2,4GHz 802.11ac, 3*3 -1.3Gbps – 5 GHz	2

2.3 Характеристика устройства

Устройство имеет следующие интерфейсы:

- Порт RJ-11 для подключения аналоговых телефонных аппаратов:
 - Для NTU-RG: 1 порт RJ-11;
- 1 порт PON SC/APC для подключения к сети оператора;
- Порты Ethernet RJ-45 LAN для подключения сетевых устройств:
 - Для NTU-RG: 4 порта RJ-45 10/100/1000Base-T;
- Приемопередатчик Wi-Fi 802.11a/b/g/n/ac;
- 2 порта USB2.0 - для подключения внешних накопителей USB или HDD.

Питание терминала осуществляется через внешний адаптер от сети 220 В/12В.

Устройство поддерживает следующие функции:

- сетевые функции:
 - работа в режиме «моста» или «маршрутизатора»;
 - поддержка PPPoE (PAP, CHAP, MSCHAP авторизация);
 - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
 - поддержка UPnP;
 - поддержка IPSec;
 - поддержка NAT;
 - поддержка Firewall;
 - поддержка NTP;
 - поддержка механизмов качества обслуживания QoS;
 - поддержка IGMP-snooping;
 - поддержка IGMP-proxy;
 - поддержка функции Parental Control;
 - поддержка функции Storage service;
 - поддержка UPNP, SMB, FTP, DLNA, Print Server;
 - VLAN в соответствии с IEEE 802.1Q.
- Wi-Fi:
 - поддержка стандартов 802.11a/b/g/n/ac;
 - одновременная работа в двух диапазонах: 2.4ГГц и 5ГГц;
- IP-телефония:
 - поддержка протокола SIP;
 - аудиокодеки: G.729 (A), G.711(A/U), G.723.1;

- ToS для пакетов RTP;
- ToS для пакетов SIP;
- эхо компенсация (рекомендации G.164, G.165);
- детектор тишины (VAD);
- генератор комфортного шума;
- обнаружение и генерирование сигналов DTMF;
- передача DTMF (INBAND, RFC2833, SIP INFO);
- передача факса: upspeed/pass-through. G.711, T.38;
- функции ДВО:
 - удержание вызова – Call Hold;
 - передача вызова – Call Transfer;
 - уведомление о поступлении нового вызова – Call Waiting;
 - безусловная переадресация - Forward unconditionally;
 - переадресация по неответу - Forward on "no answer";
 - переадресация по занятости – Forward on "busy";
 - определитель номера Caller ID по ETSI FSK;
 - запрет выдачи Caller ID (анонимный звонок) - Anonymous calling;
 - теплая линия - Warmline;
 - гибкий план нумерации;
 - индикация о наличии сообщений на голосовой почте - MWI;
 - блокировка анонимных звонков - Anonymous call blocking;
 - запрет на исходящие вызовы - Call Barring;
 - "не беспокоить" – DND.
- обновление ПО через Web-интерфейс, TR-069, OMCI;
- удаленный мониторинг, конфигурирование и настройка:
 - TR-069;
 - Web-интерфейс;
 - OMCI;
 - Telnet.

На рисунке 1 приведена схема применения оборудования NTU.

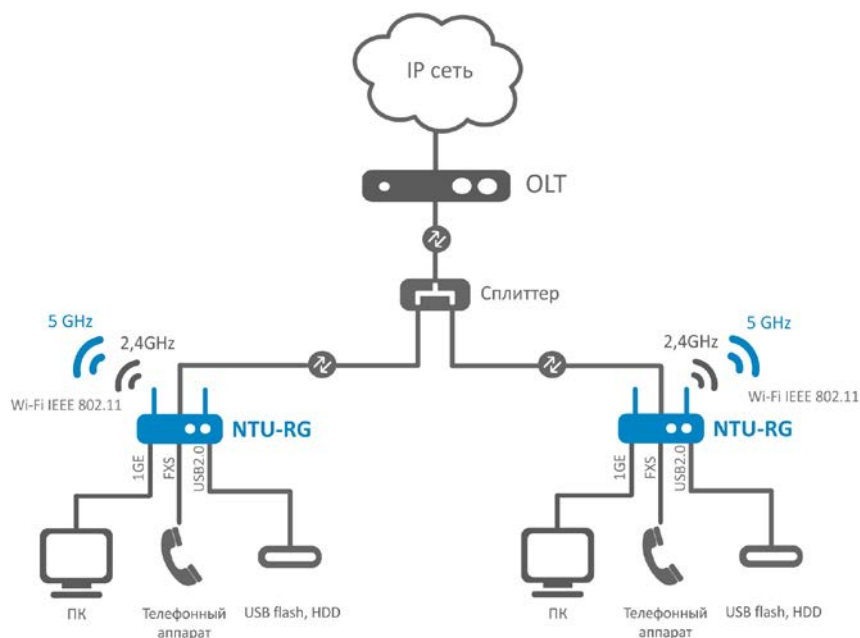


Рисунок 1 – Схема применения NTU-RG-1421G-Wac, NTU-RG-1431G-Wac

2.4 Основные технические параметры

Основные технические параметры терминалов приведены в таблице 2:

Таблица 2 – Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP
--------------------------	-----

Аудиокодеки

Кодеки	G.729, annex A G.711(A/μ) G.723.1 (5,3 Kbps) Передача факса: G.711, T.38
--------	---

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	4
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	Автоопределение, 10/100/1000 Мбит/с, дуплекс/ полудуплекс
Поддержка стандартов	IEEE 802.3i 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3ab 1000Base-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation

Параметры интерфейса PON

Количество интерфейсов PON	1
Поддержка стандартов	ITU-T G.984.x Gigabit-capable passive optical networks (GPON) ITU-T G.988 ONU management and control interface (OMCI) specification IEEE 802.1Q Tagged VLAN IEEE 802.1p Priority Queues IEEE 802.1D Spanning Tree Protocol
Тип разъема	SC/APC соответствует ITU-T G.984.2
Среда передачи	оптоволоконный кабель SMF - 9/125, G.652
Коэффициент разветвления	до 1:64
Максимальная дальность действия	20 км
Передатчик:	1310Нм
Скорость соединения upstream	1244Mb/s
Мощность передатчика	+0,5 до +5 dBm
Ширина спектра опт. излучения (RMS)	1 nm
Приемник	1490Нм
Скорость соединения downstream	2488Mb/s
Чувствительность приемника	от -8 до -28 dBm

Параметры аналоговых абонентских портов

количество портов	1
сопротивление шлейфа	до 2 кОм
прием набора	импульсный/частотный (DTMF)
выдача Caller ID	есть

Параметры беспроводного интерфейса Wi-Fi

Модель	NTU-RG-1421G-Wac	NTU-RG-1431G-Wac
Стандарт	802.11a/b/g/n/ac	802.11a/b/g/n/ac
Частотный диапазон	2400 ~ 2483,5 МГц, 5150 ~ 5350 МГц, 5650 ~ 5850 МГц Одновременная работа в двух частотных диапазонах (Simultaneous Dual Band)	2400 ~ 2483,5 МГц, 5150 ~ 5350 МГц, 5650 ~ 5850 МГц Одновременная работа в двух частотных диапазонах (Simultaneous Dual Band)
Модуляция	ССК, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM	ССК, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM
Скорость передачи данных, Мбит/с	– 802.11b/g/n: 1-13 – 802.11a/ac: 36-64, 132-165 – 802.11b: 1; 2; 5,5 и 11 Мбит/с – 802.11g: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с – 802.11n: 300 Мбит/с (канал 20 МГц), 450 Мбит/с (канал 40 МГц) – 802.11ac: 1300 Мбит/с (80 МГц)	– 802.11b/g/n: 1-13 – 802.11a/ac: 36-64, 132-165 – 802.11b: 1; 2; 5,5 и 11 Мбит/с – 802.11g: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с – 802.11n: 300 Мбит/с (канал 20 МГц), 450 Мбит/с (канал 40 МГц) – 802.11ac: 1300 Мбит/с (80 МГц)
Максимальная выходная мощность передатчика	– 802.11b (11 Mbps): 17дБм – 802.11g (54 Mbps): 15дБм – 802.11n (MCS7): 15 дБм – 802.11ac (5 ГГц): 19 дБм	
MAC-протокол	CSMA/CA модель ACK 32 MAC	
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2 802.1x AES & TKIP	
Поддержка операционной системы	Windows XP 32/64, Windows Vista 32/64, Windows 2000, Windows 7 32/64 Linux, VxWorks	
Количество антенн	NTU-RG-1421G-Wac	3
	NTU-RG-1431G-Wac	3
Коэффициентом усиления антенны	5 dBi	
Рабочий диапазон температур	от 0 до +70°C	

Управление

Локальное управление	web-интерфейс
Удаленное управление	Telnet, TR-069, OMCI
Обновление программного обеспечения	OMCI, TR-069, HTTP, TFTP
Ограничение доступа	по паролю

Общие параметры

Питание	адаптер питания 12V DC /220 AC	
Потребляемая мощность	NTU-RG-1421G-Wac	не более 15 Вт
	NTU-RG-1431G-Wac	не более 15 Вт
Рабочий диапазон температур	от +5 до +40°C	
Относительная влажность	до 80%	
Габариты	187x120x32 мм	
Масса	0,3 кг	

2.5 Конструктивное исполнение

2.5.1 NTU-RG-1421G-Wac/NTU-RG-1431G-Wac

Абонентский терминал выполнен в виде настольного изделия в пластиковом корпусе.

Внешний вид задней панели устройства приведен на рисунке 2.

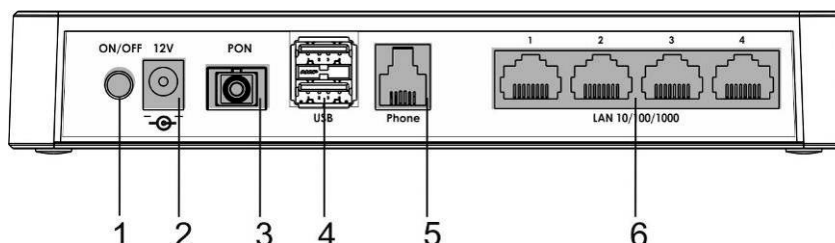


Рисунок 2 – Внешний вид задней панели NTU-RG-1421G-Wac, NTU-RG-1431G-Wac

На задней панели устройства расположены следующие разъемы и органы управления, Таблица 3.

Таблица 3 – Описание разъемов, и органов управления задней панели

№	Элемент задней панели	Описание
1	On/Off	кнопка питания
2	12V	разъем подключения адаптера питания
3	PON	разъем SC (розетка) <i>PON</i> оптического интерфейса GPON
4	USB	2 разъема для подключения внешних накопителей и других USB-устройств
5	Phone	1 разъем RJ-11 для подключения аналогового телефонного аппарата
6	LAN 10/100/1000 1..4	4 разъема RJ-45 для подключения сетевых устройств

Внешний вид боковой и верхней панелей устройства NTU-RG приведен на рисунке 3.

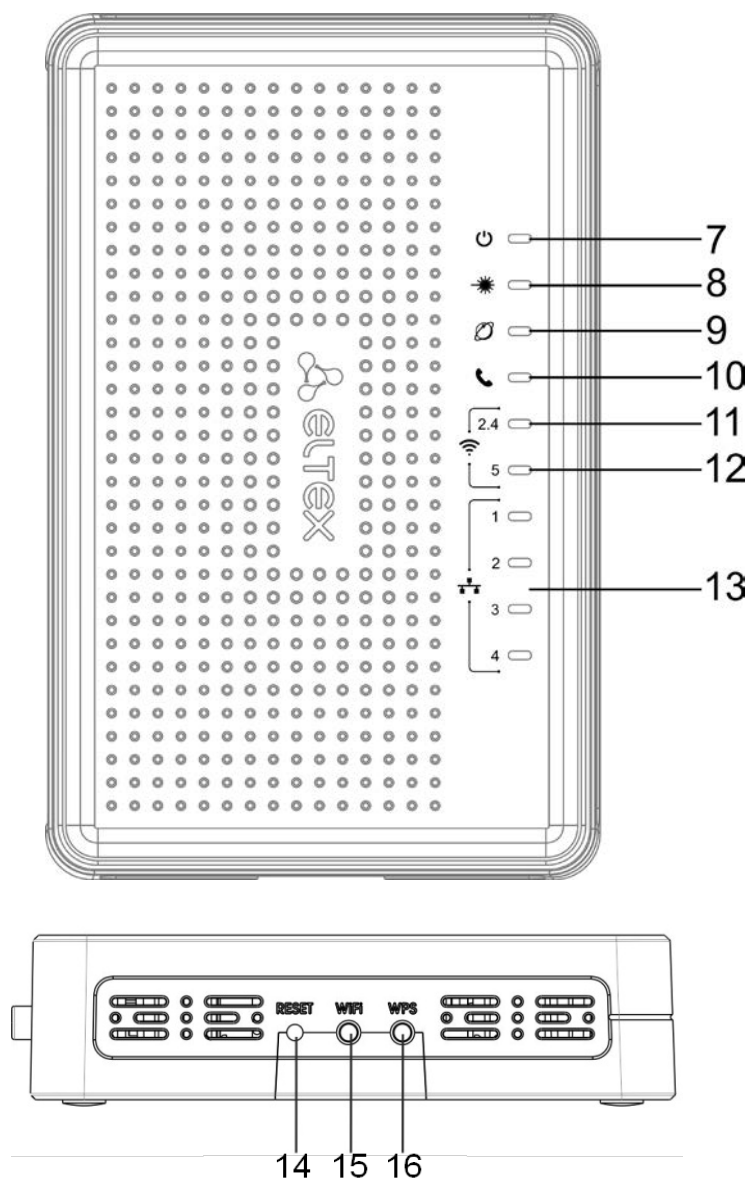


Рисунок 3 – Внешний вид боковой и верхней панели NTU-RG

На верхней панели устройства расположены следующие индикаторы, Таблица 4.

Таблица 4 –Описание индикаторов верхней панели

№	Элемент верхней панели	Описание
7		индикатор питания и статуса работы
8		индикатор работы оптического интерфейса
9		индикатор состояние сервиса «Интернет»
10		индикатор активности порта FXS
11		индикатор активности Wi-Fi в диапазоне 2.4ГГц
12		индикатор активности Wi-Fi в диапазоне 5ГГц
13		индикаторы работы Ethernet-портов

На боковой панели устройства расположены следующие кнопки, Таблица 5.

Таблица 5 – Описание кнопок боковой панели

№	Элемент боковой панели	Описание
14	Reset	функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам
15	Wi-Fi	кнопка включения/выключения Wi-Fi
16	WPS	кнопка для автоматического защищенного подключения к сети Wi-Fi на устройстве

2.5.2 NTU-RG-1421G-Wac, NTU-RG-1431G-Wac

Текущее состояние устройства отображается при помощи индикаторов, расположенных на передней панели.

Перечень состояний индикаторов приведен в таблице 6.

Таблица 6 – Световая индикация устройства

Индикатор	Состояние индикатора	Состояние устройства
 1..4	зеленый	установлено соединение 10/100 Мбит/с
	оранжевый	установлено соединение 1000 Мбит/с
	мигает	процесс пакетной передачи данных
	горит	телефонная трубка снята
	мигает	порт не зарегистрирован или не пройдена авторизация на SIP-сервере
	медленно мигает	прием сигнала вызова
 2.4/5	зеленый	сеть Wi-Fi активна
	мигает	процесс передачи данных по Wi-Fi
	не горит	сеть Wi-Fi не активна
	не горит	интерфейс с признаком Интернет не сконфигурирован
	зеленый	интерфейс с признаком Интернет сконфигурирован, на нем получен IP-адрес
	оранжевый	интерфейс с признаком Интернет сконфигурирован, но IP-адрес на нем не получен
	мигает зеленым	процесс обновления ПО на устройстве
	не горит	процесс загрузки устройства
	зеленый	установлено соединение между станционным оптическим терминалом и устройством
	мигает зеленым	установлено соединение между станционным оптическим терминалом и устройством, устройство не активировано
	мигает красным	нет сигнала от станционного оптического терминала
	не горит	устройство отключено от сети питания или неисправно
	красный	возникли проблемы при загрузке устройства
	зеленый	процесс загрузки завершен, на устройстве установлена конфигурация, отличная от конфигурации по умолчанию

	оранжевый	процесс загрузки завершен, на устройстве установлена конфигурация по умолчанию
--	-----------	--

2.5.3 Индикация интерфейсов LAN

Режимы работы, отображаемые индикаторами на портах LAN на задней панели устройства, приведены в таблице 7.

Таблица 7 – Световая индикация интерфейсов LAN

Режимы работы	Желтый индикатор	Зеленый индикатор
Порт работает в режиме 1000Base-T, нет передачи данных	горит постоянно	горит постоянно
Порт работает в режиме 1000Base-T, есть передача данных	горит постоянно	мигает
Порт работает в режиме 10/100Base-TX, нет передачи данных	не горит	горит постоянно
Порт работает в режиме 10/100Base-TX, есть передача данных	не горит	мигает

2.6 Перезагрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку «Reset» на боковой панели изделия. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку «Reset» 7-10 секунд, пока индикатор POWER не загорится красным светом. При заводских установках IP адрес: LAN - 192.168.1.1, маска подсети – 255.255.255.0. Доступ возможен с портов LAN 1 и LAN 2.

2.7 Комплект поставки

В базовый комплект поставки устройства *NTU-RG* входят:

- абонентский оптический терминал *NTU-RG*;
- адаптер питания 220/12;
- руководство по эксплуатации.

3 АРХИТЕКТУРА УСТРОЙСТВ

3.1 Архитектура NTU-RG

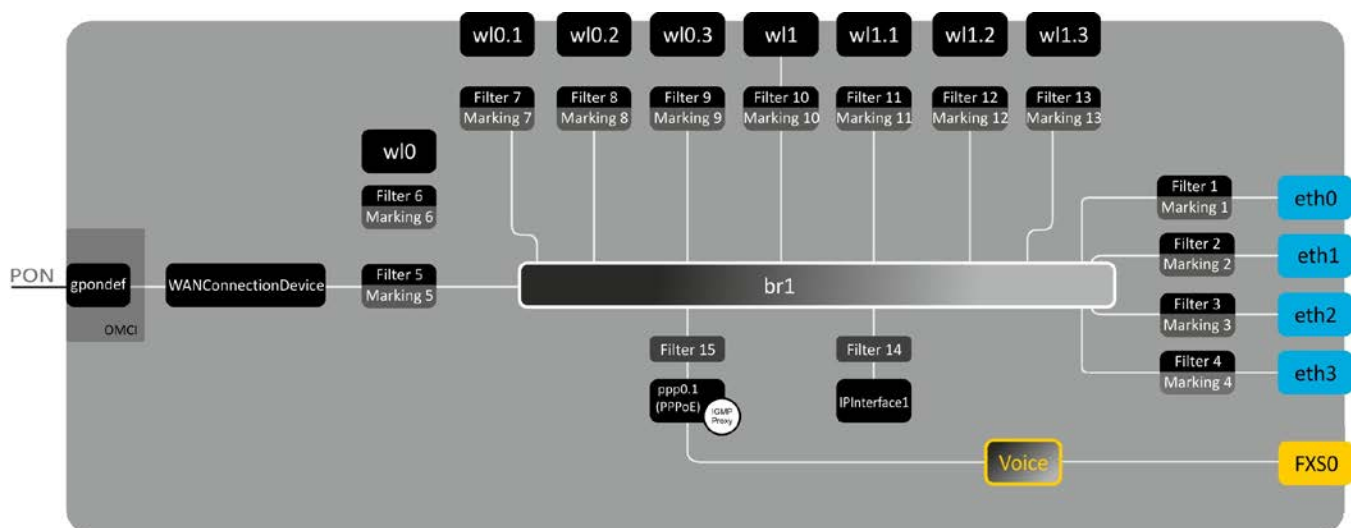


Рисунок 4 – Логическая архитектура устройства с заводской конфигурацией

Основные элементы устройства:

- **оптический приемо-передатчик (SFF-модуль)** - предназначен для преобразования оптического сигнала в электрический;
- **процессор (PON-чип)** – является конвертором интерфейсов Ethernet и GPON;
- **Wi-Fi модули** – предназначены для организации беспроводных интерфейсов на устройстве.

При заводской (начальной) конфигурации в устройстве присутствуют следующие логические блоки (Рисунок 4):

- Br1;
- Voice (блок IP телефонии);
- eth0...3;
- FXS0;
- wl0, wl0.1..wl0.3, wl1, wl1.1..wl1.3;
- ppp0.1;
- IPInterface.

Блок br1 в данном случае предназначен для объединения портов LAN в одну группу.

Блоки eth0..3 физически являются Ethernet-портами с разъемом RJ-45 для подключения ПК, STB или других сетевых устройств. Логически включены в блок **br1**.

Блок FXS0 физически является портом с разъемом RJ-11 для подключения аналогового телефонного аппарата. Логически включен в блок Voice. Управление блоком Voice может осуществляться через WEB-интерфейс, а также удаленно с помощью сервера ACS по стандарту TR-069. В данном блоке задаются параметры сервиса VoIP (адрес SIP сервера, номер телефонного аппарата, услуги ДВО и т. д.).

Блоки wl0, wl0.1...wl1.3 являются интерфейсами для подключения Wi-Fi-модулей. Блоки wl0 являются интерфейсами для работы в диапазоне 2.4ГГц, блоки wl1 – в диапазоне 5ГГц.

Блоки Filter и Marking предназначены для включения локальных интерфейсов в одну группу (в блок **br1**). Отвечают за правила прохождения трафика, блоки **Filter** отвечают за входящий трафик на интерфейс, блоки **Marking** – за исходящий.

Блок IPInterface представляет собой некий логический объект, на котором располагается IP-адрес для доступа в локальной сети, а также сервер DHCP, раздающий адреса клиентам.

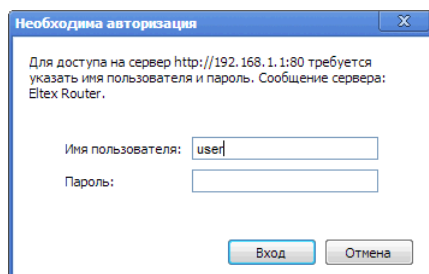
Блок **ppp0.1** является WAN-интерфейсом роутера. В заводской конфигурации этот интерфейс является интерфейсом по умолчанию для работы таких услуг, как Интернет, IP-телефония, управление устройством по стандарту TR-069 и IP-телевидение.

При подключении к устройству ОВ (установлении успешного соединения со стационарным оптическим устройством OLT) дополнительно создается блок **gpondef** при помощи протокола OMCI (ONT Management and Control Interface). Блок обеспечивает связь абонентского устройства ONT со стационарным.

4 НАСТРОЙКА NTU-RG-1421G-W, NTU-RG-1431G-W ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ

Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через web browser (программу для просмотра гипертекстовых документов), например, Firefox, Google Chrome. Для этого необходимо ввести в адресной строке браузера IP-адрес устройства (при заводских установках адрес: - 192.168.1.1, маска подсети – 255.255.255.0).

После введения IP-адреса устройство запросит имя пользователя и пароль.



Имя пользователя **user**, пароль **user**.

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (**раздел 4.5.4 Подменю Пароли. Настройка контроля доступа (установление паролей)**).

Ниже представлен общий вид окна конфигурирования устройства. Слева расположено дерево навигации по меню настроек объектов, справа – область редактирования параметров.


NTU-RG-1421G-Wac

- Информация об устройстве
- Расширенные настройки
- Беспроводная связь
- Хранилища
- Управление

Информация об устройстве / Общее

Тип платы:	NTU-RG-1421G-Wac
Серийный номер:	GP2F000057
Серийный номер PON:	454C545866000090
Основной WAN MAC:	A8:F9:4B:E3:14:D0
Идентификатор платы:	968380GERG
Версия платформы:	2v2

Версия ПО:	3.28.0.2376
CRC образа 1 (Активный):	E8F5A500
CRC образа 2:	F44AA613
Версия загрузчика (CFE):	1.0.38-116.232
Версия беспроводного драйвера:	7.14.124.47.cpe4.16L04patch2xpon

Системное время:	Чт. янв. 1 00:47:20 1970
Время в работе:	0Д 0Ч 47М 20С

4.1 Меню «Информация об устройстве»

4.1.1 Подменю *Общее*.

Информация об устройстве / Общее	
Тип платы:	NTU-RG-1421G-Wac
Серийный номер:	GP2F000057
Серийный номер PON:	454C545866000090
Основной WAN MAC:	A8:F9:4B:E3:14:D0
Идентификатор платы:	968380GERG
Версия платформы:	2v2
Версия ПО:	3.28.0.2376
CRC образа 1 (Активный):	E8F5A500
CRC образа 2:	F44AA613
Версия загрузчика (CFE):	1.0.38-116.232
Версия беспроводного драйвера:	7.14.124.47.cpe4.16L04patch2xpon
Системное время:	Чт. янв. 1 00:47:20 1970
Время в работе:	0Д 0Ч 47М 20С

4.1.2 Подменю **WAN**. Информация о состоянии сервисов

В данной вкладке выводится общая информация существующих конфигурациях интерфейса WAN.

Информация об устройстве / WAN / Общее												
Интерфейс	Описание	Тип	VlanMuxId	IPv6	Igmp Rxу	Igmp Src Вкл	MLD Rxу	MLD Src Вкл	NAT	Firewall	Статус	IPv4 Адрес
												IPv6 Адрес

4.1.2.1 Подменю *Подробно*. Подробная информация

В данной вкладке выводится подробная информация о существующих конфигурациях интерфейса WAN.

Для просмотра доступна следующая информация о сервисах:

- *Interface* – имя интерфейса;
- *Type* – режим работы интерфейса;
- *Connection Type* – тип подключения;
- *NAT* – статус NAT;
- *Firewall* – статус Firewall;
- *Status* – статус соединения;
- *IPv4 Address* – адрес для доступа;
- *Default Gateway* – шлюз по умолчанию;
- *Primary DNS Server*¹ – адрес первичного DNS сервера, используемого для работы;
- *Secondary DNS Server*¹ – адрес вторичного DNS сервера, используемого для работы;
- *Bridging to* – список связанных LAN-интерфейсов.

Информация об устройстве / WAN / Подробно	
WAN service 0: Internet.1100	
Interface: ppp0.1	
Type: PPPoE	
Connection type: IP_Routed	
NAT: Enabled	
Status: Connected	
IPv4 Address: 192.168.100.110	
Primary DNS Server: 192.168.100.1	
Secondary DNS Server: 10.10.0.2	
Bridging to: eth0,eth1,eth2,eth3,wl0	
WAN service 1: VoIP.1101	
Interface: veip0.2	
Type: IPoE	
Connection type: IP_Routed	
Status: Connected	
IPv4 Address: 192.168.101.179	
Default Gateway: 192.168.101.1	
Primary DNS Server: 192.168.198.102	
Bridging to: eth0,eth1,eth2,eth3,wl0	

¹ Только для сервиса **INTERNET, VoIP**

4.1.3 Подменю **LAN. Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса**

В данном меню доступен просмотр статусов и характеристик проводных и беспроводных интерфейсов LAN. Для проводных соединений указан статус, скорость соединения, режим работы (дуплекс/полудуплекс).

Информация об устройстве / LAN	
Порт 1	Включен; 1000M full
Порт 2	Выключен
Порт 3	Выключен
Порт 4	Включен; 1000M full
Wi-Fi 2.4	Выключен
Wi-Fi 5	Выключен

4.1.4 Подменю **Статистика. Информация о прохождении трафика на портах устройства**

В меню осуществляется просмотр статистики принятых и переданных пакетов для WAN Service, LAN и оптического интерфейса.

Интерфейс LAN:

Информация об устройстве / Статистика / LAN																
Интерфейс	Принято								Передано							
	Всего				Многоадресная		Одноадресная	Широковещательная	Всего				Многоадресная		Одноадресная	Широковещательная
	Байт	Пакетов	Ошибок	Потеряно	Байт	Пакетов	Пакетов	Пакетов	Байт	Пакетов	Ошибок	Потеряно	Байт	Пакетов	Пакетов	Пакетов
Port 1	29424	199	0	0	0	9	190	532	46822	187	0	0	0	28	159	1096
Port 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1628
Port 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1628
Port 4	5638	47	0	0	0	24	23	1102	1056	10	0	0	0	4	6	532
Wi-Fi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wi-Fi (wlan)	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0

Сброс статистики

WAN Service:

Информация об устройстве / Статистика / WAN сервисы

Интерфейс	Описание	Принято								Передано							
		Всего				Многоадресная		Одноадресная	Широковещательная	Всего				Многоадресная		Одноадресная	Широковещательная
		Байт	Пакетов	Ошибок	Потеряно	Байт	Пакетов	Пакетов	Пакетов	Байт	Пакетов	Ошибок	Потеряно	Байт	Пакетов	Пакетов	Пакетов
Сброс статистики																	

Интерфейс Optical:

Для устройств с возможностью измерения параметров оптического сигнала¹ данное меню имеет дополнительную таблицу.

¹ Опционально

Информация об устройстве / Статистика / Оптика							
Принято				Передано			
Байт	Пакетов	Ошибок	Потеряно	Байт	Пакетов	Ошибок	Потеряно
0	0	0	0	0	0	0	0

Сброс статистики

Состояние соединения	Уровень оптической мощности	Уровень оптической мощности передатчика	Температура	Всс напряжение	Ток смещения
Отключено	Нет сигнала	2.62 dBm	51.2 C	3.33 V	16.17 mA

Для обнуления данных и возобновления накопления статистики необходимо нажать «Сброс статистики».

4.1.5 Подменю **Маршрутизация**. Просмотр таблицы маршрутизации

В меню осуществляется просмотр таблицы маршрутизации.

Информация об устройстве / Маршрутизация						
Направление	Шлюз	Маска подсети	Флаг	Метрика	Сервис	Интерфейс
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br1

Flags:
 U - up,
 G - gateway,
 H - host,
 R - reinstate,
 D - dynamic (redirect),
 M - modified (redirect),
 ! - reject

- *Направление* – IP-адрес назначения;
- *Шлюз* – IP-адрес шлюза;
- *Маска подсети* – маска подсети (Genmask);
- *Флаг* – флаг маршрута:
 - *U* – маршрут активен;
 - *!* – нерабочий маршрут, пакеты будут отброшены;
 - *G* – маршрут использует шлюз (gateway);
 - *H* – адресом назначения является отдельный хост;
 - *R* – восстановленный маршрут;
 - *D* – устанавливается, если маршрут был создан по приходу перенаправляемого сообщения ICMP;
 - *M* – устанавливается, если маршрут был модифицирован перенаправляемым сообщением ICMP;
- *Метрика* – приоритет маршрута;
- *Сервис* – сервис, к которому относится маршрут;
- *Интерфейс* – сетевой интерфейс, к которому относится маршрут.

4.1.6 Подменю **ARP**. Просмотр кэша протокола ARP

Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся Internet-адреса и соответствующие им аппаратные адреса. Время жизни каждой записи в кэше 5 минут с момента создания записи.

Информация об устройстве / ARP

IP-адрес	Флаги	MAC-адрес	Устройство
192.168.1.11	Завершен	dc:85:de:b3:82:08	br1
192.168.1.10	Завершен	00:e0:52:fe:62:3a	br1

- *IP-адрес* – IP-адрес клиента
- *Флаги* – флаги состояния:
 - *Завершен* – клиент активен;
 - *Не завершен* – клиент не отвечает на ARP-запросы;
- *MAC-адрес* – MAC-адрес клиента;
- *Устройство* – интерфейс, на котором находится клиент.

4.1.7 Подменю **DHCP. Активные аренды DHCP**

В таблице DHCP можно посмотреть список активных аренд DHCP сервера и срок их истечения.

Информация об устройстве / DHCP

Interface Name	Interface Type	Имя хоста	MAC-адрес	IP-адрес	Истекает через
----------------	----------------	-----------	-----------	----------	----------------

- *Interface Name* – интерфейс, с которого был получен адрес;
- *Interface Type* – тип интерфейса;
- *Имя хоста* – имя сетевого устройства;
- *MAC адрес* – MAC адрес устройства;
- *IP адрес* – адрес устройства в локальной сети, выданный маршрутизатором из пула IP-адресов;
- *Истекает через* – время, через которое истекает аренда данного адреса.

4.1.8 Подменю **Беспроводные станции. Подключенные беспроводные устройства**

В данном меню доступен просмотр перечня аутентифицированных беспроводных устройств и их статус.

Информация об устройстве / Беспроводные станции

Эта страница показывает аутентифицированные беспроводные станции и их статус.

MAC-адрес	Связан	Авторизован	Имя сети (SSID)	Интерфейс
-----------	--------	-------------	-----------------	-----------

Обновить информацию

Данные об устройствах выводятся в таблице, содержащей следующие параметры:

- *MAC-адрес* – MAC-адрес устройства;
- *Связан* – статус связи с SSID;
- *Авторизован* – статус авторизации;
- *Имя сети (SSID)* – идентификатор сети, с которой связан клиент;
- *Интерфейс* – интерфейс доступа.

Для обновления данных необходимо нажать кнопку «Обновить информацию».

4.1.9 Подменю **Беспроводной монитор** Обнаруженные беспроводные сети

В данном меню доступен просмотр списка обнаруженных беспроводных сетей в радио-эфире.

Информация об устройстве / Беспроводной монитор

На данной странице показаны известные беспроводные сети.

2.4ГГц ▼

SSID	BSSID	Канал	RSSI
------	-------	-------	------

Обновить информацию

Данные об устройствах выводятся в таблице, содержащей следующие параметры:

- 2.4/5ГГц – частотный диапазон;
- *SSID* – идентификатор беспроводной сети;
- *BSSID* – MAC-адрес точки доступа;
- *Канал* – канал, на котором работает точка доступа;
- *RSSI* – уровень сигнала от точки доступа, принимаемый ONT.

Для обновления данных необходимо нажать кнопку «Обновить информацию».

4.1.10 Подменю **Телефония. Мониторинг состояния телефонного порта**

В данном меню доступен просмотр статуса FXS порта и параметры SIP-аккаунта.

Информация об устройстве / Телефония

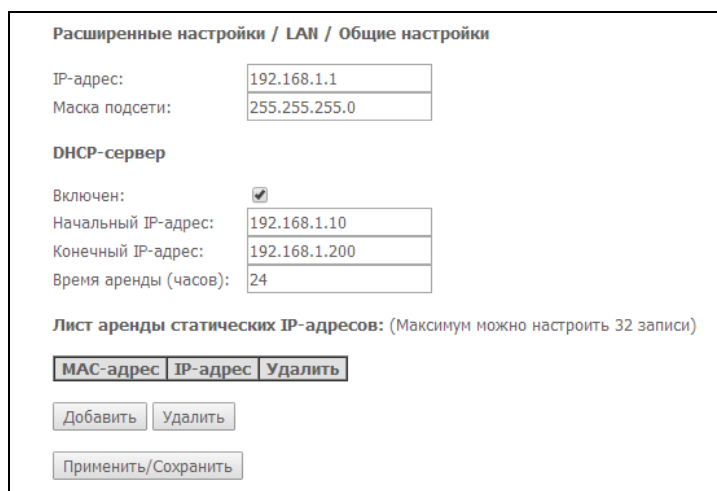
Состояние	Up
Номер	1001

- *Состояние* – состояние работы голосового демона;
- *Номер* – номер телефона.

4.2 Меню «Расширенные настройки». Расширенные настройки конфигурации

4.2.1 Подменю LAN. Настройка основных параметров

В данном меню производится настройка основных параметров для LAN интерфейса.



Расширенные настройки / LAN / Общие настройки

IP-адрес: 192.168.1.1
Маска подсети: 255.255.255.0

DHCP-сервер

Включен: ☒
Начальный IP-адрес: 192.168.1.10
Конечный IP-адрес: 192.168.1.200
Время аренды (часов): 24

Лист аренды статических IP-адресов: (Максимум можно настроить 32 записи)

MAC-адрес	IP-адрес	Удалить
Добавить Удалить		

Применить/Сохранить

IP адрес – адрес устройства в локальной сети.

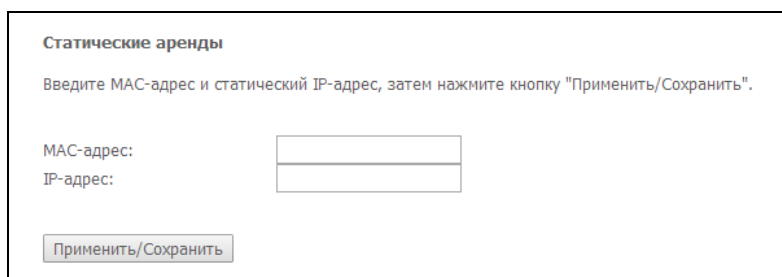
DHCP-сервер:

DHCP-сервер (Dynamic Host Configuration Protocol, протокол динамической настройки хостов) позволяет провести автоматическую настройку локальных компьютеров для работы в сети. Он назначает IP каждому компьютеру внутри сети. Эта дополнительная функция позволяет уйти от необходимости назначать IP-адреса вручную.

- *Включен* – при установленном флаге использовать DHCP сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *Начальный IP адрес* – начальный адрес диапазона;
- *Конечный IP адрес* – конечный адрес диапазона;
- *Время аренды (часов)* – время аренды адреса (в часах).

Лист аренды статических IP-адресов:

В данной таблице производится привязка выдаваемых IP-адресов MAC-адресам устройств. Для добавления записи в таблицу необходимо нажать «Add». Может быть установлено до 32 соответствий.



Статические аренды

Введите MAC-адрес и статический IP-адрес, затем нажмите кнопку "Применить/Сохранить".

MAC-адрес:
IP-адрес:

Применить/Сохранить

- *Mac адрес* – MAC-адрес устройства;
- *IP адрес* – IP-адрес устройства.

Для принятия и сохранения изменений необходимо нажать кнопку «Применить/Сохранить».

4.2.2 Подменю «NAT». Настройки NAT

Настройки NAT могут быть эффективны при работе устройства в режиме маршрутизатора.

4.2.2.1 Подменю *Виртуальные серверы*. Настройки виртуальных серверов

Виртуальный сервер – это функция маршрутизаторов, предназначенная для предоставления доступа пользователям через сеть Интернет к серверам, находящимся в Вашей локальной сети, например, к почтовым серверам, WWW, FTP. На устройстве может быть создано до 32 записей. Для обращения к устройствам из локальной сети по глобальным адресам предусмотрена функция NAT loopback.

Расширенные настройки / NAT / Виртуальные серверы

Виртуальный сервер позволяет направлять входящий трафик из WAN (идентифицирован по протоколу и внешнему порту) к внутреннему серверу, подключенному к LAN. Внутренний порт требуется только если внешний должен быть преобразован в другой порт, который используется на сервере в LAN. Можно настроить не более 32 записей.

Имя сервера	Внешний порт (начальный)	Внешний порт (конечный)	Протокол	Внутренний порт (начальный)	Внутренний порт (конечный)	IP-адрес сервера	WAN-интерфейс	NAT loopback	Удалить
Добавить Удалить									

Для добавления записи в таблицу фильтрации необходимо нажать «Добавить» и заполнить поля в открывшемся меню:

Расширенные настройки / NAT / Виртуальные серверы

Выберите имя сервиса, введите IP-адрес сервера и нажмите "Применить/Сохранить", чтобы направлять IP-пакеты для этого сервиса к указанному серверу.

Примечание: поле "Внутренний порт (конечный)" не может быть изменен напрямую. Обычно устанавливается таким же, как и "Внешний порт (конечный)".

Количество записей, которые еще можно добавить: 32

Используемый интерфейс: HSI/ppp0.1

Имя сервиса:

☒ Выберите сервис: Выберите...

☐ Другой сервис:

IP-адрес сервера: 192.168.0.

☒ Обратная петля NAT

Внешний порт (начальный)	Внешний порт (конечный)	Протокол	Внутренний порт (начальный)	Внутренний порт (конечный)
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		

Применить/Сохранить

– *Используемый интерфейс;*



Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов.

– *Имя сервиса* – настройки сервиса:

– *Выберите сервис* – выбор преднастроенного правила;

- *Другой сервис* – создать свои, не указанные в списке *Select a Service*, правила;
 - *IP-адрес сервера* – IP-адрес сервера, находящегося в локальной сети;
 - *Обратная петля NAT* – при установленном флаге пользователи из локальной сети могут получить доступ к локальным серверам по внешнему IP-адресу или доменному имени.
- *Внешний порт (начальный)* – начальный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
 - *Внешний порт (конечный)* – конечный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
 - *Протокол* – выбор сетевого протокола;
 - *Внутренний порт (начальный)* – начальный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора;
 - *Внутренний порт (конечный)* – конечный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора.

Для принятия и сохранения изменений необходимо нажать кнопку «Применить/Сохранить».

4.2.2.2 Подменю *Перенаправление портов*. Настройки запуска портов

Маршрутизатор по умолчанию блокирует все входящие запросы на установку соединения. Механизм работы функции Port Triggering заключается в том, чтобы при появлении определенного события динамически открывать порты на своем внешнем интерфейсе и привязывать их к соответствующим портам компьютера в локальной сети.

Расширенные настройки / NAT / Перенаправление портов

Некоторые приложения требуют отдельный определенный порт в firewall маршрутизатора для доступа из внешней сети. Функционал позволяет динамически открывать порт в firewall когда приложение в локальной сети инициирует TCP/UDP соединение с удаленной стороной, используя 'Триггер порты'. Маршрутизатор позволяет удаленной стороне устанавливать новые соединения к приложению в локальной сети, используя 'Открываемые порты'. Максимум можно сконфигурировать 32 записи.

Имя приложения	Протокол	Триггер		Протокол	Открываемый		WAN-интерфейс	Удалить
		Начало	Конец		Начало	Конец		
Asheron's Call	UDP	9000	9013	UDP	9000	9013	ppp0.1	☐

Для добавления правил в таблицу необходимо нажать кнопку «Добавить», удаление происходит нажатием кнопки «Удалить» напротив выбранного правила.

Расширенные настройки / NAT / Перенаправление портов

Некоторые приложения, такие как игры, видео конференции, программы удаленного доступа и другие, требуют отдельный определенный порт в firewall маршрутизатора для доступа этих приложений. Вы можете настроить конфигурацию порта из этого меню выбрав существующее приложение либо задав вручную (Другое приложение) и нажмете "Применить/Сохранить" чтобы его добавить.

Оставшееся число записей которые могут быть добавлены:31

Используемый интерфейс:

Имя приложения:

☒ Выберите приложение:

☐ Другое приложение:

Начальный триггер порт	Конечный триггер порт	Триггер протокол	Начальный открываемый порт	Конечный открываемый порт	Используемый протокол
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼

- Используемый интерфейс;



Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов.

- *Имя приложения* – настройки приложения:
 - *Выберите приложение* – выбор преднастроенного правила.
 - *Другое приложение* – создать свои, не указанные в списке Select an application, правила.

В отличие от функции *Virtual Server*, здесь нет необходимости фиксировано задавать IP-адрес компьютера в LAN.

- *Начальный триггер порт* – начальный порт диапазона портов, которые осуществляют функцию триггера;
- *Конечный триггер порт* – конечный порт диапазона портов, которые осуществляют функцию триггера;
- *Триггер протокол* – протокол, используемый для триггера;
- *Начальный открываемый порт* – начальный порт диапазона портов, которые маршрутизатор будет открывать;
- *Конечный открываемый порт* – конечный порт диапазона портов, которые маршрутизатор будет открывать;
- *Используемый протокол* – используемый протокол для открываемых портов.

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

4.2.2.3 Подменю **DMZ-хост**. Настройки демилитаризованной зоны

При установке IP-адреса в поле «*IP-адрес DMZ хоста*» все запросы из внешней сети, не попадающие под правила *Virtual Servers*, будут направляться на DMZ-хост (доверительный хост с указанным адресом, расположенный в локальной сети);

Для отключения данной настройки необходимо стереть IP-адрес из поля ввода.

Расширенные настройки / NAT / DMZ-хост

IP пакеты из WAN будут переданы на DMZ-хост, если они не принадлежат ни одному созданному виртуальному серверу.

Введите IP-адрес компьютера и нажмите "Применить/Сохранить" чтобы активировать DMZ-хост.

Очистите поле IP-адреса и нажмите "Применить/Сохранить" чтобы деактивировать DMZ-хост.

IP-адрес DMZ-хоста:

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

4.2.3 Подменю «**Безопасность**». Настройки безопасности

В данном разделе проводится настройка параметров безопасности устройства.

4.2.3.1 Подменю **IP фильтрация**. Настройки фильтрации адресов

Функция *IP фильтрация* позволяет фильтровать проходящий через маршрутизатор трафик по IP-адресам и портам.

Настройки фильтрации исходящего трафика (Outgoing):

Расширенные настройки / Безопасность / IP-фильтрация / Исходящий трафик

Весь исходящий трафик из локальной сети доступен, но нежелательный трафик может быть **ЗАБЛОКИРОВАН** с помощью создания фильтров.

ПРЕДУПРЕЖДЕНИЕ: Изменение одной политики на другую на интерфейсе приведет к автоматическому удалению всех правил для этого интерфейса! Вам необходимо создать новые правила для новой политики.

Нажмите "Добавить" или "Удалить" для настройки фильтрации исходящего трафика по IP-адресам.

Имя фильтра	Версия протокола IP	Протокол	MAC-адрес отправителя	IP-адрес источника / Префикс	Порт источника	IP-адрес назначения / Префикс	Порт назначения	Удалить
Добавить Удалить								



По умолчанию весь исходящий трафик будет пропускаться, правила, созданные в этом меню, позволят блокировать нежелательный трафик.

Для добавления нового правила фильтрации необходимо нажать кнопку «Добавить».

Расширенные настройки / Безопасность / IP-адреса / Исходящий трафик / Добавить

Здесь можно создать правило фильтрации чтобы идентифицировать исходящий IP-трафик определив имя фильтра и как минимум один параметр ниже. Все указанные условия в этом правиле фильтра должны удовлетворять условиям чтобы вступить в силу. Чтобы сохранить и активировать фильтр нажмите кнопку 'Применить/Сохранить'.

Имя фильтра:

Версия протокола IP:

Протокол:

MAC-адрес:

IP-адрес источника [/префикс]:

Порт источника (port либо port:port):

IP-адрес назначения[/префикс]:

Порт назначения (port либо port:port):

- Имя фильтра – текстовое описание фильтра;
- Версия протокола IP– выбор версии протокола IP;
- Протокол – выбор протокола(TCP/UDP, TCP, UDP, ICMP);
- MAC-адрес– MAC-адрес источника;
- IP адрес источника[/префикс] – IP-адрес источника (через слэш возможно указать длину префикса);
- Порт источника (port либо port:port) – порт источника или диапазон портов через двоеточие;
- IP адрес назначения [/префикс] – IP-адрес места назначения (через слэш возможно указать длину префикса);
- Порт назначения (port либо port:port) – порт места назначения или диапазон портов через двоеточие.

Для принятия и сохранения настроек необходимо нажать кнопку «Применить/Сохранить».

Настройки фильтрации входящего трафика:

Расширенные настройки / Безопасность / IP-фильтрация / Входящий трафик

При включении firewall на интерфейсе WAN или LAN весь входящий трафик будет заблокирован. Тем не менее, некоторый трафик может быть **ПРИНЯТ** с помощью создания фильтров.

Нажмите "Добавить" или "Удалить" для настройки фильтров по IP-адресам для входящего трафика.

Имя фильтра	Интерфейсы	Версия протокола IP	Протокол	MAC-адрес источника	IP-адрес источника / Длина префикса	Порт источника	IP-адрес назначения / Длина префикса	Порт назначения	Удалить
Добавить Удалить									



При включении брандмауэра на интерфейсе WAN или LAN весь входящий трафик, не попадающий под установленные правила, будет заблокирован.

Для добавления нового правила фильтрации необходимо нажать кнопку «Добавить».

Расширенные настройки / Безопасность / IP-адреса / Входящий трафик / Добавить

Здесь можно создать правила фильтрации, чтобы идентифицировать входящий IP-трафик определив имя фильтра и как минимум один параметр. Чтобы правило сработало, необходимо выполнение всех условий для данного фильтра. Чтобы сохранить и активировать фильтр нажмите кнопку 'Применить/Сохранить'.

Имя фильтра:

Версия IP:

Протокол:

MAC-адрес источника:

IP-адрес источника [/длина префикса]:

Порт источника (port либо port:port):

IP-адрес назначения [/длина префикса]:

Порт назначения:

Интерфейсы WAN (в режиме маршрутизации с включенным firewall) и интерфейсы LAN
 Выберите один или несколько интерфейсов WAN/LAN, из списка ниже, для применения данного правила.

☐ Выбрать все ☒ br1/br1

- *Имя фильтра* – текстовое описание фильтра;
- *Версия IP*– выбор версии протокола IP;
- *Протокол* – выбор сетевого протокола;
- *MAC-адрес*– MAC-адрес источника;
- *IP адрес источника[/префикс]* – IP-адрес источника (через слэш возможно указать длину префикса);
- *Порт источника (port либо port:port)* – порт источника или диапазон портов через двоеточие;
- *IP адрес назначения [/префикс]* – IP-адрес места назначения (через слэш возможно указать длину префикса);
- *Порт назначения (port либо port:port)* – порт места назначения или диапазон портов через двоеточие.

Интерфейсы WAN (сконфигурированные в режиме маршрутизатора и с включенным брандмауэром) и интерфейсы LAN:

- *Выбрать все* – при установленном флаге выбрать все возможные интерфейсы.

Либо выбрать интерфейс из приведенного списка, установив флаг напротив.

Для принятия и сохранения настроек необходимо нажать кнопку «Применить/Сохранить».

4.2.3.2 Подменю **MAC фильтрация**. Настройки фильтрации по MAC-адресам

Фильтрация на основе MAC-адресов позволяет пересылать или блокировать трафик с учетом MAC-адреса источника и получателя.

Расширенные настройки / Безопасность / MAC-фильтрация

Фильтрация по MAC влияет только на ATM PVCs настроенные в режим Bridge. **ОТПРАВЛЕН** значит, что все фреймы уровня MAC будут **ОТПРАВЛЕН** кроме тех которые соответствуют любым из правил приведенных в таблице ниже. **ЗАБЛОКИРОВАН** значит, что все фреймы уровня MAC будут **ЗАБЛОКИРОВАН** кроме тех, которые соответствуют любому правилу фильтрации из таблицы ниже.

Политика фильтрации MAC для каждого интерфейса:
ПРЕДУПРЕЖДЕНИЕ: Изменение одной политики на другую на интерфейсе приведет к автоматическому удалению всех правил для этого интерфейса! Вам необходимо создать новые правила для новой политики.

Интерфейс | Политика | Изменить

Изменить политику

Выберите "Добавить" или "Удалить" для настройки фильтров по MAC-адресам.

Добавить | Удалить

Интерфейс	Протокол	MAC-адрес назначения	MAC-адрес источника	Направление передачи	Удалить
-----------	----------	----------------------	---------------------	----------------------	---------

 **Фильтрация на основе MAC-адресов работает только для интерфейсов, находящихся в режиме моста (Bridge).**

Для изменения глобальной политики установите флаг напротив необходимого интерфейса и нажмите кнопку «Изменить политику» (изменить политику). Доступно два варианта: FORWARDED и BLOCKED.

В режиме FORWARDED созданные правила будут запрещать прохождение трафика с указанными MAC-адресами источника/получателя, в режиме BLOCKED – разрешать.

Добавить фильтр по MAC-адресу

Добавить фильтр для идентификации фреймов MAC уровня, указав как минимум одно условие. При задании нескольких условий все они вступят в силу. Чтобы сохранить и активировать фильтр нажмите кнопку "Применить/Сохранить".

Тип протокола:

MAC-адрес назначения:

MAC-адрес источника:

Направление передачи:

Выбор интерфейса WAN (доступны только интерфейсы, настроенные в режиме моста)

- Тип протокола – выбор протокола (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- MAC-адрес назначения – MAC-адрес получателя;
- MAC-адрес источника – MAC-адрес отправителя;
- Направление передачи – направление передачи (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- Выбор интерфейса WAN (доступны только интерфейсы, настроенные в режиме моста) – выбор WAN интерфейса из выпадающего списка (доступны только интерфейсы, работающие в режиме моста).

Для принятия и сохранения настроек необходимо нажать кнопку «Применить/Сохранить».

4.2.4 Подменю «Родительский контроль» – настройки ограничения

4.2.4.1 Подменю *Ограничение по времени*. Настройки ограничения продолжительности сеансов

В данном разделе производится конфигурирование расписания работы компьютеров с использованием дней недели и часов, по которым определенному компьютеру в локальной сети будет запрещен доступ в Интернет.

Расширенные настройки / Родительский контроль / Ограничение по времени

Максимум 16 записей может быть настроено.

Имя пользователя	MAC	Пн	Вт	Ср	Чт	Пт	Сб	Вс	Блокировать с	До	Удалить
Мом	00:e0:52:fe:62:3a	x	x	x	x	x			16:30	23:59	

Для создания нового расписания необходимо нажать кнопку «Добавить», всего может быть добавлено не более 16 записей.

Расширенные настройки / Родительский контроль / Ограничение по времени / Добавить

На этой странице можно добавить время дневного ограничения для конкретного устройства LAN, соединенное с маршрутизатором. 'MAC-адрес браузера' автоматически показывает MAC-адрес устройства LAN с которого запущен браузер. Чтобы ограничить другое устройство LAN, нажмите кнопку "Другой MAC-адрес" и введите нужный MAC. Чтобы определить MAC-адрес Windows-PK, необходимо открыть командную строку и напечатать "ipconfig /all".

Имя пользователя

☒ MAC-адрес браузера

☐ Другой MAC-адрес

(xx:xx:xx:xx:xx:xx)

Дни недели	Пн	Вт	Ср	Чт	Пт	Сб	Вс
Нажмите для выбора							

Время начала блокировки (чч:мм)

Время окончания блокировки (чч:мм)

- Имя пользователя – имя пользователя;
- MAC адрес браузера – автоматически определенный MAC-адрес компьютера, для которого задается расписание;
- Другой MAC адрес (xx:xx:xx:xx:xx:xx) – заданный вручную MAC-адрес компьютера, для которого определяется расписание;
- Дни недели – дни недели, запрещенные для доступа в интернет;
- Время начала блокировки (чч:мм) – время начала блокировки в формате ЧЧ:ММ;
- Время окончания блокировки (чч:мм) – время окончания блокировки в формате ЧЧ:ММ;



Ограничения будут действовать, если на устройстве установлено корректное системное время.

Для добавления настроек в таблицу необходимо нажать кнопку «Применить/Сохранить».

4.2.4.2 Подменю **Фильтр Url**. Настройки ограничения доступа в интернет

Фильтр Url– функция полноценного анализа и контроля доступа к определённым ресурсам сети интернет. В данном разделе задается список запрещенных/разрешенных **Url**-адресов для посещения.

Расширенные настройки / Родительский контроль / Фильтр URL-адресов

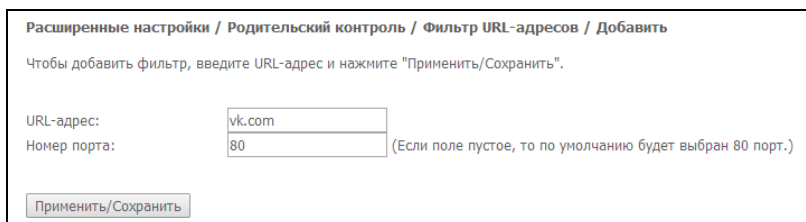
Пожалуйста, выберите сначала тип, а затем настройте остальные параметры. Максимум 100 записей может быть настроено.

Тип списка URL-адресов: ☒ Запрещенные ☐ Разрешенные

Адрес	Порт	Удалить
vk.com	80	

- Тип списка URL адресов – тип списка:
 - **Запрещенные** – запрещенные адреса;
 - **Разрешенные** – разрешенные адреса.

Для добавления нового адреса в список необходимо установить флаг напротив требуемого типа списка (*Тип списка URL адресов*) и нажать кнопку «Добавить».



- *URL адрес* – URL-адрес;
- *Номер порта* – номер порта (если оставить поле пустым, будет использоваться 80 порт).

Для добавления настроек в таблицу необходимо нажать кнопку «Применить/Сохранить».

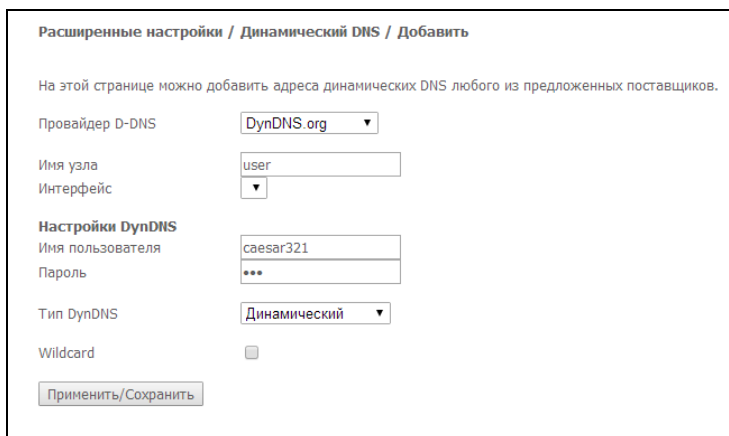
4.2.5 Меню «Динамическая DNS». Настройки динамической системы доменных имен

Динамическая DNS (динамическая система доменных имен) позволяет информации на DNS-сервере обновляться в реальном времени и (по желанию) в автоматическом режиме. Применяется для назначения постоянного доменного имени устройству (компьютеру, роутеру, например NTP-RG) с динамическим IP-адресом. Это может быть IP-адрес, полученный по IPCP в PPP-соединениях или по DHCP.

Динамическая DNS часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена в локальном DNS-сервере.



Для добавления записи необходимо нажать кнопку «Добавить», удаление происходит нажатием кнопки «Удалить» напротив выбранной записи.



- *Провайдер D-DNS*– выбор типа службы D-DNS (провайдера): *DynDNS.org, TZO.com, ZoneEdit.com, freedns.afraid.org, easyDNS.com, 3322.org, DynSIP.org, No-IP.com, dnsomatic.com, sitelutions.com;*
- *Custom* – иной провайдер, выбранный пользователем. В данном случае необходимо самостоятельно указать имя и адрес провайдера:

Расширенные настройки / Динамический DNS / Добавить

На этой странице можно добавить адреса динамических DNS любого из предложенных поставщиков.

Провайдер D-DNS: Custom

Имя узла:

Интерфейс:

Пользовательский D-DNS провайдер

Имя пользователя:

Пароль:

Имя провайдера сервера DDNS:

Адрес провайдера DDNS:

- *Имя пользователя* – имя пользователя для учетной записи DDNS;
 - *Пароль* – установка пароля для учетной записи DDNS;
 - *Имя провайдера сервера DDNS* – имя провайдера услуг DDNS;
 - *Адрес провайдера DDNS* – адрес провайдера услуг DDNS
- *Имя узла* – имя хоста, зарегистрированное у провайдера DDNS;
 - *Интерфейс* – интерфейс доступа;

В зависимости от выбранного провайдера возможны следующие поля для заполнения:

Расширенные настройки / Динамический DNS / Добавить

На этой странице можно добавить адреса динамических DNS любого из предложенных поставщиков.

Провайдер D-DNS: DynDNS.org

Имя узла:

Интерфейс:

Настройки DynDNS

Имя пользователя:

Пароль:

Тип DynDNS: Динамический

Wildcard: ☐

Расширенные настройки / Динамический DNS / Добавить

На этой странице можно добавить адреса динамических DNS любого из предложенных поставщиков.

Провайдер D-DNS: freedns.afraid.org

Имя узла:

Интерфейс:

Настройки freedns.afraid.org

Имя пользователя:

Пароль:

Расширенные настройки / Динамический DNS / Добавить

На этой странице можно добавить адреса динамических DNS любого из предложенных поставщиков.

Провайдер D-DNS: TZO.com

Имя узла:

Интерфейс:

Настройки TZO

Адрес электронной почты:

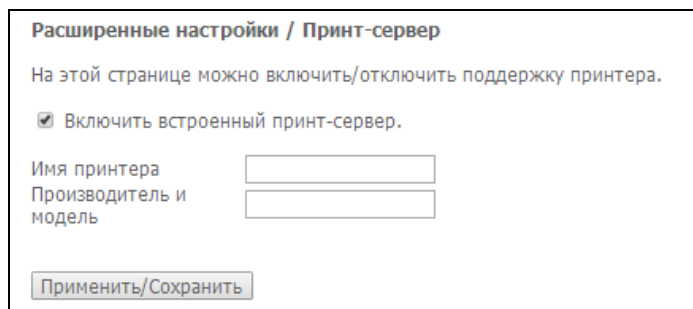
Ключ:

- *Имя пользователя* – имя пользователя для учетной записи DDNS;
- *Пароль* – установка пароля для учетной записи DDNS;
- *Тип DynDNS* – выбор типа услуги, зарегистрированной Вами у провайдера:
 - *Динамический* – зарегистрирована услуга Динамический DNS (Dynamic DNS);
 - *Статический* – зарегистрирована услуга Статический DNS (Static DNS);
 - *Пользовательский* – зарегистрирована услуга Пользовательский DNS (Custom DNS);
- *Wildcard* – при установленном флаге использовать специальную запись DNS, отвечающую за все поддомены, которая будет соответствовать любому запросу к несуществующему поддомену. Она указывается в виде * в качестве поддомена, например *.domain.tld.
- *Адрес электронной почты* – электронный адрес для аутентификации;
- *Ключ* – ключ для учетной записи DDNS.

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

4.2.6 Меню *Принт-сервер*. Настройки сервера печати

Принт-сервер (сервер печати) — программное обеспечение или устройство, позволяющее группе пользователей проводных и беспроводных сетей совместно использовать принтер дома или в офисе. Он не зависит ни от одного компьютера в сети, что дает возможность не перегружать рабочую среду пользователя. Кроме того, принт-сервер обеспечивает бесперебойную связь с принтером, МФУ, сканером или другой оргтехникой, находящейся в локальной сети.



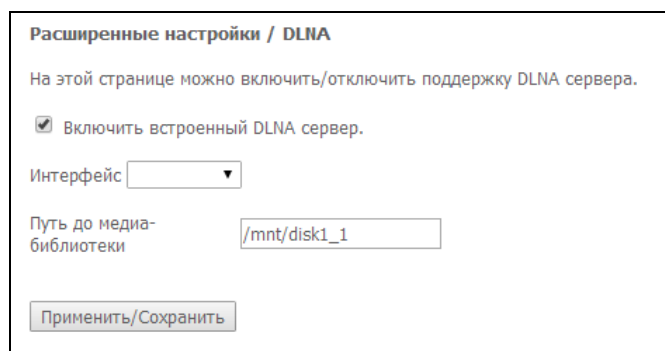
- *Включить встроенный принт-сервер* – при установленном флаге принт-сервер активен, иначе – нет;
- *Имя принтера* – имя принтера;
- *Производитель и модель* – производитель и модель принтера.

Для принятия и сохранения настроек необходимо нажать кнопку «*Применить/Сохранить*».

4.2.7 Меню *DLNA*. Настройки сервера DLNA

DLNA (англ. Digital Living Network Alliance) — набор стандартов, позволяющих совместимым устройствам передавать и принимать по домашней сети различный медиаконтент (изображения, музыку, видео), а также отображать его в режиме реального времени. То есть — технология для соединения домашних компьютеров, мобильных телефонов, ноутбуков и бытовой электроники в единую цифровую сеть. Устройства, которые поддерживают спецификацию DLNA, по желанию пользователя могут настраиваться и объединяться в сеть в автоматическом режиме.

Средой передачи медиаконтента обычно является домашняя локальная сеть (IP-сеть). Подключение DLNA-совместимых устройств к домашней сети может быть как проводным (Ethernet), так и беспроводным (Wi-Fi).



- *Включить встроенный DLNA сервер* – при установленном флаге медиасервер активен, иначе – нет;
- *Интерфейс* – имя интерфейса для подключения к серверу;
- *Путь до медиа-библиотеки* – каталог для медиафайлов.

Для принятия и сохранения настроек необходимо нажать кнопку «*Применить/Сохранить*».

4.2.8 Меню «UPnP». Автоматическая настройка сетевых устройств

В данном разделе производится настройка функции Universal Plug and Play (UPnP™).

UPnP обеспечивает совместимость с сетевым оборудованием, программным обеспечением и периферийными устройствами.

Расширенные настройки / UPnP

Примечание: UPnP активируется только тогда, когда есть WAN-сервис с включенным NAT.

☒ Включить UPnP



Для использования UPnP необходимо настроить NAT на активном WAN интерфейсе.

Для включения UPnP необходимо установить флаг «Включить UPnP».

Для принятия и сохранения настроек необходимо нажать кнопку «Применить/Сохранить».

4.3 Меню «Беспроводная связь». Настройка беспроводной сети

Настройки в данном меню производятся отдельно для рабочих диапазонов 2.4 ГГц и 5 ГГц

4.3.1 Подменю **Основные настройки**. Общая информация

В данном меню производятся основные настройки беспроводного интерфейса LAN, а также возможно задать до трех виртуальных точек беспроводного доступа.

Беспроводная связь / Основные настройки

На данной странице можно настроить основные параметры беспроводного LAN-интерфейса. Вы можете включить или выключить беспроводной LAN-интерфейс, скрыть сеть от активного сканирования, настроить имя беспроводной сети (SSID) и установить канал в соответствии с законодательством страны. Нажмите "Применить/Сохранить" для настройки основных параметров беспроводной сети.

☒ Включить беспроводную связь

Беспроводная связь - Точка доступа:

☒ Активировать точку доступа

☐ Скрыть точку доступа

☐ Изоляция клиентов

☐ Отключить распространение WMM

☒ Включить беспроводную многоадресную рассылку

SSID:

BSSID:

Страна:

Идентификатор региона:

Максимум клиентов:

Беспроводная связь - Гостевые/Виртуальные точки доступа:

Включен	SSID	Скрыт	Изолировать клиентов	Отключить распространение WMM	Включить WMF	Максимум клиентов	BSSID
☒	wl0_Guest1	☐	☐	☐	☒	16	A8:F9:4B:E3:14:D1
☐	wl0_Guest2	☐	☐	☐	☒	16	N/A
☐	wl0_Guest3	☐	☐	☐	☒	16	N/A

- **Включить беспроводную связь** – включить Wi-Fi на устройстве;
- **Активировать точку доступа** - включить поддержку Hotspot2.0 на устройстве;
- **Скрыть точку доступа** – скрытый режим работы точки доступа (в данном режиме SSID беспроводной сети не будет широкоэвещательно распространяться маршрутизатором);
- **Изоляция клиентов** – при установленном флаге беспроводные клиенты не смогут взаимодействовать друг с другом;
- **Отключить распространение WMM** – отключить WMM (Wi-Fi Multimedia – QoS для беспроводных сетей);
- **Включить беспроводную многоадресную рассылку (WMF)** – включить WMF;
- **SSID – Service Set Identifier** – назначить имя беспроводной сети(ввод с учетом регистра клавиатуры);



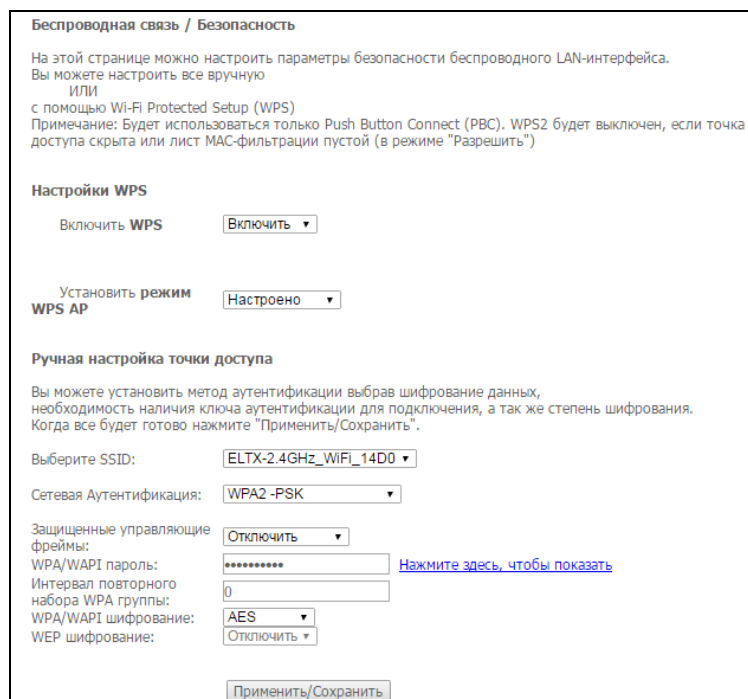
По умолчанию на устройстве установлено имя беспроводной сети (SSID) **ELTX-2.4GHz_WiFi-aaaa/ELTX-5GHz_WiFi-aaaa**, где aaaa - это 4 последние цифры WAN MAC. WAN MAC указан в наклейке на корпусе устройства. В имени сети фигурирует частотный диапазон (2.4/5ГГц).

- **BSSID** – MAC-адрес точки доступа;
- **Страна** – установить местоположение (страну);
- **Идентификатор региона** - установить идентификатор региона (для России: 0-34);
- **Максимум клиентов** – установить максимально возможное количество одновременных беспроводных подключений.

Для принятия изменений необходимо нажать кнопку «Применить/Сохранить».

4.3.2 Подменю **Безопасность**. Настройка параметров безопасности

В данном меню производятся основные настройки шифрования данных в беспроводной сети. Возможно настроить клиентское оборудование беспроводного доступа вручную или автоматически, используя WPS.



WPS (Wi-Fi Protected Setup) – стандарт, разработанный альянсом производителей беспроводного оборудования Wi-Fi с целью упрощения процесса настройки беспроводной сети. Данная технология позволяет пользователю быстро, просто и безопасно настроить беспроводную сеть, не вникая в тонкости работы Wi-Fi и протоколов шифрования. WPS автоматически задает имя сети и шифрование для защиты от несанкционированного доступа, что в иных случаях приходилось делать вручную.

Для того чтобы подключиться, достаточно нажать на кнопку WPS, расположенную на боковой панели устройства, или же ввести PIN-код, используя web-конфигуратор.

WPS setup:

- *Включить WPS* – для разрешения доступа по WPS в выпадающем списке выберите «Включить», если сетевой адаптер Wi-Fi Вашего устройства поддерживает данный режим настройки;
- *Установить режим WPS AP*– установить режим точки доступа WPS;



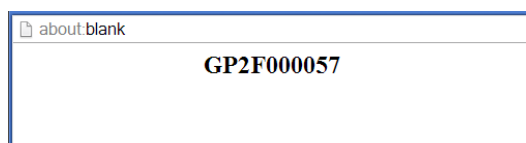
Недостатки метода WPS

В Wi-Fi роутерах с поддержкой технологии WPS существует уязвимость относительно безопасности сети. Используя эту уязвимость, возможно подобрать пароли к протоколам шифрования WPA и WPA2. Уязвимость заключается в том, что можно методом подбора узнать используемый восьмизначный ключ сети (PIN-код).

Ручная настройка точки доступа:

- *Выберите SSID*– выбрать имя беспроводной сети из списка;
- *Сетевая Аутентификация*– установить режим сетевой аутентификации из перечня в выпадающем списке:
 - *Open* – открытый – защита беспроводной сети отсутствует (в этом режиме может использоваться только WEP-ключ);

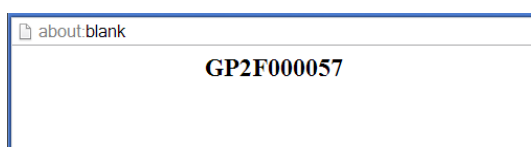
- *Shared* – общий (режим позволяет пользователям получать аутентификацию по их SSID или WEP-ключу);
- *802.1x* – включает стандарт 802.1x(позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ);
 - IP-адрес RADIUS-сервера – IP-адрес RADIUS-сервера;
 - *Порт RADIUS*– номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *Ключ RADIUS*– секретный ключ для доступа к RADIUS-серверу;
- *WPA2* – включает WPA2 (режим использует протокол WPA2 и требует использования сервера аутентификации RADIUS);
 - *Интервал повторного набора WPA группы* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *Порт RADIUS*– номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *Ключ RADIUS*– секретный ключ для доступа к RADIUS-серверу;
 - *WPA/WAPI шифрование* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);
- *WPA2-PSK* – включает WPA2-PSK (режим использует протокол WPA2, но не требует использования сервера аутентификации RADIUS);
 - *WPA/WAPI пароль* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «Нажмите здесь, чтобы показать», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

- *Интервал повторного набора WPA группы* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI шифрование* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);

- *Mixed WPA2/WPA* – включает комбинацию WPA2/WPA (данный режим шифрования использует протоколы WPA2 и WPA, требует использования сервера аутентификации RADIUS);
 - *Преаутентификация WPA2*– предварительная проверка подлинности беспроводного клиента на других беспроводных точках доступа в используемом диапазоне. В течение проверки связь осуществляется через текущую беспроводную точку доступа;
 - *Интервал преаутентификации сети* – период повторной проверки подлинности. Определяет, как часто точка доступа посылает сообщение и требует от клиентов ответа, содержащего правильные данные безопасности;
 - *Интервал повторного набора WPA группы* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *IP адрес RADIUS сервера* – IP-адрес RADIUS-сервера;
 - *Порт RADIUS*– номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *Ключ RADIUS*– секретный ключ для доступа к RADIUS-серверу;
 - *WPA/WAPI шифрование* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);
- *Mixed WPA2/WPA-PSK* – включает комбинацию WPA2/WPA-PSK (этот режим шифрования использует протоколы WPA2-PSK и WPA-PSK, не требует использования сервера аутентификации RADIUS).
 - *WPA/WAPI пароль* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*нажмите здесь, чтобы показать*», пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

- *Интервал повторного набора WPA группы* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI шифрование* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:
 - TKIP – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - AES – алгоритм 128 битного блочного шифрования с ключом 128/192/256 бит, используется обычно для WPA2);

Убедитесь, что беспроводной адаптер компьютера поддерживает выбранный тип шифрования.



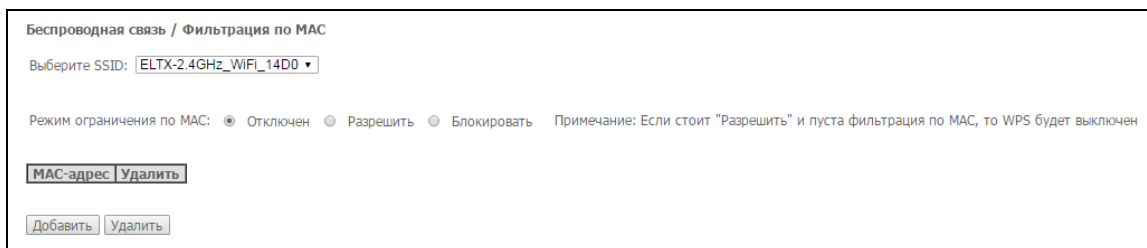
Наиболее стойкую защиту беспроводного канала даёт совместная работа точки доступа и RADIUS сервера (для аутентификации беспроводных клиентов).

- *WEP шифрование*— для включения шифрования WEP выберите *Enable* в выпадающем списке;
 - *Степень шифрования* – 64- или 128-битное шифрование ключа;
 - *Текущий сетевой ключ* – выбор ключа, который будет использоваться для установления соединения;
 - *Сетевой ключ 1..4* - возможно задать до четырех различных ключей из 10 символов в 16-ричной системе счисления либо 5 символов ASCII¹ для 64-х битного шифрования. Или 26 символов в 16-ричной системе счисления либо 13 символов ASCII для 128-х битного шифрования.

Для принятия изменений необходимо нажать кнопку «*Применить/Сохранить*».

4.3.3 Подменю **MAC-Фильтрация**. Настройки фильтрации MAC-адресов

В данном меню производится настройка фильтрации MAC-адресов



Беспроводная связь / Фильтрация по MAC

Выберите SSID: ELTX-2.4GHz_WiFi_14D0

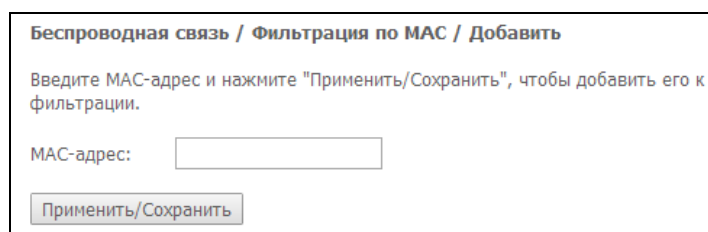
Режим ограничения по MAC: ☒ Отключен ☐ Разрешить ☐ Блокировать Примечание: Если стоит "Разрешить" и пуста фильтрация по MAC, то WPS будет выключен

MAC-адрес	Удалить

Добавить Удалить

- *Выберите SSID* – выбрать идентификатор беспроводной сети, для которой будет создано правило;
- *Режим ограничения по MAC*– выбор режима фильтрации по MAC-адресам:
 - *Отключен* – не использовать фильтр;
 - *Разрешить* – фильтр по разрешенным адресам;
 - *Блокировать* – фильтр по запрещенным адресам.

Для добавления MAC-адреса в таблицу фильтрации необходимо нажать «*Добавить*» и ввести его значение в поле «MAC адрес» в открывшемся меню:



Беспроводная связь / Фильтрация по MAC / Добавить

Введите MAC-адрес и нажмите "Применить/Сохранить", чтобы добавить его к фильтрации.

MAC-адрес:

Применить/Сохранить

Для принятия изменений необходимо нажать кнопку «*Применить/Сохранить*».

4.3.4 Подменю **Беспроводной мост**. Настройки беспроводного соединения в режиме моста

В данном меню задается режим работы точки доступа: в качестве точки доступа или беспроводного моста.

¹ ASCII - набор из 128 символов для машинного представления прописных и строчных букв латинского алфавита, чисел, знаков препинания и специальных символов.

При использовании режима моста необходимо ввести MAC-адреса удаленных мостов. Данный режим используется для установки беспроводного соединения между двумя отдельными сетями.

Беспроводная связь / Мост

На этой странице можно настроить параметры беспроводного моста в беспроводном LAN-интерфейсе. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Любые беспроводные мосты получают доступ. При выборе "Включен" или "Включен (Сканирование)" включится ограничение беспроводных мостов. Только указанные беспроводные мосты получают доступ..

Нажмите "Обновить" чтобы обновить удаленные мосты. Подождите несколько секунд. Нажмите "Применить/Сохранить" для настройки параметров беспроводного моста.

Ограничения моста:

Включен

MAC-адреса удаленных мостов:

MAC-адреса удаленных мостов:

SSID

BSSID

Обновить

Применить/Сохранить

В режиме «Беспроводной мост» возможно задать следующие настройки:

- *Ограничение моста* – выбор режима работы моста:
 - *Включен* – включить фильтр по MAC-адресам (разрешены только заданные адреса);
 - *Включен (Сканирование)* – поиск удаленных мостов;
 - *Выключен* – ограничения по MAC-адресам отсутствуют;
- *MAC адреса удаленных мостов* – адреса удаленных мостов.



В режиме моста маршрутизатор не поддерживает функцию Wi-Fi Multimedia (WMM).

Для обновления доступных удаленных мостов необходимо нажать «Обновить».

Для принятия и сохранения изменений необходимо нажать кнопку «Применить/сохранить».

4.3.5 Подменю *Расширенные настройки*

В данном меню производится расширенные настройки беспроводной сети.

Беспроводная связь / Расширенные настройки

На этой странице можно настроить расширенные параметры беспроводного LAN-интерфейса. Вы можете выбрать определенный канал для работы, установить определенную скорость передачи, порог фрагментации, порог RTS, интервал пробуждения для клиентов в режиме энергосбережения, установить интервал сигнализации для точки доступа, установить режим XPress, а также выбрать длину преамбулы.

Нажмите "Применить/Сохранить" для настройки расширенных параметров беспроводной связи.

Диапазон:

2.4GHz

Канал:

Auto

Текущее значение: 4 (помехи: приемлемые)

Таймер автоматического выбора канала(мин)

15

Standard:

n

Auto Channel Set:

Full

Allowed Channels:

1	2	3	4	5	6	7	8	9	10	11	12	13
☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

802.11n/EWC:

Авто

Ширина полосы:

Авто

Текущее значение: 20MHz

Боковая полоса управления:

Нижняя

Текущее значение: N/A

802.11n Уровень:

Auto

802.11n Защита:	Авто ▾	Состояние энергосбережения: Полная мощность
Трансляция RIFS:	Авто ▾	
Энергосбережение входной цепи:	Выключено ▾	
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Уровень:	1 Mbps ▾	
Уровень многоадресной рассылки:	Авто ▾	
Основной уровень:	По умолчанию ▾	
Порог фрагментации:	2346	
Порог RTS:	2347	
Интервал DTIM:	1	
Интервал сигнализации:	100	
Максимум клиентов:	16	
XPress™ Технология:	Выключено ▾	
Мощность передатчика:	100% ▾	
WMM(Wi-Fi Multimedia):	Включен ▾	
WMM без подтверждения:	Выключено ▾	
WMM APSD:	Включен ▾	
Формирование луча при передаче (BFR):	Выключено ▾	
Концентрация сигнала на приеме (BFE):	Выключено ▾	
Применить/Сохранить По умолчанию		

- *Диапазон* – установка частотного диапазона (2,4/5ГГц);
- *Канал* – устанавливает рабочий канал для маршрутизатора. При наличии помех или проблем в работе беспроводной сети изменение канала может способствовать их устранению. Рекомендуется установить значение "Auto" во избежание помех, вызываемых работой смежных сетей;
- *Таймер автоматического выбора канала (мин)* – время в минутах, через которое маршрутизатор будет искать более оптимальный беспроводный канал. Параметр доступен, если установлен Auto выбор канала (0 – выключить);
- *Standard* – установка стандарта 802.11;
- *Auto Channel Set* – определяет режим работы автовыбора каналов:
- *Full* – автовыбор производит сканирование и выбор канала из всех доступных каналов;
- *Legacy* – автовыбор производит сканирование и выбор канала из набора каналов, поддерживаемых старыми устройствами (только для диапазона 2.4 ГГц);
- *Custom* – автовыбор производит сканирование и выбор канала из списка, заданного пользователем в настройках «Allowed Channel».
- *802.11n/EWC* – режим совместимости с оборудованием 802.11n Draft2.0 и EWC(Enhanced Wireless Consortium);
- *Ширина полосы* – установка полосы пропускания 20ГГц или 40 ГГц. В режиме 40 МГц используются две смежные полосы по 20 МГц для увеличения пропускной способности канала;
- *Боковая полоса управления* – выбор второго канала(Lower или Upper) в режиме 40 МГц;
- *802.11n Уровень* – установка скорости соединения;
- *802.11n Защита* – при включении увеличится безопасность, но уменьшится пропускная способность;
- *Трансляция RIFS* – (Reduced Interframe Space) уменьшение интервала между блоками данных (PDUs), повышает эффективность Wi-Fi;
- *Энергосбережение входной цепи* – настройка толерантности при выборе режима работы (20МГц или 40МГц). Если параметр в состоянии «Включен» – будет выбран оптимальный режим работы устройства, учитывая «Полосу пропускания», иначе режим работы будет зависеть только от параметра «Полоса пропускания»;

- *RX Chain Power Save Quiet Time* – период времени, в течении которого интенсивность трафика должна быть ниже PPS, для включения режима энергосбережения;
- *RX Chain Power Save PPS* – верхняя граница параметра PPS (packet per second). Если в течение времени, определенного параметром «*RX Chain Power Save Quiet Time*», интенсивность пакетов на интерфейсе WLAN не превышает данную величину, включается режим энергосбережения;
- *54g™ Rate* – установка скорости в режиме совместимости с устройствами 54g™;
- *Уровень многоадресной рассылки* – установка скорости трафика при многоадресной передаче;
- *Основной уровень* – базовая скорость передачи;
- *Порог фрагментации* – установка порога фрагментации в байтах. Если размер пакета будет превышать заданное значение, он будет фрагментирован на части подходящего размера;
- *Порог RTS*– если сетевой пакет меньше, чем установленное пороговое значение RTS, механизм RTS/CTS (механизм соединения по каналу с использованием сигналов готовности к передаче/готовности к приему) задействован не будет;
- *Интервал DTIM*– временной интервал, по истечении которого широковещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам;
- *Интервал сигнализации* – период отправки информационного пакета в беспроводную сеть, сигнализирующего о том, что точка доступа активна;
- *Максимум клиентов* – максимальное количество беспроводных клиентов;
- *XPress™ Технология* – использование позволяет повысить пропускную способность до 27% в сетях стандарта 802.11g. А в смешанных сетях 802.11g и 802.11b использование XPress™ Technology может повысить пропускную способность до 75%;
- *Мощность передатчика* – определяется мощность сигнала точки доступа;
- *WMM (Wi-Fi Multimedia)* – установка режима Wi-Fi Multimedia (WMM). Данный режим позволяет быстро и качественно передавать аудио- и видеоконтент одновременно с передачей данных;
- *WMM без подтверждения* – при использовании данного режима приёмная сторона не подтверждает принятые пакеты. В среде с малым количеством помех это позволит увеличить эффективность передачи, в среде с большим количеством помех эффективность передачи снизится;
- *WMM APSD* – установить автоматический переход в режим экономии энергии (enabled – автоматический переход разрешен);
- *Beamforming Transmission (BFR)* – функция формирования луча позволяет уменьшить интерференцию при передаче беспроводного сигнала и улучшить качество Wi-Fi соединения;
- *Beamforming Reception (BFE)* – функция концентрации при приеме сигнала позволяет улучшить качество Wi-Fi соединения.

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

4.4 Меню «Хранилища». Службы файловых хранилищ

4.4.1 Подменю *Информация по устройству хранения*. Информация о подключенных USB-устройствах

В данном меню доступен список всех подключенных запоминающих устройств. Предоставляется следующая информация:

Служба хранения / Информация по устройству хранения				
Служба файловых хранилищ позволяет легко получить доступ к файловому хранилищу через сеть				
Имя раздела	Файловая система	Общий объем	Используемый объем	Действие

- *Имя раздела* – имя устройства;
- *Файловая система* – тип файловой системы;
- *Unmount* – для безопасного извлечения устройства необходимо предварительно нажать данную кнопку.

4.4.2 Подменю *Пользовательские аккаунты*. Настройка пользователей Samba

В данном меню происходит настройка учетных записей пользователей Samba.

Сервис хранения / Пользовательские аккаунты		
Нажмите "Добавить"/"Удалить" для настройки пользовательских аккаунтов.		
Имя пользователя	Домашняя папка	Удалить
Добавить Удалить		

Для добавления записи необходимо нажать кнопку «Добавить». Для удаления - установить флаг напротив требуемой записи в колонке Remove и нажать кнопку «Удалить».

Сервис хранения / Пользовательские аккаунты	
В полях ниже введите имя пользователя, пароль и имя тома на котором должен быть создан корневой каталог.	
Имя пользователя:	
Пароль:	
Подтвердите пароль:	
Имя тома:	
Применить/Сохранить	

- *Имя пользователя* – логин для доступа к сетевому ресурсу;
- *Пароль* – пароль для доступа к сетевому ресурсу;
- *Подтвердите пароль* – подтверждение пароля для доступа;
- *Имя тома* – путь к сетевому ресурсу (имя подключенного запоминающего устройства отображается на странице «Информация по устройству хранения»).

4.5 Меню «Управление». Управление устройством

4.5.1 Подменю *Настройки*

4.5.1.1 Подменю *Резервное копирование*

Меню позволяет по нажатию кнопки «Создать резервный файл» выгрузить конфигурацию на ПК.

Управление / Настройки / Резервное копирование

Сделать резервное копирование конфигурации широкополосного маршрутизатора. Вы можете сохранить все конфигурацию маршрутизатора в файл на вашем ПК.

Создать резервный файл

4.5.1.2 Подменю *Заводские настройки*. Возврат к настройкам по умолчанию

Меню позволяет вернуться к настройкам устройства, установленным по умолчанию. Устройство при этом будет перезагружено.

Управление / Настройки / Заводские настройки

Восстановить все настройки маршрутизатора к заводским.

Восстановить настройки по умолчанию



При выполнении данной операции все выполненные Вами настройки будут утрачены.

По нажатию на кнопку «Восстановить настройки по умолчанию» происходит сброс настроек к заводским. Устройство при этом будет перезагружено.

4.5.2 Подменю *Дата и время*. Настройки системного времени

Управление / Дата и время

НА этой странице можно настроить время на устройстве.

☒ Автоматически синхронизировать с сервисом времени через интернет

Первый NTP-сервер:	Другой ▼	ntp.local
Второй NTP-сервер:	Не выбран ▼	
Третий NTP-сервер:	Не выбран ▼	
Четвертый NTP-сервер:	Не выбран ▼	
Пятый NTP-сервер:	Не выбран ▼	

Часовой пояс: (GMT+03:00) Волгоград, Москва, Санкт-Петербург ▼

Применить/Сохранить

Во вкладке настраивается системное время на устройстве.

— *Автоматически синхронизировать с сервисом времени через интернет* — при установленном флаге производить автоматическую синхронизацию с интернет-серверами точного времени;

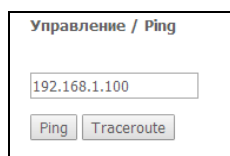
- *Первый NTP-сервер* – выбор основного сервера точного времени;
- *Второй NTP-сервер* – выбор второго сервера точного времени, *none* – не использовать дополнительные сервера;
- *Третий NTP-сервер* – выбор третьего сервера точного времени, *none* – не использовать дополнительные сервера;
- *Четвертый NTP-сервер* – выбор четвертого сервера точного времени, *none* – не использовать дополнительные сервера;
- *Пятый NTP-сервер* – выбор пятого сервера точного времени, *none* – не использовать дополнительные сервера;
- *Часовой пояс* – установка часового пояса в соответствии с всемирным координационным временем (UTC).



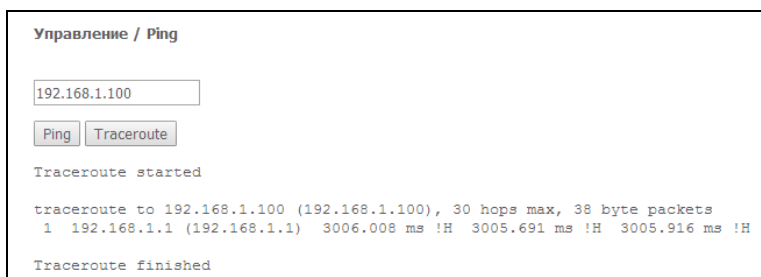
При выборе в выпадающем списке серверов значения *Другой* справа станет активным окно для заполнения, куда следует вручную ввести адрес сервера точного времени.

4.5.3 Подменю *Ping*. Проверка доступности сетевых устройств

Данное меню предназначено для проверки доступности подключенных к маршрутизатору сетевых устройств при помощи утилиты Ping.

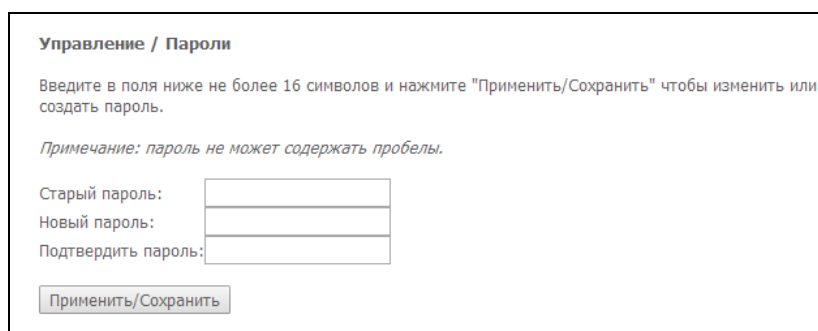


Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле и нажать кнопку «*Ping*». Для просмотра трассировки маршрута нажмите кнопку «*TraceRoute*». Вывод будет осуществлен на данной странице web-конфигуратора.



4.5.4 Подменю *Пароли*. Настройка контроля доступа (установка паролей)

В данном меню осуществляется смена пароля для доступа к устройству.



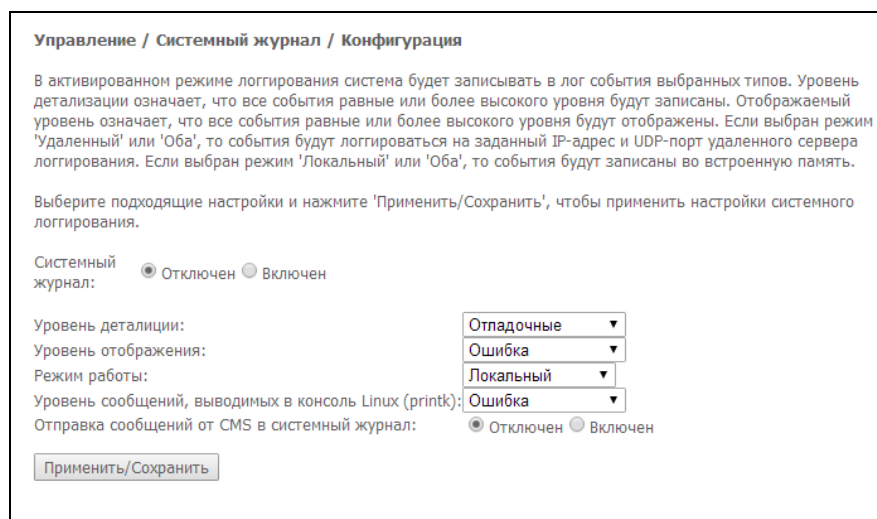
Для смены пароля необходимо ввести существующий пароль, затем новый пароль и подтвердить его.

Для принятия изменений и сохранения необходимо нажать кнопку «Применить/Сохранить».

4.5.5 Подменю **Системный журнал**. Просмотр и настройка системного журнала

4.5.5.1 Подменю **Конфигурация**. Настройка системного журнала

Меню используется для настройки событий, происходящих на маршрутизаторе.



Управление / Системный журнал / Конфигурация

В активированном режиме логирования система будет записывать в лог события выбранных типов. Уровень детализации означает, что все события равные или более высокого уровня будут записаны. Отображаемый уровень означает, что все события равные или более высокого уровня будут отображены. Если выбран режим 'Удаленный' или 'Оба', то события будут логгироваться на заданный IP-адрес и UDP-порт удаленного сервера логирования. Если выбран режим 'Локальный' или 'Оба', то события будут записаны во встроенную память.

Выберите подходящие настройки и нажмите 'Применить/Сохранить', чтобы применить настройки системного логирования.

Системный журнал: ☒ Отключен ☐ Включен

Уровень детализации: Отладочные ▼

Уровень отображения: Ошибка ▼

Режим работы: Локальный ▼

Уровень сообщений, выводимых в консоль Linux (printk): Ошибка ▼

Отправка сообщений от CMS в системный журнал: ☒ Отключен ☐ Включен

Применить/Сохранить

- **Системный журнал** – включение/выключение системного журнала(Отключен/Включен);
- **Уровень детализации** – установка уровня детализации журнала событий. Классификация уровней важности в порядке снижения значимости:
 - *Аварийный* – аварийный случай;
 - *Предупреждение* – тревога;
 - *Критический* – критическое событие;
 - *Отладочные* – устранение неполадок;
- **Уровень отображения** – установка уровня отображения выводимых сообщений журнала событий;
- **Режим работы** – режим работы журнала:
 - *Локальный* – местный (все события возвращаются на маршрутизатор через буферную память);
 - *Удаленный* – удаленный (все события возвращаются на сервер Syslog);
 - *Оба* – работают оба режима;
 - *USB-накопитель* – отправка на USB-накопитель;
- **Уровень сообщений, выводимых в консоль Linux (printk)** – установка уровня сообщений, выводимых в консоль Linux;
- **Отправка сообщений от CMS в системный журнал** – включение/выключение отправки сообщений от CMS в системный журнал.

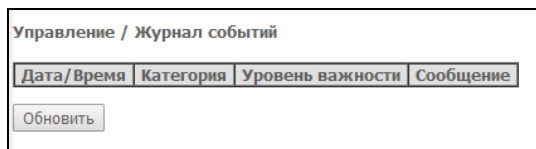
При выборе удаленного режима (Remote) доступны следующие настройки:

- **IP адрес сервера** – IP-адрес сервера Syslog, на котором сохраняются все события;
- **UDP-порт сервера** – номер порта сервера Syslog.

Для принятия изменений и сохранения необходимо нажать кнопку «Применить/Сохранить».

4.5.5.2 Подменю **Просмотр**. Просмотр системного журнала

Меню служит для просмотра событий, происходящих на маршрутизаторе.



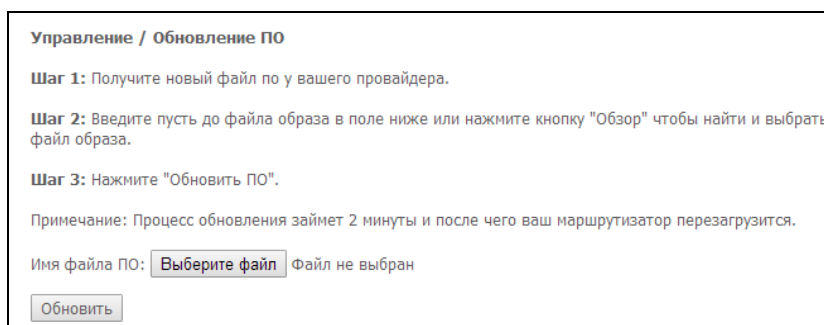
Обновить информацию можно кнопкой «Обновить».

4.5.6 Подменю **Обновить ПО**. Обновление ПО

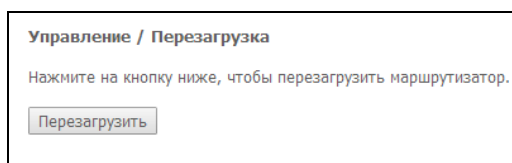
Для обновления ПО необходимо выбрать файл ПО в строке «Имя файла ПО» (используя кнопку «Выберите файл» или «Обзор») и нажать «Обновить».



В процессе обновления не допускается отключение питания устройства, либо его перезагрузка. Процесс обновления может занимать несколько минут, после чего устройство автоматически перезагружается.

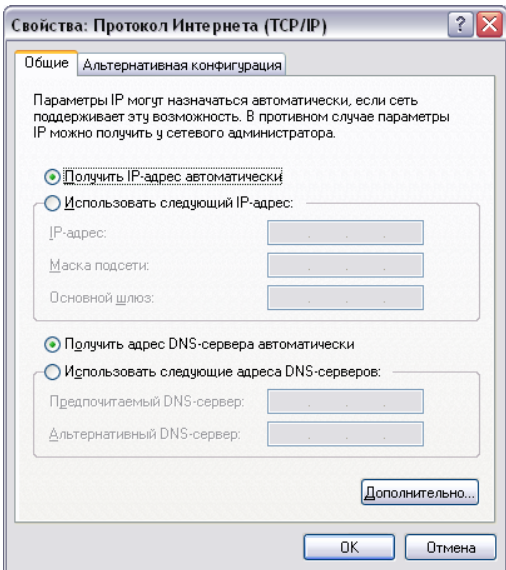


4.5.7 Подменю **Перезагрузка**. Перезагрузка устройства



Для перезагрузки устройства необходимо нажать на кнопку «Перезагрузить». Перезагрузка устройства может занять несколько минут.

ПРИЛОЖЕНИЕ А. ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ

Проблема	Возможная причина	Решение
При вводе IP-адреса маршрутизатора (например, 192.168.1.1) не удается получить доступ к Web-интерфейсу	компьютер не принадлежит к данной IP-подсети для подключения к Web-интерфейсу.	В свойствах подключения к интернету на Вашем компьютере установите параметр «Получать IP-адрес автоматически». 
	на компьютере установлен Web-браузер с выключенной опцией Java-script	включите опцию Java-script в Вашем браузере или воспользуйтесь другим Web-браузером
	неисправный кабель	проверьте физическое соединение по статусу индикаторов (они должны гореть). Если индикаторы не горят, попробуйте использовать другой кабель или подключитесь к другому порту устройства, если это возможно. Если компьютер выключен, индикатор может не гореть.
	доступ запрещен программным обеспечением интернет-безопасности Вашего компьютера	отключите программное обеспечение интернет-безопасности на компьютере (брандмауэры)
Утерян/не подходит пароль доступа к WEB-интерфейсу устройства	_____	Необходимо сбросить маршрутизатор к настройкам по умолчанию с помощью кнопки F на задней панели устройства. К сожалению, при этом все выполненные настройки будут утрачены.

СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ NTU-RG

Абонентский оптический терминал NTU-RG _____ зав. № _____
соответствует требованиям технических условий ТУ6650-101-33433783-2013, ТУ6650-108-33433783-2014 и
признан годным для эксплуатации.

Транспортирование оборудования должно производиться по условиям 5, хранение – по условиям 1
по ГОСТ 15150.

Предприятие-изготовитель ООО «Предприятие «ЭЛТЕКС» гарантирует соответствие абонентского
шлюза требованиям технических условий ТУ6650-101-33433783-2013, ТУ6650-108-33433783-2014 при
соблюдении потребителем условий эксплуатации, установленных в настоящем руководстве.

Гарантийный срок 1 год. Дата изготовления указана на упаковке.

Изделие не содержит драгоценных материалов.

Директор предприятия _____

подпись

Черников А. Н.

Ф.И.О.

Начальник ОТК предприятия _____

подпись

Игонин С.И.

Ф.И.О.

Изготовитель:
ООО «Предприятие «ЭЛТЕКС»
630020 г. Новосибирск,
ул. Окружная, 29В
E-mail: eltex@eltex.nsk.ru

Сделано в России

