



# Руководство администратора

## ВЕРСИЯ 4.8

## АННОТАЦИЯ

Настоящий документ предназначен для выполнения работ по администрированию программного обеспечения «Kraftway Terminal Linux», которое устанавливается на терминальные станции модельного ряда Kraftway Credo VV. В документе содержится подробная информация: о назначении, функциональных особенностях, установке, настройке, работе и системном обслуживании программного обеспечения «Kraftway Terminal Linux», приводятся информационные сообщения, сообщения об ошибках и способы их устранения. В данном документе большое внимание уделяется настройке терминальной станции.

Данное руководство ориентировано на системных администраторов, а также специалистов, прошедших специальный курс подготовки в сфере терминальных технологий.

## СОДЕРЖАНИЕ

1. Общие сведения .....	6
1.1. Общая информация .....	6
1.2. Назначение и функции ПО «KTL» .....	6
1.3. Архитектура информационной системы терминального решения .....	8
1.4. Сведения о функциональных ограничениях на применение ПО«KTL» .....	10
1.5. Аппаратные средства терминала .....	10
1.6. Программные средства терминала .....	17
2. Состав ПО «KTL» .....	18
3. Загрузка ПО «KTL» .....	19
3.1. Загрузка терминальной станции в режиме Legacy BIOS .....	20
3.1.1. Вход в режиме пользователя .....	20
3.1.2. Вход в режиме администратора .....	21
3.2. Загрузка терминальной станции в режиме UEFI .....	23
3.2.1. Настройка параметров загрузки .....	23
3.2.2. Вход в режиме администратора .....	26
3.2.3. Проверка подписи KTL .....	27
3.3. Загрузка терминальной станции по PXE .....	29
3.3.1. Настройка параметров загрузки .....	29
3.3.1.1. Настройка PXE сервера .....	29
3.3.1.2. Настройка терминальной станции .....	30
3.3.2. Вход в режиме администратора .....	32
4. Настройка ПО «KTL» .....	33
4.1. Описание рабочего стола .....	33
4.2. Настройка клиентского окружения терминальной станции с помощью консоли администратора .....	35
4.2.1. Локальный вход в консоль администратора .....	35
4.2.2. Удалённый вход в консоль администратора .....	37
4.2.3. Описание меню консоли администратора .....	39
4.2.4. Пункт меню Информация .....	39
4.2.4.1. Вкладка Система .....	40
4.2.4.2. Вкладка Основная .....	40

4.2.4.3. Вкладка Сетевой интерфейс .....	41
4.2.4.4. Вкладка USB.....	42
4.2.4.5. Вкладка Процессор .....	43
4.2.4.6. Вкладка Трафик.....	44
4.2.4.7. Вкладка Журналы.....	45
4.2.5. Пункт меню Система .....	47
4.2.5.1. Вкладка Время .....	47
4.2.5.2. Вкладка Приложения.....	49
4.2.5.3. Вкладка Пароль .....	51
4.2.5.4. Вкладка VNC .....	53
4.2.5.5. Вкладка Обновить .....	54
4.2.5.6. Вкладка Автообновление.....	59
4.2.5.7. Вкладка Сертификаты .....	62
4.2.6. Пункт меню Устройства.....	64
4.2.6.1. Вкладка Устройства .....	64
4.2.6.2. Вкладка COM over IP.....	70
4.2.7. Пункт меню Сеть .....	71
4.2.7.1. Вкладка TCP/IP.....	72
4.2.7.2. Вкладка DNS.....	79
4.2.7.3. Вкладка Routes .....	80
4.2.7.4. Вкладка Proxu.....	82
4.2.7.5. Вкладка Проверка .....	84
4.2.7.6. Вкладка Active Directory.....	86
4.2.7.7. Вкладка KSM .....	88
4.2.7.8. Вкладка VPN .....	91
4.2.8. Пункт меню Подключения.....	100
4.2.8.1. Вкладка Автоподключение.....	100
4.2.8.2. Вкладка Сценарии .....	103
4.2.9. Пункт меню Безопасность.....	116
4.2.9.1. Вкладка Ограничение доступа .....	116
4.2.9.2. Вкладка Kaspersky .....	117
4.2.9.3. Вкладка SSL .....	120
4.2.10. Пункт меню Управление .....	121



4.2.10.1. Вкладка Управление .....	121
4.2.10.2. Вкладка Настройки.....	122
4.3. Настройка клиентского окружения терминальной станции с удалённого компьютера через VNC сессию .....	126
4.4. Установка и настройка печатающих устройств .....	128
4.4.1. Установка локального принтера .....	129
4.4.2. Настройка локального принтера.....	136
4.4.3. Установка и настройка принт-сервера.....	138
4.4.4. Установка и настройка сетевого принтера .....	152
4.5. Удаление печатающих устройств.....	157
4.6. Установка и настройка сканирующих устройств .....	159
4.6.1. Установка и настройка скан-сервера .....	159
4.6.2. Установка и настройка сканера штрих-кодов .....	159
4.7. Обновление ПО терминальной станции.....	160
4.7.1. Обновление ПО терминальной станции из системного меню.....	160
4.7.2. Создание загрузочного USB-flash диска для установки ПО .....	163
4.8. Подключение к терминальному серверу .....	164
4.9. Дополнительные возможности системного меню.....	166
4.9.1. Работа в командной строке .....	166
4.9.2. Работа с утилитой сканирования .....	167
4.9.3. Вывод информации о системе .....	169
4.9.4. Контрольная сумма системы .....	169
4.9.5. Настройка звука.....	170
4.9.6. Спящий режим .....	172
4.10. Аутентификации пользователя с помощью USB-ключа (смарт-карты).....	173
5. Сообщения администратору .....	174
Приложение 1 .....	175
Перечень принятых сокращений .....	176

## 1. ОБЩИЕ СВЕДЕНИЯ

### 1.1. Общая информация

Наименование программного обеспечения (ПО) - Программное обеспечение «Kraftway Terminal Linux».

Краткое наименование ПО - ПО «Kraftway Terminal Linux» или ПО «KTL».

Версия ПО - 4.8.

Обозначение ПО - 643.18184162.00005-09.

Дата изготовления - 15.05.2019.

Адрес предприятия-изготовителя: 249032, Калужская область, г. Обнинск, Киевское ш., д.64, АО «Крафтвэй корпорэйшн ПЛС».

### 1.2. Назначение и функции ПО «KTL»

ПО «KTL» - это операционная система Linux разработки компании АО «Крафтвэй корпорэйшн ПЛС». ПО «KTL» представляет собой комплексное системное решение, предназначенное для создания защищённых автоматизированных систем и обеспечивающее эффективный и безопасный доступ к распределённым сетевым информационным ресурсам организации на основе технологии терминального доступа. В качестве клиентских рабочих мест используются терминальные устройства, терминальные станции модельного ряда Kraftway Credo VV, далее именуемые терминалами или тонкими клиентами.

Основные возможности терминального решения ПО «KTL», составляющие его функционал и описывающие классы решаемых задач, представлены ниже:

#### 1) функциональность:

- предоставление пользователю терминала возможности запуска сессий ОС Windows по протоколам: ICA, RDP, Spice, ALP, сессий ОС Unix (Linux) по протоколам: X11, NX, OpenSSH, Spice, ALP, X2GO, платформонезависимой сессии VNC по протоколу RFB, сессий VMWare View по протоколам RDP, PCOIP;

- предоставление пользователю терминала возможности работы с программами, входящими в состав ПО «KTL» без предварительного открытия терминальных сессий: web-браузером Mozilla FireFox версии 52.3.0, web-браузером

7Chromium версии 54.0.2840.59, программой просмотра и печати публикаций (pdf-файлов) Document Viewer версии 2.32.0, «опубликованными» Windows-приложениями через Citrix-клиент;

- поддержка возможности использования на терминале внешних USB-устройств: флэш-дисков, дисководов гибких дисков (floppy disk), CD/DVD приводов или жестких дисков (HDD);

- поддержка USB Ethernet сетевых устройств;

- поддержка звука на терминале;

- поддержка печати на локальном и сетевом принтерах;

- поддержка сканирования документов на локальном сканере;

- предоставление пользователю возможности использования терминала в роли принт-, скан-сервера (выполняется администратором);

## 2) надёжность:

- долгий срок службы терминала (отсутствие движущихся механических частей);

- снижение тепловыделения за счёт использования менее мощных процессоров;

- сохранение состояния пользовательской сессии на сервере при внезапном отключении электропитания терминала или аппаратных сбоях в терминальной системе;

## 3) безопасность:

- исключение возможности несанкционированного съёма информации за счёт отключения портов ввода-вывода на уровне ОС (выполняется администратором);

- выполнение разграничения доступа к данным и программам обеспечивается с помощью системных средств на сервере;

- обеспечение защиты информации благодаря шифрованию сетевого трафика;

- исключение возможности установки программных средств с клиентского рабочего места, что позволяет снизить риски нарушения целостности информации от воздействия вирусов и других деструктивных программ «внутри» вычислительной сети;

- обеспечение аутентификации пользователя при входе в сессии ОС Windows по протоколам RDP, ICA с помощью персональных средств строгой аутентификации и хранения данных, аппаратно поддерживающих работу с цифровыми сертификатами и ЭЦП (USB-ключей или смарт-карт компании ЗАО «Аладдин Р.Д.»: eToken Pro, eToken NG-OTP, eToken NG-FLASH, eToken Pro 72K (Java), eToken GT 4k/8k, JaCarta

<http://www.aladdin-rd.ru>, идентификаторов компании ЗАО «Актив-софт»: Rutoken S, Rutoken iBank2Key, Rutoken ЭЦП, <http://www.rutoken.ru>;

4) производительность:

- предоставление увеличения скорости выполнения пользовательских офисных приложений, а также программ, которые требуют передачи больших объёмов данных по локальной сети, таких как: 1С, Парус - обеспечивается за счёт использования мощных серверов, на которые возложена обработка пользовательских расчётов, и уменьшения объёма пересылаемых по локальной сети данных;

5) удобство:

- обеспечение комфортной работы пользователя за счёт использования «бесшумных» терминалов, в которых применены пассивные методы охлаждения процессора и системной логики;

- предоставление возможности получения доступа к рабочему столу пользователя и его данным с любого терминала организации;

- обеспечение возможности простого изменения количества пользовательских программ за счёт их установки или удаления на терминальном сервере;

6) администрирование:

- перенос функционала клиентского рабочего места на серверную сторону, что позволяет обеспечить централизованное управление информационными ресурсами, системой защиты информации и антивирусной защитой, практически исключить постоянные затраты сил и средств на локальное администрирование рабочих мест;

- предоставление возможности локальной и удалённой настройки терминальной станции;

- обеспечение быстрой установки новой и замены неисправной терминальной станции;

7) экономичность:

- обеспечение экономии электроэнергии.

### 1.3. Архитектура информационной системы терминального решения

Информационная система (ИС), построенная с применением ПО «КТЛ» включает в себя следующие компоненты: клиентские рабочие места (терминальные станции), терминальные серверы, одновременно выступающие в роли серверов-посредников, и

существующие информационные подсистемы предприятия с различными уровнями защиты информации.

Процесс работы ИС на примере одной терминальной станции выглядит следующим образом: терминальная станция при загрузке получает в зависимости от настроек виртуальный или статический IP-адрес для доступа к соответствующим терминальным серверам. Терминальные серверы, в свою очередь, выступают в роли серверов-посредников, которые обеспечивают связь с терминальной станцией, формирование запрашиваемой пользовательской сессии, связь выполняемых приложений с соответствующими прикладными ресурсами существующих подсетей (Интранет и Интернет). При выполнении запросов с терминальной станции и обработке пользовательской информации терминальные серверы транслируют состояние выполняемой сессии на монитор терминала.

Пример построения ИС при использовании ПО «KTL» представлен на рис.1.1.

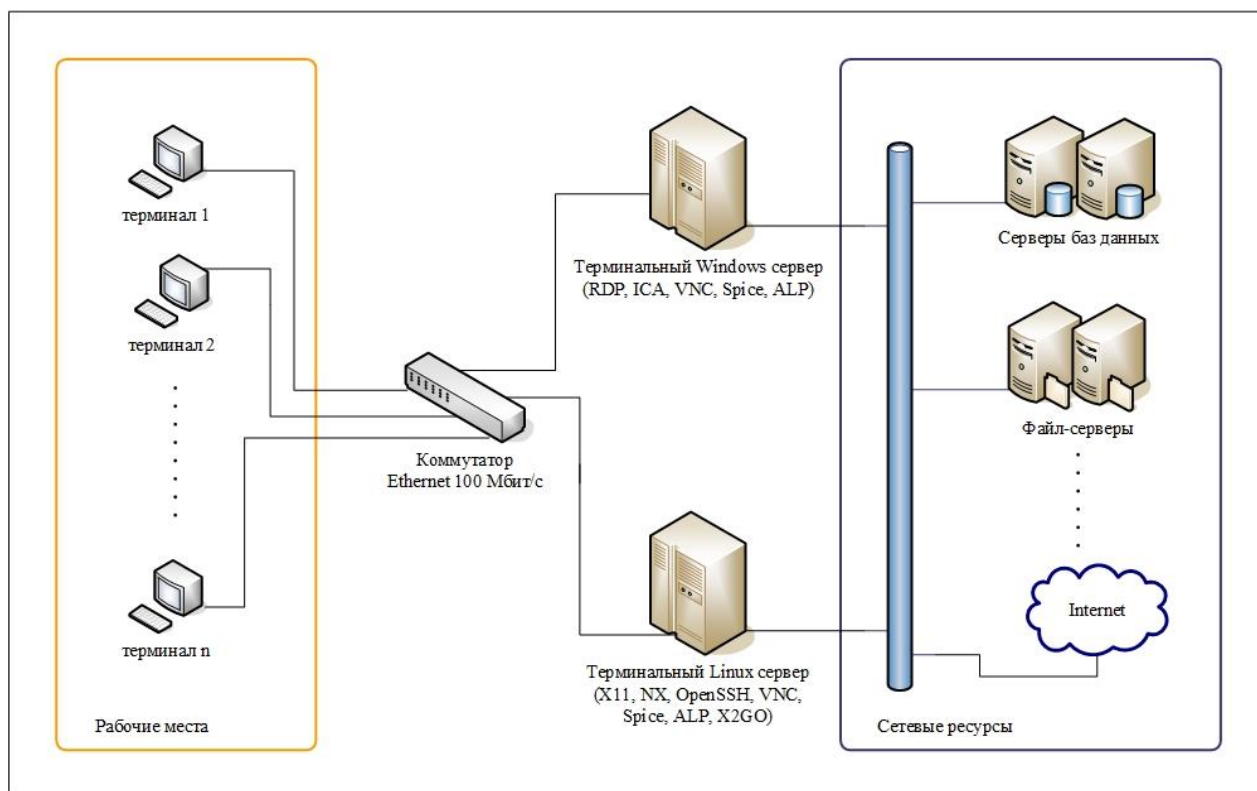


Рис.1.1

#### 1.4. Сведения о функциональных ограничениях на применение ПО «KTL»

ПО «KTL» устанавливается на терминалы и в основном предназначена для сетевого использования. При этом ЛВС должна быть построена на технологии Ethernet 100 Мбит/с с подключением терминалов к сетевому коммутатору. ОЗУ терминала:

- для моделей Credo VV18, Credo VV20, Credo VV22 составляет 2 Гб;
- для модели Credo VV23 - до 4 Гб;
- для модели Credo VV25, VV26 - до 8 Гб.

Ёмкость устройства обеспечения загрузки (flash-диск) терминала - не менее 512 Мб.

#### 1.5. Аппаратные средства терминала

Внешний вид терминальных станций модельного ряда Kraftway Credo VV представлен на рисунках 1.2-1.6.

Терминальная станция Kraftway Credo VV18 (рис.1.2)



Рис. 1.2

Терминальная станция Kraftway Credo VV20 (рис.1.3)



Рис. 1.3

Терминальная станция Kraftway Credo VV22 (рис.1.4)



Рис.1.4

Терминальная станция Kraftway Credo VV23 (рис.1.5)



Рис.1.5

Терминальная станция Kraftway Credo VV25/ Kraftway Credo VV26 (рис.1.6)



Рис.1.6

Более подробная информация о технических характеристиках терминальных станций приведена в таблице 1.1.



Таблица 1.1 - Технические характеристики терминальных станций модельного ряда Kraftway Credo VV

Наименование характеристики	Описание характеристики				
	VV18	VV20	VV22	VV23	VV25
Форм-фактор	уменьшенный Mini ITX (170 x 120 мм)	уменьшенный Mini ITX (170 x 120 мм)	уменьшенный Mini ITX (170 x 120 мм)	уменьшенный Mini ITX (170 x 120 мм)	Специальный (уменьшенный Mini ITX (170 x 140 мм))
BIOS	Award от Kraftway	Award от Kraftway	UEFI AMI от Kraftway	UEFI AMI от Kraftway	UEFI AMI от Kraftway
Чипсет	Intel NM10	Intel NM10	Intel NM10	Intel NM10	интегрированный в процессор (SoC)
Процессор	Intel Atom N 450 (1.66 ГГц, 2 потока, 512 КБ кэш L2)	Intel Atom N 450 (1.66 ГГц, 2 потока, 512 КБ кэш L2)	Intel Atom N 2600 (1.6 ГГц, 2 ядра, 4 потока, 1024 КБ кэш L2)	Intel Atom N 2800 (1.86 ГГц, 2 ядра, 4 потока, 1024 КБ кэш L2)	Intel Celeron N 2930 (1.83 ГГц, 4 ядра, 4 потока, 2 МБ кэш L2)
Оперативная память	Unbuffered SDRAM, DDR2, SoDIMM, 667 МГц, до 2 ГБ	Unbuffered SDRAM, DDR2, SoDIMM, 667 МГц, до 2 ГБ	Unbuffered SDRAM, DDR3, SoDIMM, 800 МГц, до 2 ГБ	Unbuffered SDRAM, DDR3, SoDIMM, 800 МГц, до 4 ГБ	Unbuffered SDRAM, DDR3L, SoDIMM, 1066 МГц, до 8 ГБ
Количество SoDIMM слотов	1	1	1	1	2
Режим работы оперативной памяти	1 каналный	1 каналный	1 каналный	1 каналный	2 каналный
Слоты расширения	1xMini PCI-Express (x1)	1 x Mini PCI-Express (x1)	1 x Mini PCI-Express (x1)	1 x Mini PCI-Express (x1)	2 x Mini PCI-Express (x1)
Разъёмы IDE	—	—	—	—	—
Разъёмы SATA	2xSATA II	2 x SATA II	1 x SATA II с комбинированным питанием, 1 x SATA II с отдельным питанием	1 x SATA II с комбинированным питанием, 1 x SATA II с отдельным питанием	1 x SATA II с комбинированным питанием
Видео адаптер	интегрированный в процессор Intel GMA 3150	интегрированный в процессор Intel GMA 3150	интегрированный в процессор Intel GMA 3600	интегрированный в процессор Intel GMA 3600	интегрированный в процессор Intel HD Graphics
Аудио адаптер	интегрированный в	интегрированный в	интегрированный в	интегрированный в	интегрированный в

Наименование характеристики	Описание характеристики				
	VV18	VV20	VV22	VV23	VV25
	материнскую плату 5.1 channel HDA	материнскую плату 5.1 channel HDA	материнскую плату 5.1 channel HDA	материнскую плату 5.1 channel HDA	материнскую плату 5.1 channel HDA
Сетевой адаптер	Ethernet контроллер 10/100/1000 Мбит/с (тип разъёма RJ45), интегрированный в материнскую плату	Ethernet контроллер 10/100/1000 Мбит/с (тип разъёма RJ45), интегрированный в материнскую плату	2 Ethernet контроллера 10/100/1000 Мбит/с (тип разъёма RJ45), интегрированных в материнскую плату	2 Ethernet контроллера 10/100/1000 Мбит/с (тип разъёма RJ45), интегрированных в материнскую плату, встроенный оптоволоконный многомодовый 100Base-FX адаптер	2 Ethernet контроллера, интегрированных в материнскую плату: Gigabit Ethernet 10/100/1000 Мбит/с (тип разъёма RJ45), оптоволоконный многомодовый 100/1000 Base-FX адаптер (тип разъёма SFP GBIC)
Носители информации	4 ГБ Flash Disk	4 ГБ Flash Disk, от 128 ГБ до 500 ГБ (2.5") SATA 2 HDD, 5400 об/мин или SSD	от 250 ГБ до 500 ГБ (2.5") SATA 2 HDD, 5400 об/мин или SSD	от 250 ГБ до 500 ГБ (2.5") SATA 2 HDD, 5400 об/мин, или SSD, или SATA DOM	от 60 ГБ до 512 ГБ (2.5") SATA SDD или SATA DOM
Считыватель смарт- карт	–	–	–	интегрированный считыватель смарт-карт стандарта ISO 7816 класса А, В и С	интегрированный считыватель смарт- карт стандарта ISO 7816 класса А, В и С
Разъёмы на передней панели	2 x USB 2.0, 1 x Line-Out, 1 x Mic	2 x USB 2.0, 1 x Line-Out, 1 x Mic	4 x USB 2.0, 1 x Line-Out, 1 x Mic	2 x USB 2.0, 1 x слот считывателя смарт-карт, 1 x Line-Out, 1 x Mic	1 x USB 3.0, 2 x USB 2.0, 1 x слот считывателя смарт-карт
Разъёмы на задней панели	4 x USB 2.0/1.1, 1 x D-Sub (VGA), 1 x RJ45, 1 x Line-Out, 1 x Mic, 1 x разъем внешнего питания	4 x USB 2.0/1.1, 1 x D-Sub (VGA), 1 x RJ45, 1 x Line-Out, 1 x Mic, 1 x разъем внешнего питания	4 x USB 2.0/1.1, 1 x D-Sub (VGA), 1 x HDMI, 2 x RJ45, 1 x Line-Out, 1 x разъем внешнего питания	4 x USB 2.0/1.1, 1 x D-Sub (VGA), 1 x HDMI, 2 x RJ45, 1 x SC duplex Outlet, 1 x Line-Out, 1 x разъем внешнего	4 x USB 2.0/1.1, 2 x HDMI, 1 x RJ45, 1 x SFP, 1 x Line- Out, 1 x Mic, 1 x разъем внешнего питания

Наименование характеристики	Описание характеристики				
	VV18	VV20	VV22	VV23	VV25
				питания	
Адаптер Wi-Fi	Wi-Fi 802.11 B/G	Wi-Fi 802.11 B/G	Wi-Fi 802.11 B/G	–	–
Элементы управления на корпусе	1 кнопка включения/ выключения питания	1 кнопка включения/ выключения питания	1 кнопка включения/ выключения питания	1 кнопка включения/ выключения питания	1 кнопка включения/ выключения питания
Индикаторы на корпусе	1 х индикатор активности в кнопке включения/ выключения питания, 1 х индикатор активности жесткого диска, 1 х индикатор сетевой активности	1 х индикатор активности в кнопке включения/ выключения питания, 1 х индикатор активности жесткого диска, 1 х индикатор сетевой активности	1 х индикатор активности в кнопке включения/ выключения питания, 1 индикатор активности жесткого диска, 1 х индикатор сетевой активности (индикаторы RJ45 - 4 шт. на задней панели)	1 х индикатор активности в кнопке включения/ выключения питания, 1 индикатор активности жесткого диска, 1 индикатор активности считывателя смарт-карт, 1 х индикатор сетевой активности (индикаторы RJ45 - 4 шт. на задней панели)	1 х индикатор активности в кнопке включения/ выключения питания, 1 индикатор активности жесткого диска, 1 индикатор активности считывателя смарт-карт, 1 индикатор МДЗ, 2 х индикатора сетевой активности (на передней панели), 2 индикатора RJ45 (на задней панели), 2 индикатора оптической сетевой карты (на задней панели)
Корпус (тип, цвет, ВхШхГ, доп. инф.)	специального исполнения, чёрный, 30 х 202 х 133 мм (без учета VESA-крепежа), отсеки для установки дополнительных устройств и вентиляторы охлаждения отсутствуют, VESA- крепление в комплекте	специального исполнения, черный, 45 х 202 х 133 мм (без учета VESA-крепежа), отсеки для установки дополнительных устройств и вентиляторы охлаждения отсутствуют, VESA- крепление в комплекте	специального исполнения, черный, 37 х 202 х 133 мм (без учета VESA-крепежа), отсеки для установки дополнительных устройств и вентиляторы охлаждения отсутствуют, VESA- крепление в комплекте	настольного исполнения, черный, 240 х 55 х 135 мм, отсеки для установки дополнительных устройств и вентиляторы охлаждения отсутствуют	настольного исполнения, черный, 45 х 180 х 145 мм, отсеки для установки дополнительных устройств и вентиляторы охлаждения отсутствуют

Наименование характеристики	Описание характеристики				
	VV18	VV20	VV22	VV23	VV25
Блок питания	внешний, 36 Вт	внешний, 36 Вт	внешний, 36 Вт	внешний, 36 Вт	внешний, 36 Вт
Специализированная версия BIOS (опционально)	–	–	полностью переработанная версия UEFI AMI BIOS от Kraftway, не содержит не декларированных возможностей	полностью переработанная версия UEFI AMI BIOS от Kraftway, не содержит не декларированных возможностей	полностью переработанная версия UEFI AMI BIOS от Kraftway, не содержит не декларированных возможностей
Оболочка безопасности (опционально)	–	–	оболочка Kraftway Secure Shell (KSS) для запуска модулей безопасности на уровне UEFI BIOS	оболочка Kraftway Secure Shell (KSS) для запуска модулей безопасности на уровне UEFI BIOS	оболочка Kraftway Secure Shell (KSS) для запуска модулей безопасности на уровне UEFI BIOS
Идентификация и аутентификация (опционально)	–	–	модуль безопасности СЗ от НСД «ПК электронный замок Витязь» v 1.1	модуль безопасности СЗ от НСД «ПК электронный замок Витязь» v 1.1	модуль безопасности СЗ от НСД «ПК электронный замок Витязь» или интегрированный не извлекаемый АПМДЗ "Криптон-Витязь"
Антивирусная защита (опционально)	–	–	модуль безопасности Kaspersky Antivirus for UEFI	модуль безопасности Kaspersky Antivirus for UEFI	модуль безопасности Kaspersky Antivirus for UEFI
Сетевой контроль и управление (опционально)	–	–	сервер безопасности Kraftway Security Center (KSC)	сервер безопасности Kraftway Security Center (KSC)	сервер безопасности Kraftway Security Center (KSC)
Мониторинг и групповое управление (опционально)	ПО Kraftway System Manager (KSM)	ПО Kraftway System Manager (KSM)	ПО Kraftway System Manager (KSM)	ПО Kraftway System Manager (KSM)	ПО Kraftway System Manager (KSM)

В приложении 1 приведена информация о технической поддержке пользователей.

#### 1.6. Программные средства терминала

ПО «KTL» содержится в устройстве обеспечения загрузки (SATA Flash Disk, SATA II HDD, SATA II SSD, SATA DOM).

## 2. СОСТАВ ПО «KTL»

ПО «KTL» состоит из следующих элементов:

- подсистема загрузки ОС «Kraftway Terminal Linux» терминальной станции;
- системные пакеты расширения;
- подсистема настройки терминальной станции.

### 3. ЗАГРУЗКА ПО «KTL»

Перед тем, как приступить к работе с ПО «KTL» необходимо выполнить подготовительные действия по созданию рабочего места пользователя: распаковка, установка, подключение периферийных устройств к терминальной станции.

Для большей наглядности, при описании действий, названия кнопок приводятся в квадратных скобках ([ ]), активация или нажатие на них обозначается стрелкой (→), а последовательность действий обозначается с помощью последовательности стрелок, например, →<название пункта 1 меню 1> →<название подпункта 1 подменю 1>, название окон и различных параметров приводится курсивом, например: в окне *Мой компьютер*. При описании последовательностей действий предполагается, что нажатие на кнопки, выбор требуемых параметров, значений в интерфейсе ПО и каких-либо элементов интерфейса ПО выполняется пользователем следующим образом: наведение курсора мыши на требуемый объект (кнопка, параметр, значение и элемент интерфейса ПО) и нажатие левой кнопки мыши. В тексте данные действия пользователя приводятся в краткой форме, например: нажать на кнопку [Сохранить изменения] или →[Сохранить изменения], выбрать вкладку *Принтеры*. Также при описании последовательностей действий предполагается, что вызов контекстного меню какого-либо объекта интерфейса ПО выполняется пользователем следующим образом: наведение курсора мыши на требуемый объект и нажатие правой кнопки мыши.

Загрузка ОС «Kraftway Terminal Linux» терминальной станции по умолчанию автоматически производится через традиционный BIOS (Legacy BIOS). Пользователям ПО KTL версий 4.5 и выше стали доступны и другие режимы загрузки:

- режим UEFI;
- загрузка по сети в PXE режиме.

Выбор режима загрузки производится администратором при настройке ПО терминальной станции.

Вход в ОС может выполняться в двух режимах: нормальном (пользователя, normal), безопасном (администратора, safe). Далее приводится подробное описание этих режимов.

### 3.1. Загрузка терминальной станции в режиме Legacy BIOS

Для загрузки ОС необходимо включить терминал, нажав кнопку включения питания. После включения терминала программа BIOS выполняет процедуру тестирования и начальную настройку оборудования (POST - Power On Self Test).

Далее выполняется загрузка ядра ОС и запуск системных процессов, сопровождающихся выводом соответствующих сообщений. На экран выводится заставка Kraftway с системным приглашением boot: (рис. 3.1).

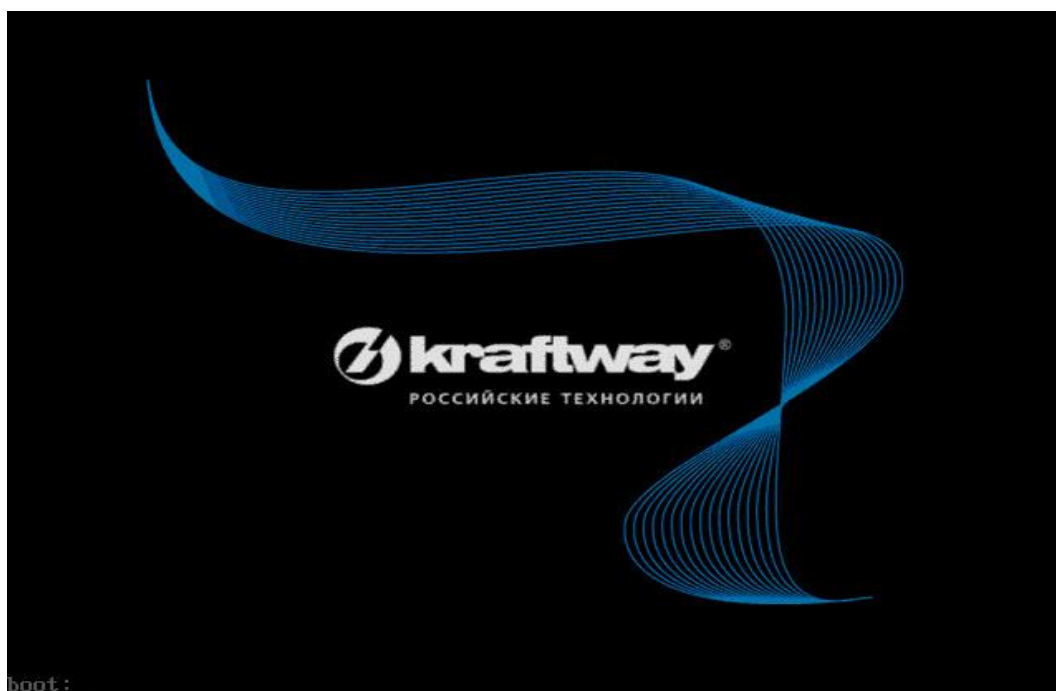


Рис. 3.1

Если не вводить специальных команд на этом этапе терминальная станция автоматически загрузится в нормальном режиме (режиме пользователя).

#### 3.1.1. Вход в режиме пользователя

Вход в систему в режиме пользователя (нормальном режиме, normal) после включения терминальной станции выполняется двумя способами:

1) автоматически (ОС «Kraftway Terminal Linux» загружается в нормальном режиме по умолчанию);



2) вручную (ввод команды normal при выводе системного приглашения boot:).

Процесс загрузки в режиме пользователя завершается запуском рабочего стола пользователя (рис. 3.2).

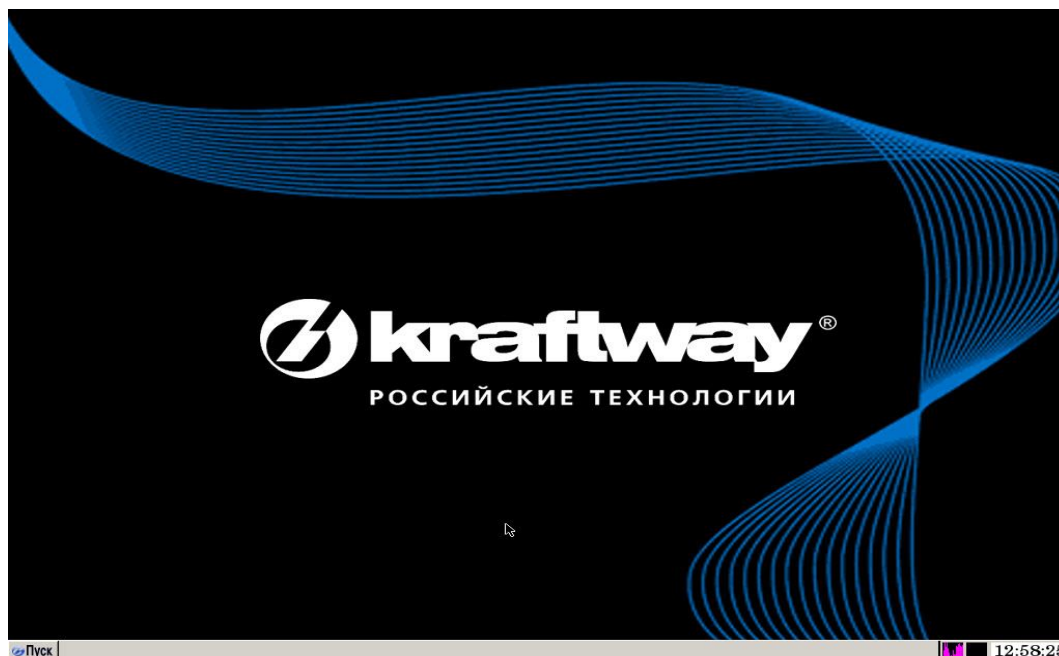


Рис. 3.2

### 3.1.2. Вход в режиме администратора

Вход в систему в режиме администратора (безопасном режиме safe) после включения терминальной станции следует:

- 1) дождаться окончания выполнения процедуры тестирования и начальной настройки оборудования (POST - Power On Self Test);
- 2) ввести команду s или safe при выводе системного приглашения boot: (рис.3.3);
- 3) нажать клавишу [Enter] на клавиатуре, далее на этапе загрузки ОС «Kraftway Terminal Linux» терминальной станции на экран выводится системное окно (рис. 3.4) для ввода пароля администратора;
- 4) →[OK], процесс загрузки ОС завершается запуском рабочего стола администратора (рис. 3.5).



Рис. 3.3

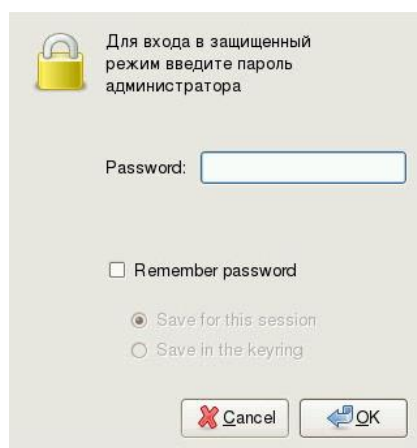


Рис. 3.4



Рис. 3.5

### 3.2. Загрузка терминальной станции в режиме UEFI

Пользователю ПО «КТЛ» (версий 4.5 и выше) предоставляется возможность загрузки терминальной станции в режиме UEFI (Unified Extensible Firmware Interface). UEFI это стандартный интерфейс встроенного ПО для компьютеров, заменяющий BIOS.

#### 3.2.1. Настройка параметров загрузки

Для использования UEFI-режима при загрузке ПО нужно предварительно настроить параметры загрузки в BIOS терминальной станции:

- 1) вход в BIOS→*Сохранение и выход*;
- 2) в настройках параметра *Произвести загрузку с* выбрать из списка загрузок пункт *UEFI OS* (рис. 3.6);
- 3) →[Enter].

Терминальная станция перезагрузится в UEFI в режиме пользователя.

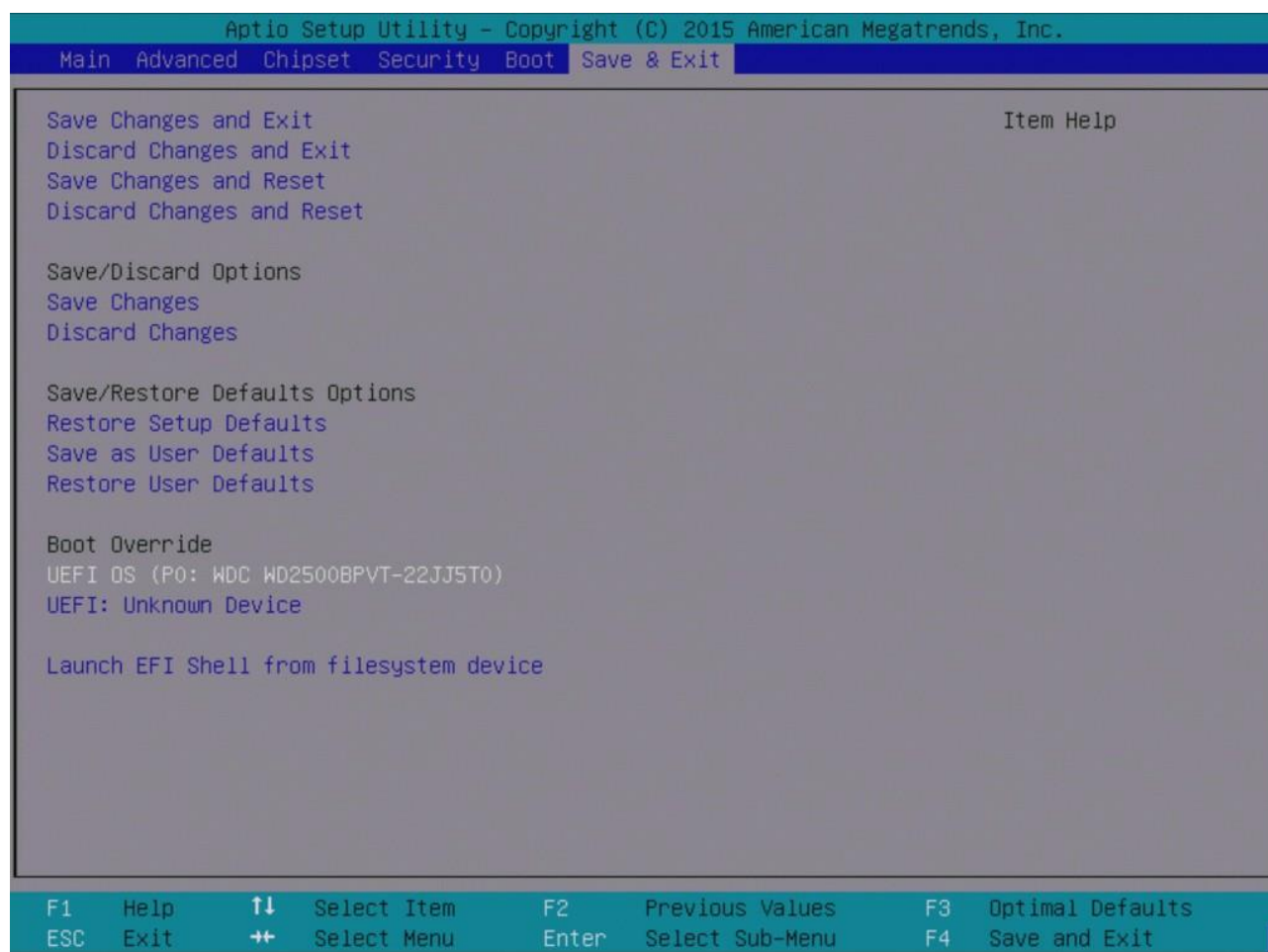


Рис. 3.6

Если в списках загрузки нет UEFI, то требуется произвести следующие настройки:

- 1) вход в BIOS→*Настройки*;
- 2) →*Настройка модуля совместимости* →*Фильтр начальной загрузки*;
- 3) выбрать пункт *UEFI и наследуемые* или *Только UEFI* (рис. 3.7);
- 4) →[Enter].

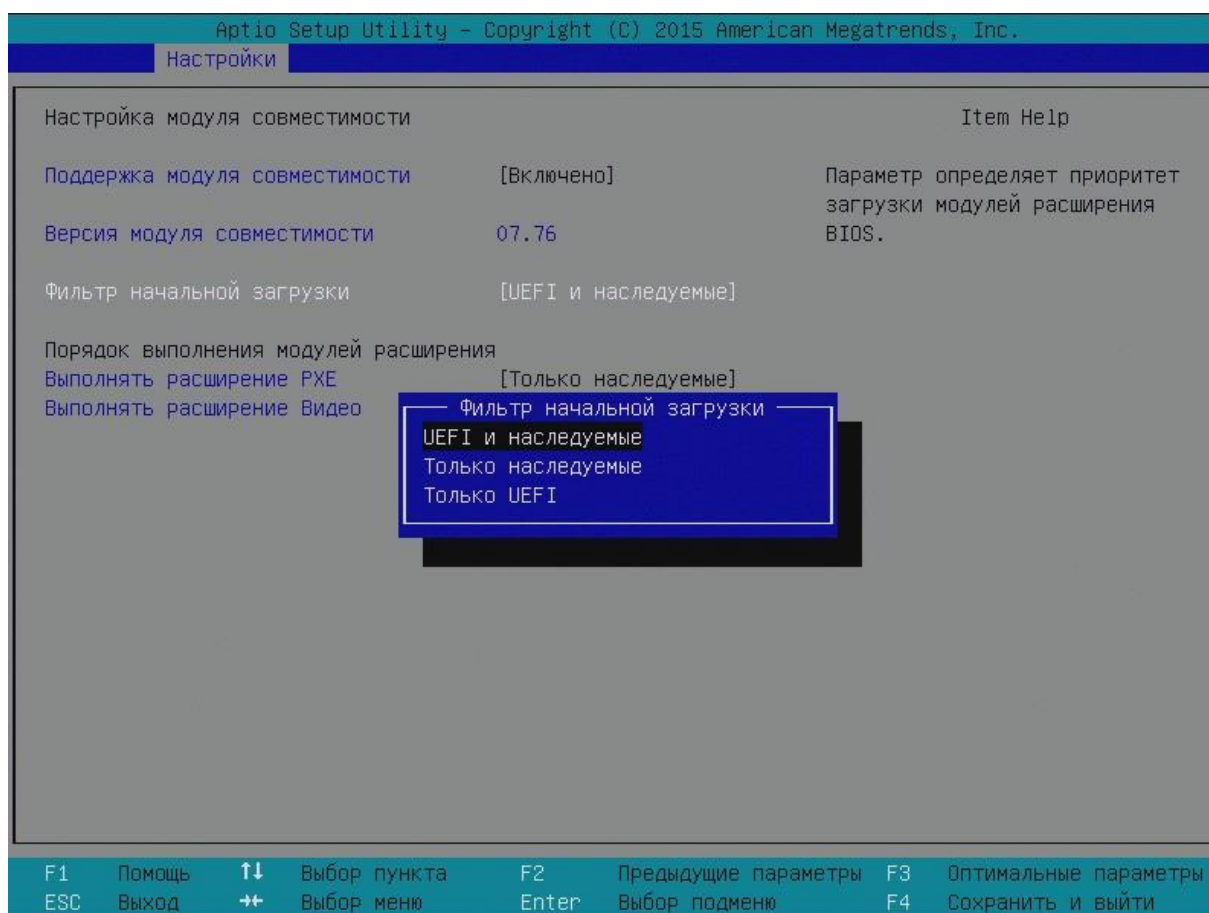


Рис. 3.7

Включение режима UEFI в BIOS следует производить каждый раз при необходимости. Для использования режима по умолчанию при настройках параметров BIOS следует в пункте меню *Загрузка* загрузку UEFI OS сделать первым приоритетом (рис.3.8).

Примечание. Загрузочный образ ПО KTL содержит оба режима загрузки - UEFI BIOS и традиционный BIOS (Legacy BIOS).

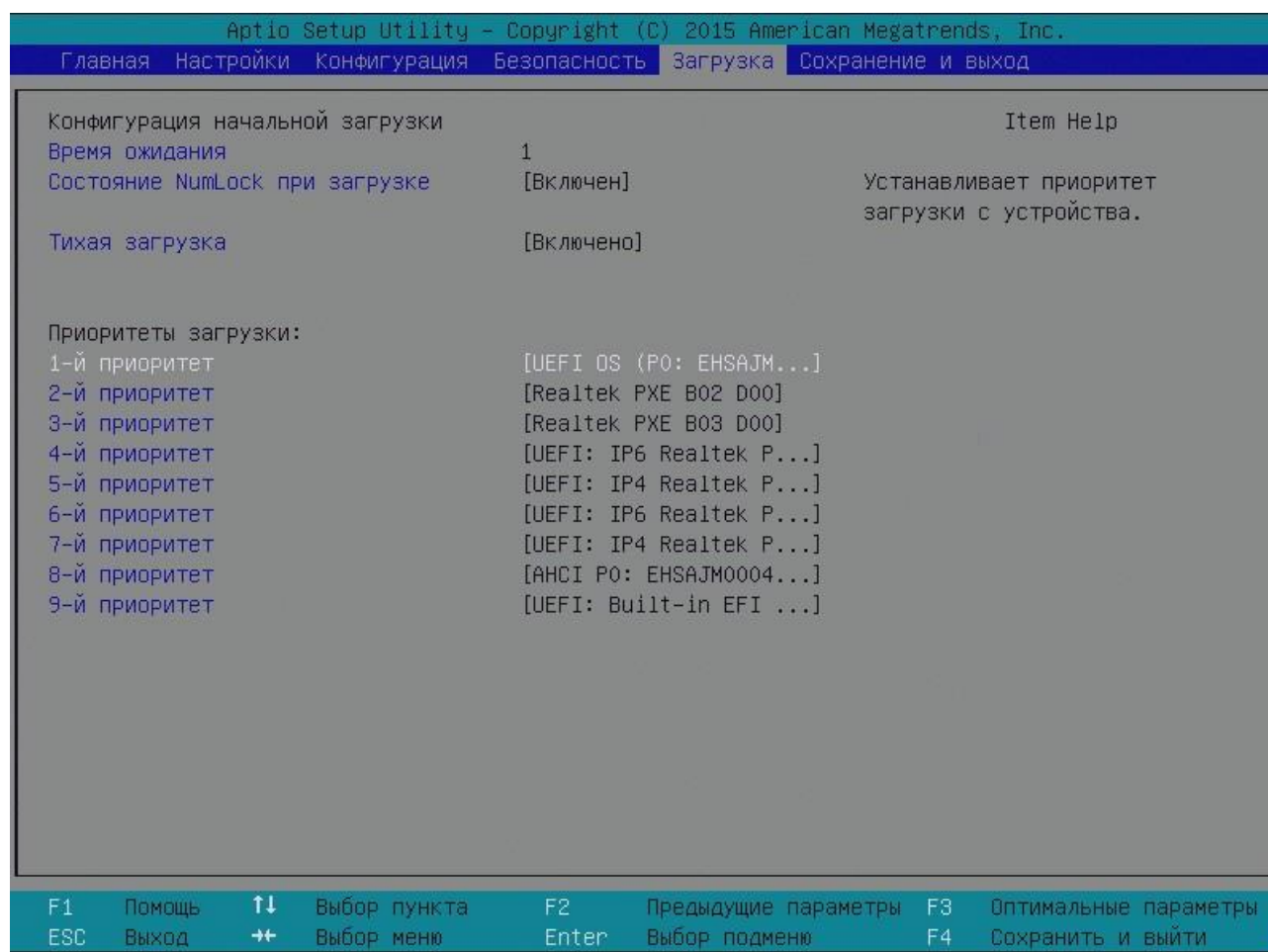


Рис. 3.8

### 3.2.2. Вход в режиме администратора

При загрузке ПО в режиме UEFI может возникнуть необходимость входа в режиме администратора. Для этого, после выполнения настройки параметров загрузки (выполнения действий 1-3 пункта 3.2.1), во время дальнейшей загрузки при появлении заставки Kraftway следует:

- 1) →[Esc], появится меню выбора режима загрузки (рис. 3.9);
- 2) выбрать из списка пункт *CTL-safe*;
- 3) →[Enter].



Рис. 3.9

### 3.2.3. Проверка подписи KTL

Загрузка ПО KTL (версий 4.7 и выше) в режиме UEFI снабжена дополнительной функцией в системе безопасности - проверкой подлинности подписи KTL. Пользователям более ранних версий для активации проверки следует обновить ПО через web или установить нужную версию ПО с USB-flash. Проверка подписи проходит автоматически при загрузке ОС. Если проверка успешна на экран выводится соответствующее сообщение (рис.3.10), терминальная станция загружается. Если проверка не пройдена, на экран выводится сообщение об ошибке (рис. 3.11), загрузка ПО прерывается, терминальная станция выключается.



```
Kraftway Terminal Linux
Подготовка к запуску KTL, ждите
Проверка ядра KTL
Ядро KTL соответствует подписи
Проверка основного образа KTL
Основной образ KTL соответствует подписи
—
```



Рис. 3.10

```
Kraftway Terminal Linux
Подготовка к запуску KTL, ждите
Проверка ядра KTL
Ядро KTL соответствует подписи
Проверка основного образа KTL
error: bad signature.
Ошибка!Основной образ KTL не соответствует подписи
—
```



Рис. 3.11



### 3.3. Загрузка терминальной станции по PXE

Пользователю ПО KTL (версий 4.5 и выше) предоставляется возможность загрузки и работы терминальной станции в PXE режиме (Preboot eXecution Environment). PXE - среда для загрузки компьютера с помощью сетевой карты без использования локальных носителей данных (жёсткого диска, USB-накопителя и т.п.). Режим удобен для загрузки и работы по сети бездисковых терминальных станций.

#### 3.3.1. Настройка параметров загрузки

Для загрузки ПО терминальной станции в PXE-режиме администратору следует настроить PXE сервер и активировать загрузку этого режима в BIOS терминальной станции.

##### 3.3.1.1. Настройка PXE сервера

Требования и рекомендации по настройке PXE сервера:

Требования к DHCP:

- 1) в 066 опции (Boot Server Host name) внести IP адрес PXE сервера (например 192.168.0.1);
- 2) в опции 067 (Boot File name) внести имя загрузочного файла: *pxelinux.0*.

Требования к TFTP:

- 1) в корневую папку TFTP скопировать содержимое каталога, расположенного по адресу *ftp.kraftway.ru/pxe/*
- 2) содержимое установочной флешки скопировать в подкаталоги:
  - в корневой TFTP - для бездискового режима;
  - в *upgrade* - для установки по PXE.
- 3) Настроить опции ядра в конфигурационном файле загрузчика *pxelinux.cfg/default*:
  - в опции *tftp=*IP-адрес сервера внести IP-адрес TFTP сервера (например *tftp=192.168.0.1*);

– в опции `bsize= blocksize` рекомендуется внести 8192 (`bsize=8192`, подбирать для своей сети);

– опция `trueftp` - рекомендуется использование FTP.

Требования к FTP-серверу:

- 1) анонимный;
- 2) обслуживает корневой каталог TFTP-сервера.

Настройки терминальных станций по умолчанию:

Корневой каталог *TFTP/settings.txt*

#### 3.3.1.2. Настройка терминальной станции

Для выполнения данной настройки при загрузке терминальной станции следует:

- 1) вход в BIOS → *Сохранение и выход*;
- 2) в настройках параметра *Произвести загрузку с* выбрать из списка загрузок пункт *Realtek PXE* требуемого сетевого устройства (рис. 3.12);
- 3) →[Enter], в появившемся списке выбрать требуемый параметр загрузки (рис. 3.13);
- 4) →[Enter].

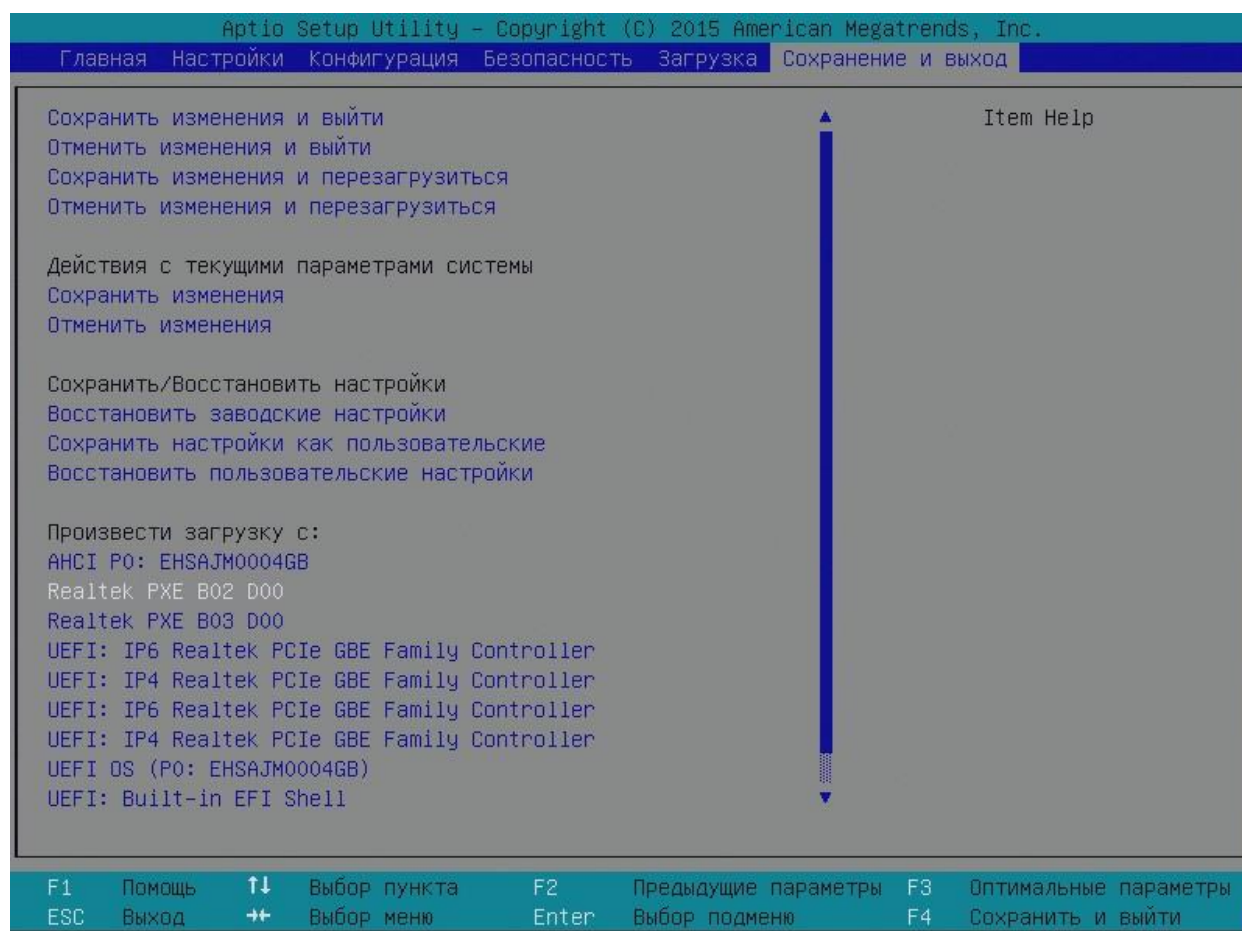


Рис. 3.12

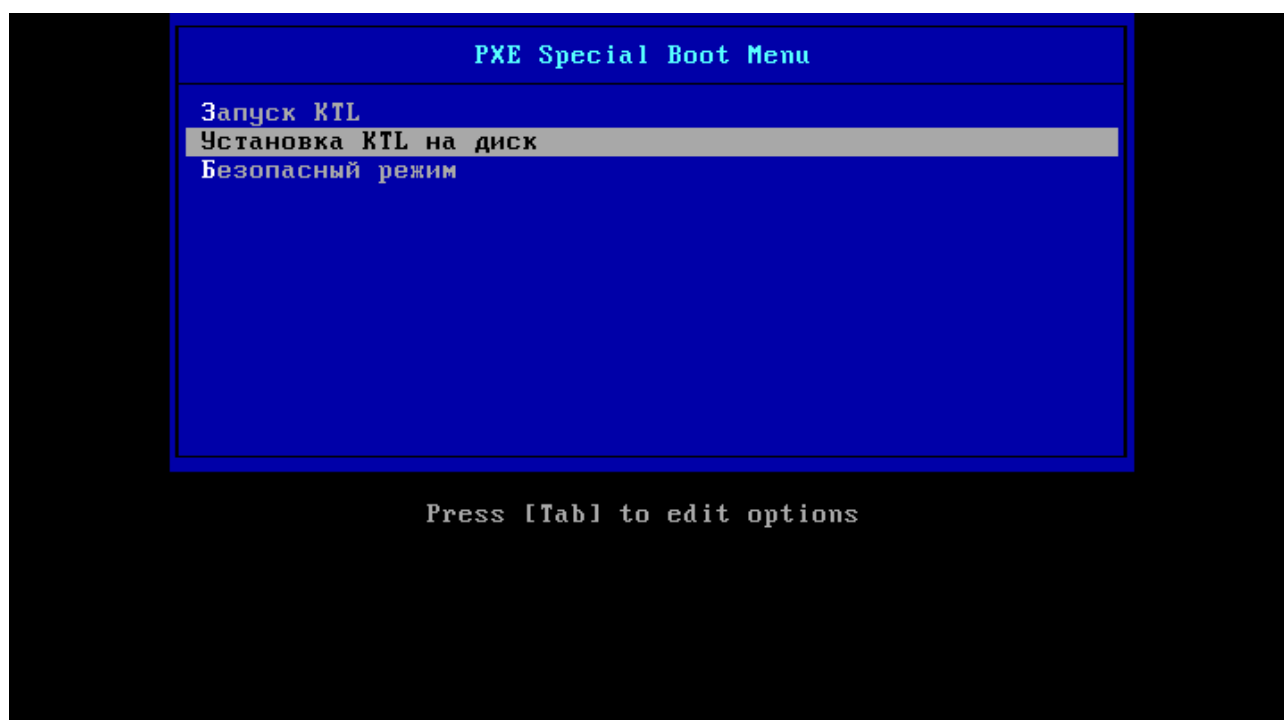


Рис. 3.13

Настройки терминальной станции при загрузке по PXE сохраняются на сервере при завершении работы в файле вида */корневой каталог TFTP/settings/MAC-адрес терминальной станции* и скачиваются при последующих стартах KTL.

Если настройки по каким-либо причинам не сохранились, то используются настройки по умолчанию, содержащиеся в *файле settings.txt*.

### 3.3.2. Вход в режиме администратора

При загрузке ПО в режиме PXE может возникнуть необходимость входа в режиме администратора. Для этого следует при настройке параметров загрузки по PXE (см. пункт 3.3.1.2) при выполнении действия 3 в появившемся списке выбирать параметр *Безопасный режим* (см. рис.3.13).

## 4. НАСТРОЙКА ПО «KTL»

### 4.1. Описание рабочего стола

Рабочий стол состоит из панели задач, системного меню и рабочего пространства (рис.4.1)

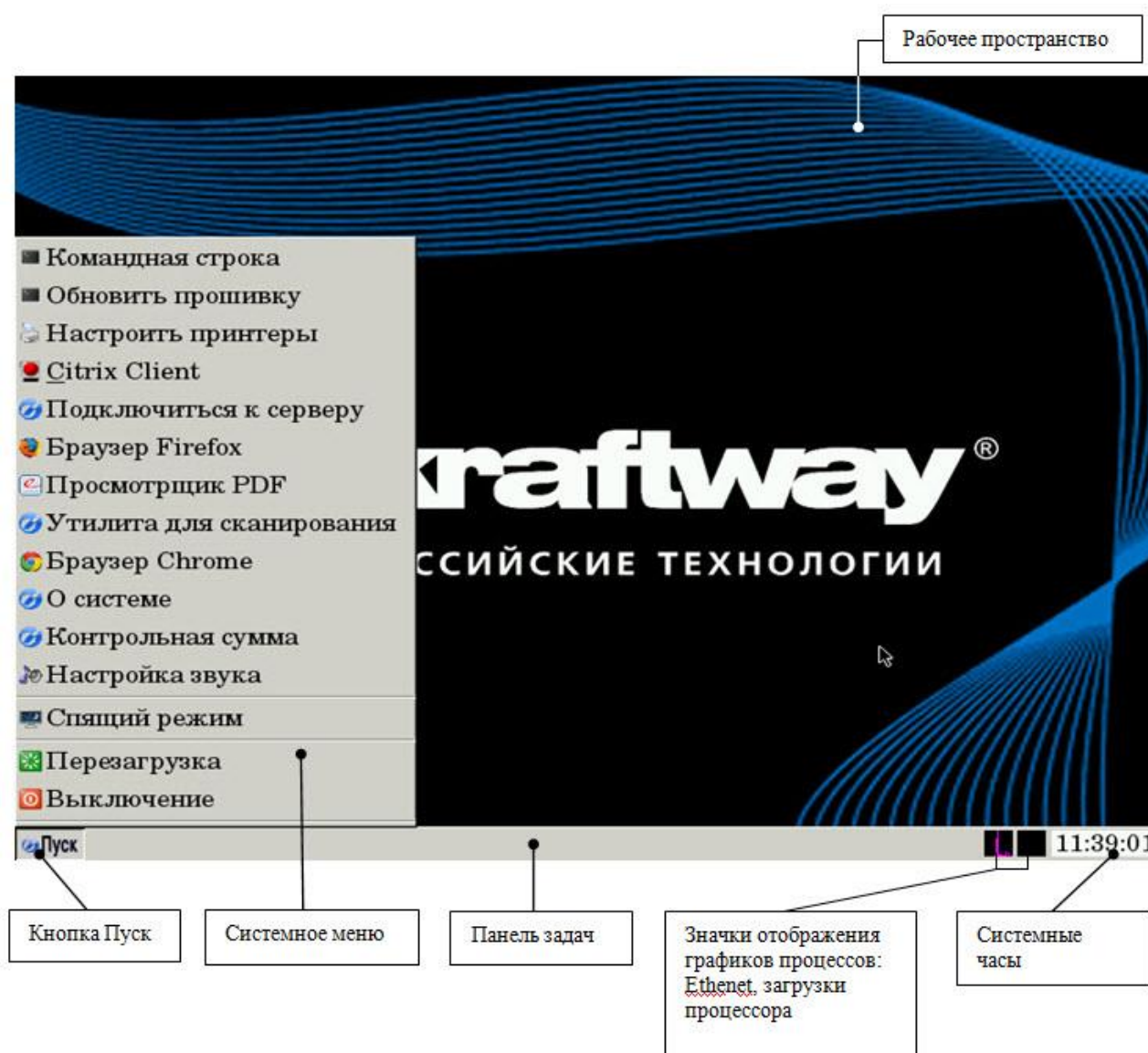


Рис. 4.1

На панели задач отображаются: кнопка «Пуск», значки отображения графиков процессов и часы. Кнопка «Пуск» предназначена для вызова системного меню. Свободное пространство панели задач предназначено для отображения кнопок запущенных программ и открытых терминальных сессий.

Системное меню вызывается путем нажатия кнопки «Пуск» на панели задач. Перемещение по меню и активация его пунктов выполняются с помощью мыши или курсорных клавиш на клавиатуре. Для выбора и активации требуемого пункта меню необходимо привести курсор мыши на этот пункт, при этом пункт выделяется цветом, и нажать левую кнопку мыши или клавишу [Enter] на клавиатуре.

Системное меню представлено в виде списка пунктов. Вид системного меню приведён на рис. 4.2

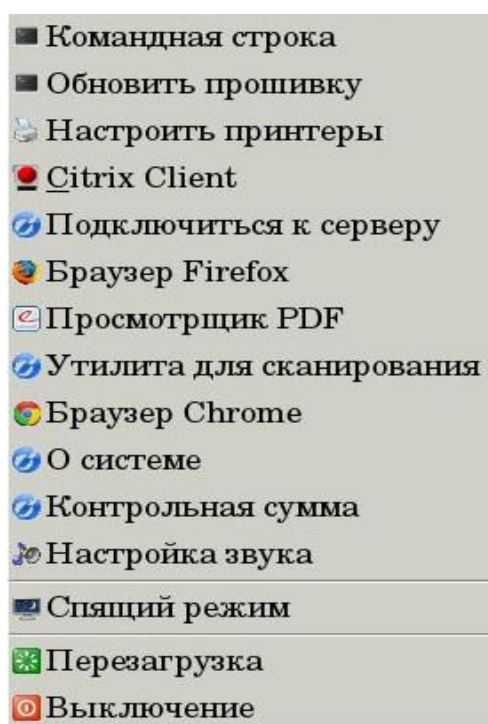


Рис. 4.2

Рабочий стол пользователя и его элементы при загрузке ОС терминальной станции в нормальном и безопасном режиме почти идентичны. После загрузки ОС терминальной станции в безопасном режиме в системном меню рабочего стола пользователя выводятся пункты: *Командная строка* - для выполнения стандартных команд ОС Linux, *Обновить прошивку* - для обновления ПО терминальной станции, *Настроить принтеры* - для выполнения установки, настройки и удаления печатающих устройств, *Citrix Client* - для настройки доступа к определённым программам, установленным на Windows-сервере, *Подключиться к серверу* - для запуска пользовательских сессий, *Браузер Firefox* и *Браузер Chrome* - для запуска web-браузера Интернет (Mozilla Firefox или Google Chrome) с последующим открытием в нём сетевых

ресурсов, *Просмотрщик PDF* - для просмотра и настройки документов формата PDF, *Утилита для сканирования* - для сканирования документов, *О системе* - для вывода информации об используемом ПО, *Контрольная сумма* - для вывода информационного окна, выводящего контрольную сумму ОС, *Настройка звука* - для настройки звуковой карты, *Спящий режим*, *Перезагрузка*, *Выключение* - для перезагрузки, выключения и ввода терминальной станции в спящий режим.

#### 4.2. Настройка клиентского окружения терминальной станции с помощью консоли администратора

Настройка клиентского окружения терминальной станции с помощью консоли администратора выполняется:

- локально (на самой настраиваемой терминальной станции при загрузке ОС в безопасном режиме);
- удалённо (на компьютере, подключённом к сети терминальных станций).

Консоль администратора обладает web-интерфейсом, который практически идентичен для этих двух способов настройки. Локальная и удаленная настройка клиентского окружения терминальной станции выполняется с помощью браузера, который поддерживает язык разметки масштабируемой векторной графики SVG, например, Mozilla FireFox.

##### 4.2.1. Локальный вход в консоль администратора

Для выполнения локальной настройки клиентского окружения терминальной станции следует:

- 1) →[Пуск] на панели задач;
- 2) выбрать пункт *Браузер FireFox* в появившемся системном меню, на экран выводится окно *Требуется аутентификация* для ввода имени и пароля администратора (рис. 4.3);



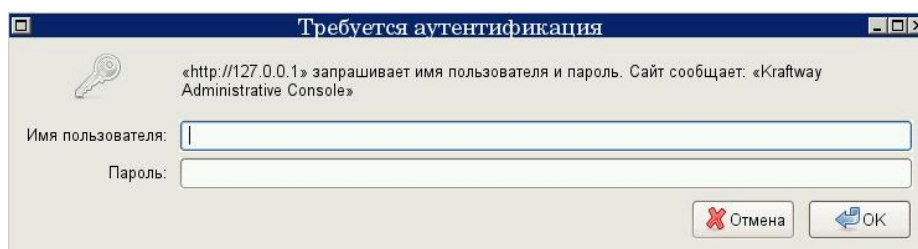


Рис. 4.3

3) ввести имя и пароль администратора в соответствующие поля (имя администратора - admin, пароль администратора - admin. Данные значения определены значениями по умолчанию);

4) →[OK], после выполнения данного действия, во вкладке web-браузера Система - Административная консоль, открывается начальная страница консоли администратора (вкладка Система пункта меню Информация (рис. 4.4)).

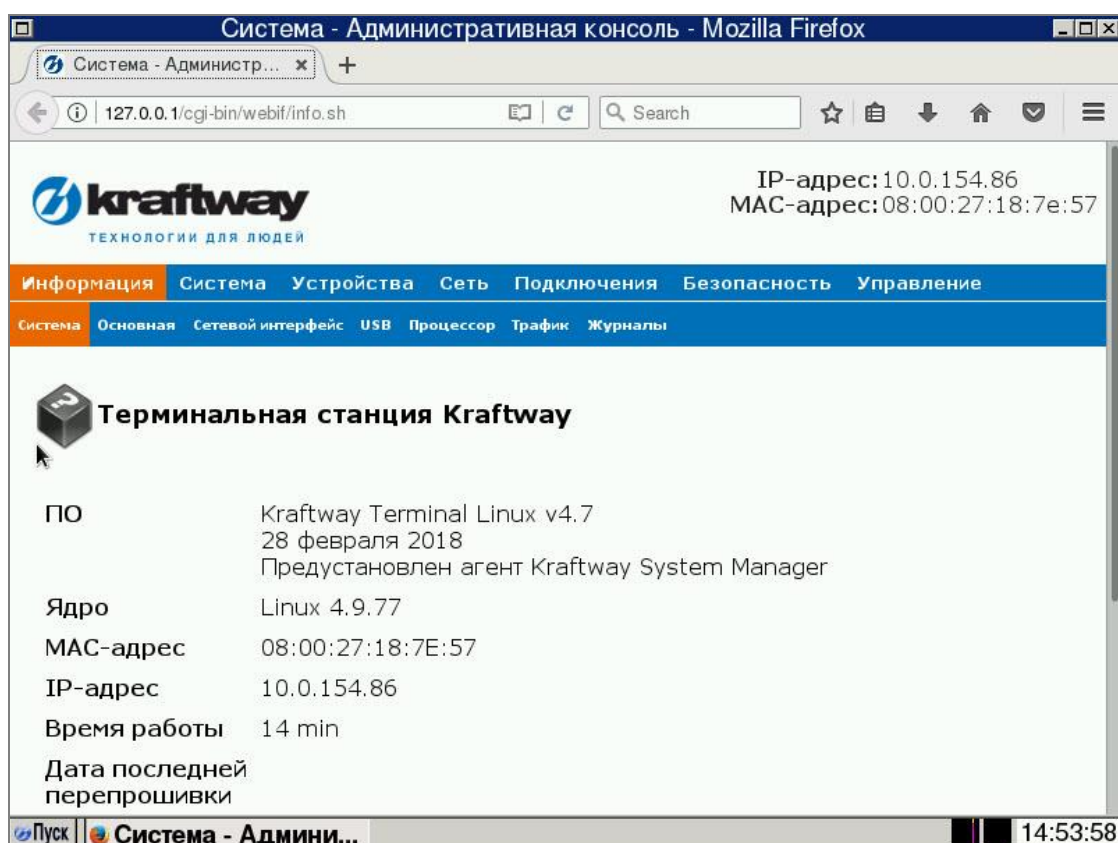


Рис. 4.4




Примечание. Также для входа в консоль администратора в адресной строке web-браузера можно ввести IP-адрес 127.0.0.1 специального сетевого интерфейса внутренней петли («loopback») сетевого протокола TCP/IP.

#### 4.2.2. Удалённый вход в консоль администратора

Для выполнения удалённой настройки клиентского окружения терминальной станции следует:

- 1) запустить web-браузер Mozilla FireFox на удалённом компьютере, подключённом к сети терминальных станций;
- 2) ввести IP-адрес настраиваемой терминальной станции в адресной строке web-браузера, например: 10.0.150.7, после чего на экран будет выведено окно для ввода имени и пароля администратора (см.рис.4.3);
- 3) ввести имя и пароль администратора в соответствующие поля (имя администратора - admin, пароль администратора - admin. Данные значения определены значениями по умолчанию);
- 4) →[ОК], после выполнения данного действия, во вкладке web-браузера *Система - Административная консоль*, открывается начальная страница консоли администратора (вкладка *Система* пункта меню *Информация* (рис. 4.5));




ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ

IP-адрес: 10.0.154.86  
MAC-адрес: 08:00:27:18:7e:57

Информация Система Устройства Сеть Подключения Безопасность Управление

Система Основная Сетевой интерфейс USB Процессор Трафик Журналы

 **Терминальная станция Kraftway**

**ПО** Kraftway Terminal Linux v4.7  
28 февраля 2018  
Предустановлен агент Kraftway System Manager

**Ядро** Linux 4.9.77

**MAC-адрес** 08:00:27:18:7E:57

**IP-адрес** 10.0.154.86

**Время работы** 23 min

**Дата последней перепрошивки**

**Поддержка** +7 (495) 969-2400 для московских пользователей  
+7 (800) 200-0355 для клиентов из регионов  
[On-line запрос](#)

Выйти

Рис. 4.5

#### 4.2.3. Описание меню консоли администратора

Основные пункты меню консоли администратора (см. рис.4.5):

- *Информация*;
- *Система*;
- *Устройства*;
- *Сеть*;
- *Подключения*;
- *Безопасность*;
- *Управление*.

Далее по тексту рассматривается каждый из приведённых выше пунктов меню консоли администратора. Каждый пункт меню содержит определённое количество вкладок. Вкладки разделяются на информационные и вкладки настроек. На информационных вкладках приводятся сведения по интересующим темам, а вкладки настроек содержат определённые параметры для изменения или выбора их значений.

Примечание. Следует помнить, что для сохранения изменений, сделанных на вкладках настроек, необходимо нажать на кнопку [Сохранить изменения], расположенную в правом нижнем углу вкладки настроек, а для того, чтобы данные изменения вступили в силу терминальную станцию необходимо перезагрузить. Перезагрузку терминальной станции можно выполнить любым из следующих способов:

- из консоли администратора локально или удалённо (см. п. 4.2.10.1);
- из системного меню рабочего стола пользователя (см. п. 4.1, рис.4.2);
- при нажатии кнопки Power, если режим работы кнопки Power установлен в значение «Выключение» (см. п. 4.2.6.1).

#### 4.2.4. Пункт меню Информация

Пункт меню *Информация* содержит семь вкладок: *Система*, *Основная*, *Сетевой интерфейс*, *USB*, *Процессор*, *Трафик*, *Журналы*.

#### 4.2.4.1. Вкладка Система

Для перехода на вкладку *Система* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *Система*. На вкладке *Система* содержится информация: название ПО, версии ПО, дата разработки ПО, ядро ОС «Kraftway Terminal Linux», MAC-адрес сетевого контроллера, IP-адрес терминальной станции, продолжительность работы терминальной станции, дата последней прошивки, контактная информация Единого центра поддержки пользователей (см. рис. 4.5).

Примечание. Вывести информацию о системе возможно через системное меню (пункт *О системе*)

#### 4.2.4.2. Вкладка Основная

Для перехода на вкладку *Основная* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *Основная*. На вкладке *Основная* содержится информация: об использовании оперативной памяти (использованной и свободной), использовании файлового пространства на накопителях, подключенных к терминальной станции (рис. 4.6).

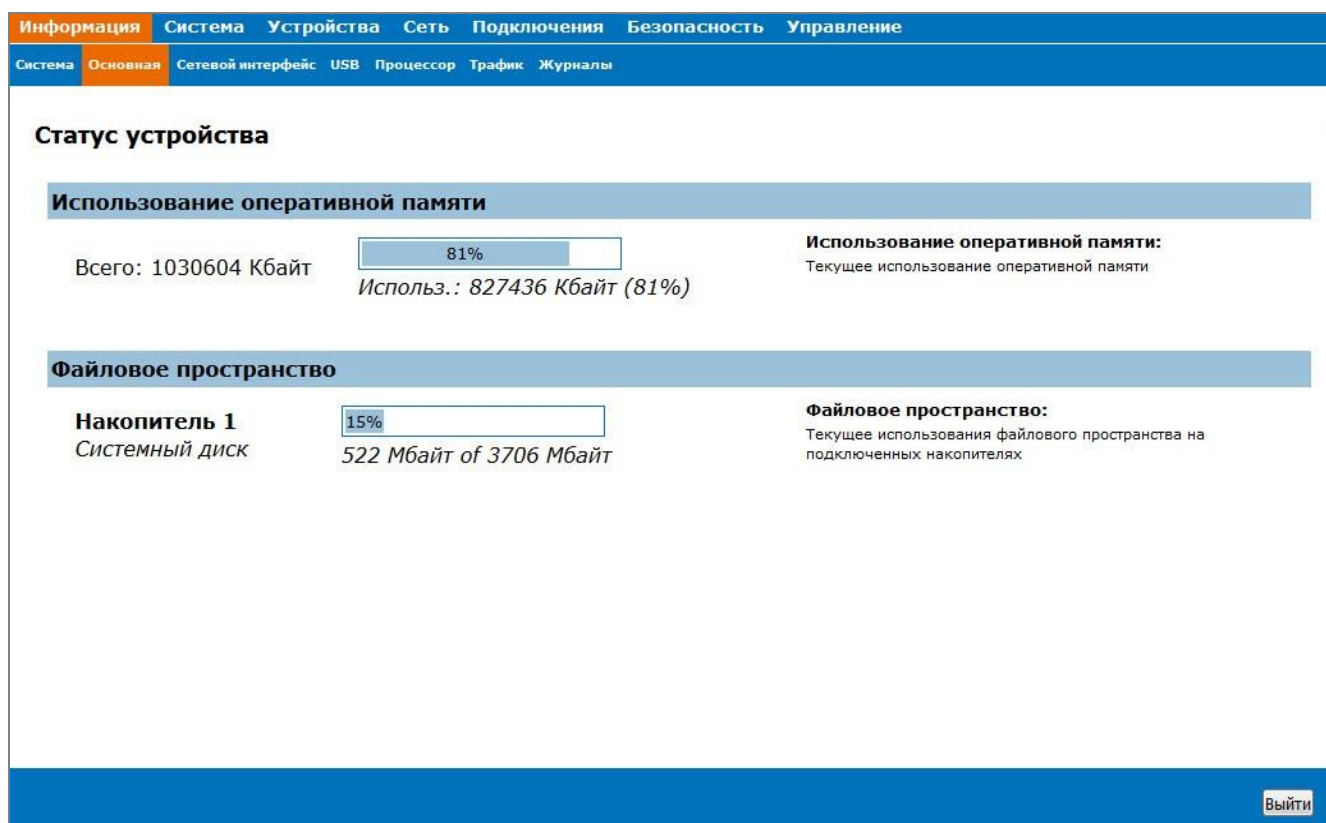


Рис. 4.6

#### 4.2.4.3. Вкладка Сетевой интерфейс

Для перехода на вкладку *Сетевой интерфейс* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *Сетевой интерфейс*. На вкладке *Сетевой интерфейс* содержится информация о виртуальных сетевых интерфейсах (*eth0*, *eth1* и *bond0* и т.п.): MAC-адресе сетевого контроллера, IP-адресе терминальной станции, количестве принятых и отправленных данных в байтах (рис. 4.7).

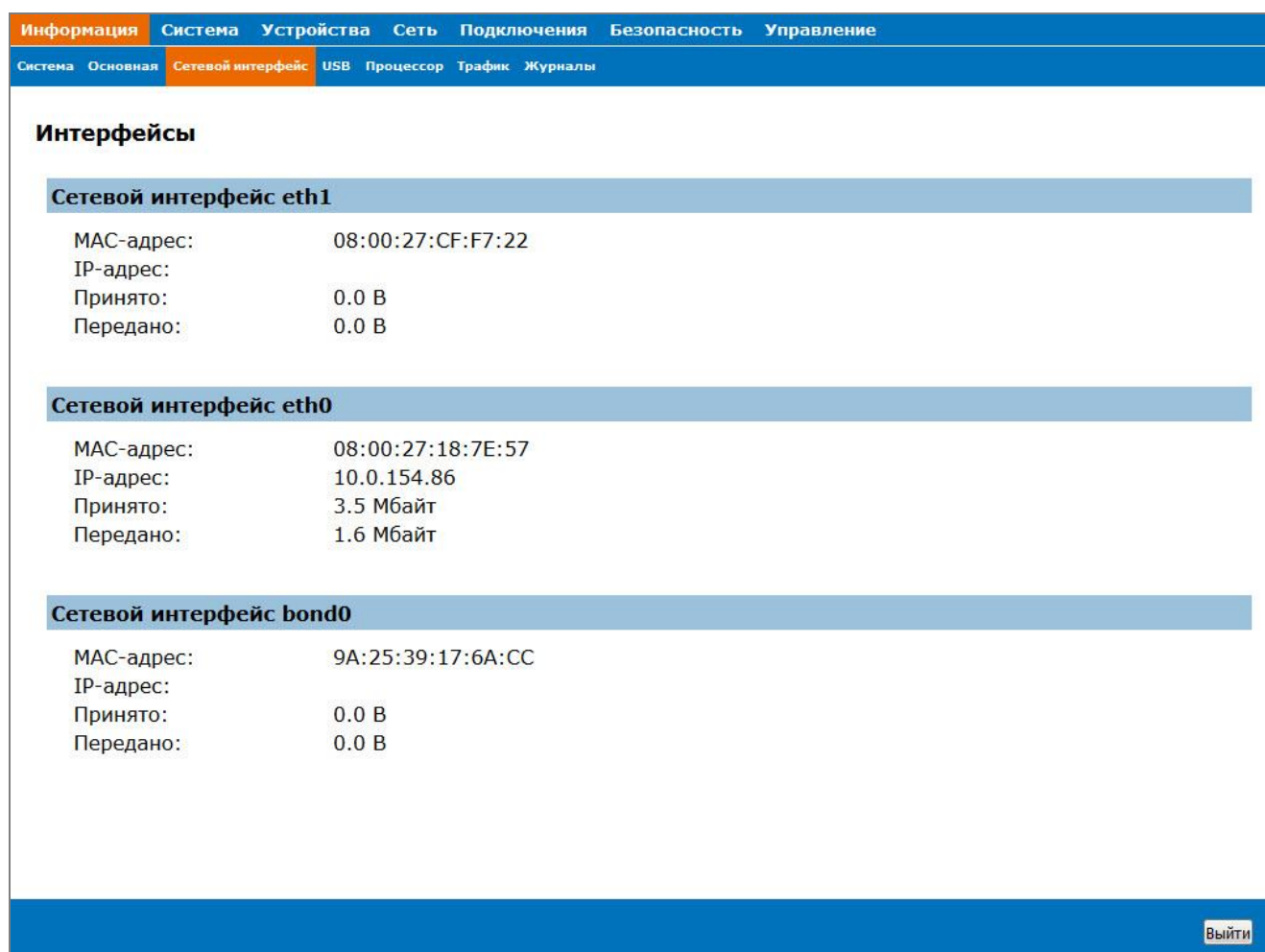


Рис. 4.7

#### 4.2.4.4. Вкладка USB

Для перехода на вкладку *USB* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *USB*. На вкладке *USB* содержится информация обо всех подключённых USB-устройствах, в соответствующих графах приводятся сведения: шине, номере подключённого устройства, типе устройства, изготовителе, идентификаторе изготовителя, идентификаторе устройства, версии USB-интерфейса (рис. 4.8).

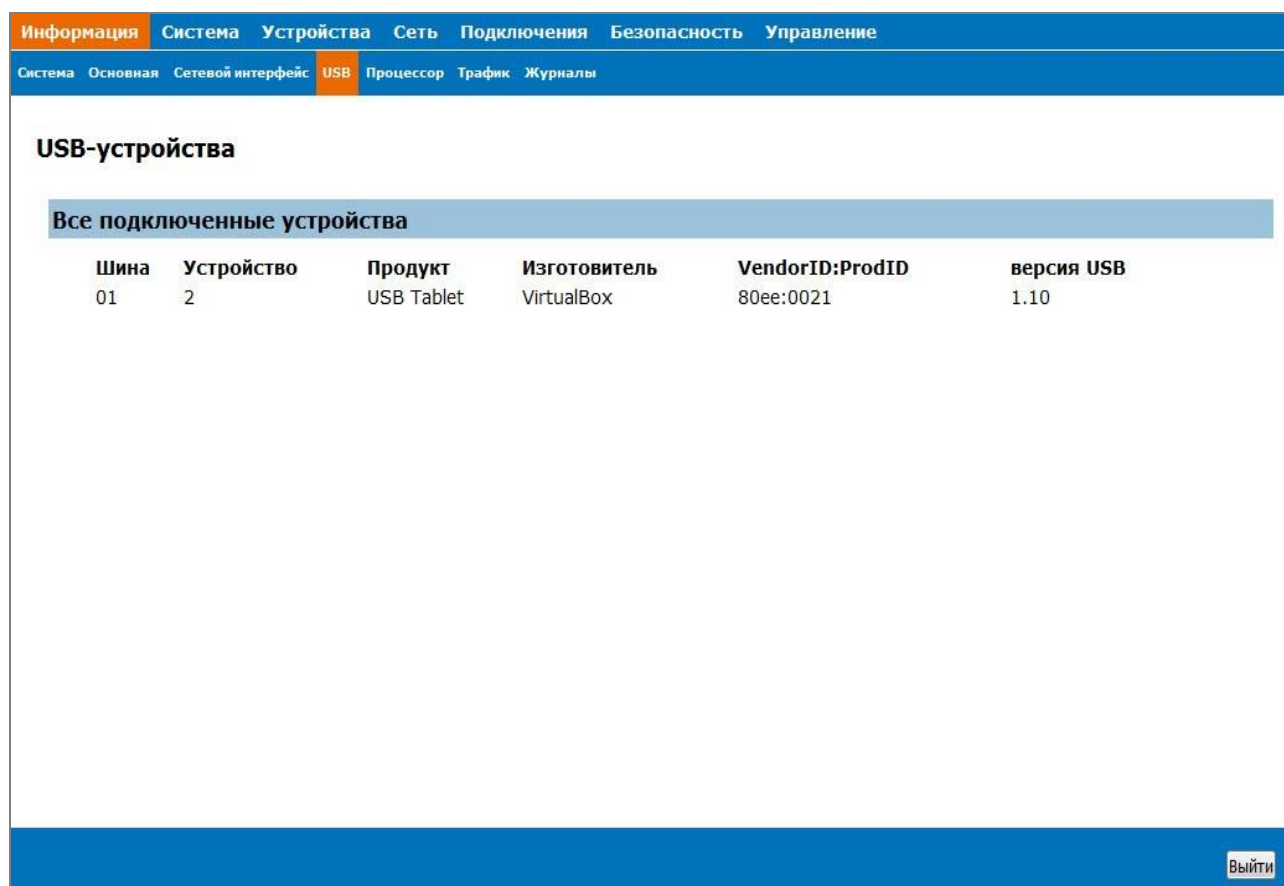


Рис. 4.8

#### 4.2.4.5. Вкладка Процессор

Для перехода на вкладку *Процессор* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *Процессор*. На вкладке *Процессор* выводится график загрузки процессора терминальной станции (рис. 4.9).

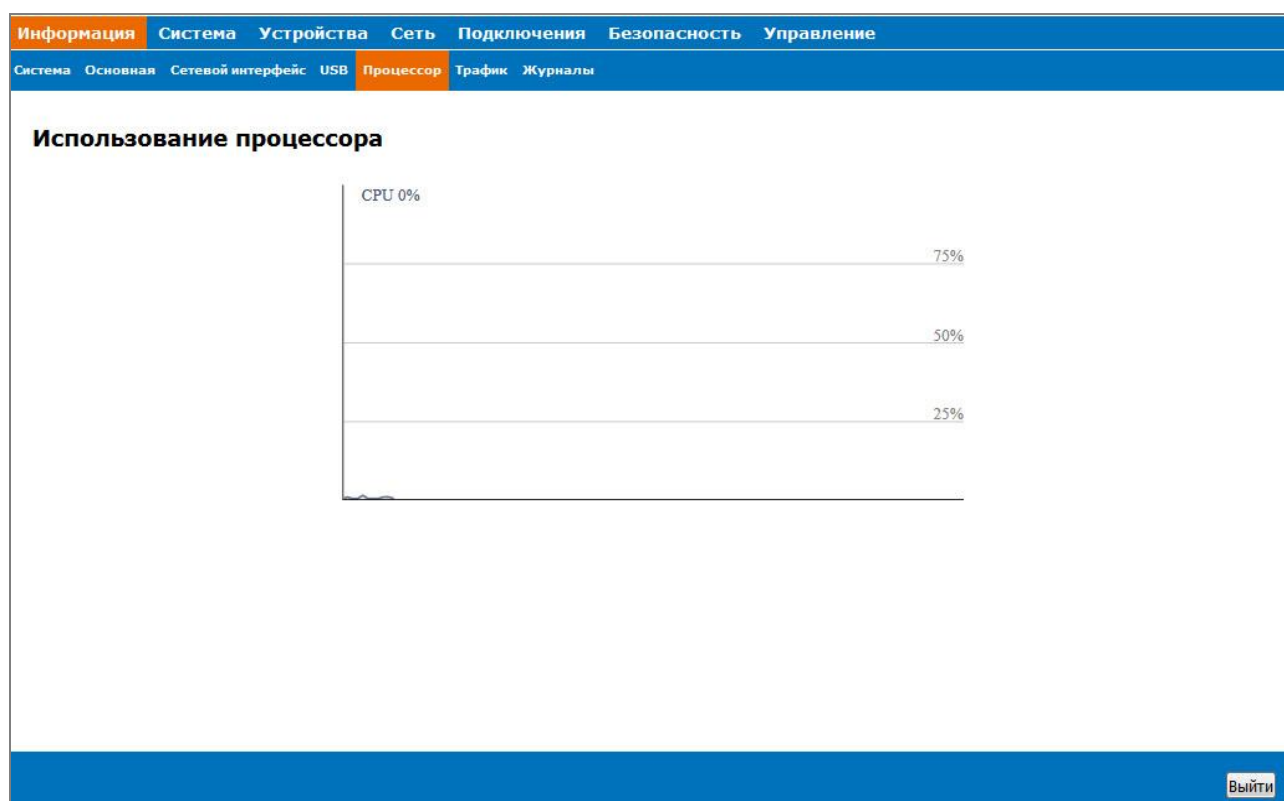


Рис. 4.9

#### 4.2.4.6. Вкладка Трафик

Для перехода на вкладку *Трафик* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *Трафик*. На вкладке *Трафик* выводятся графики производительности сети сетевых интерфейсов терминальной станции (рис. 4.10).



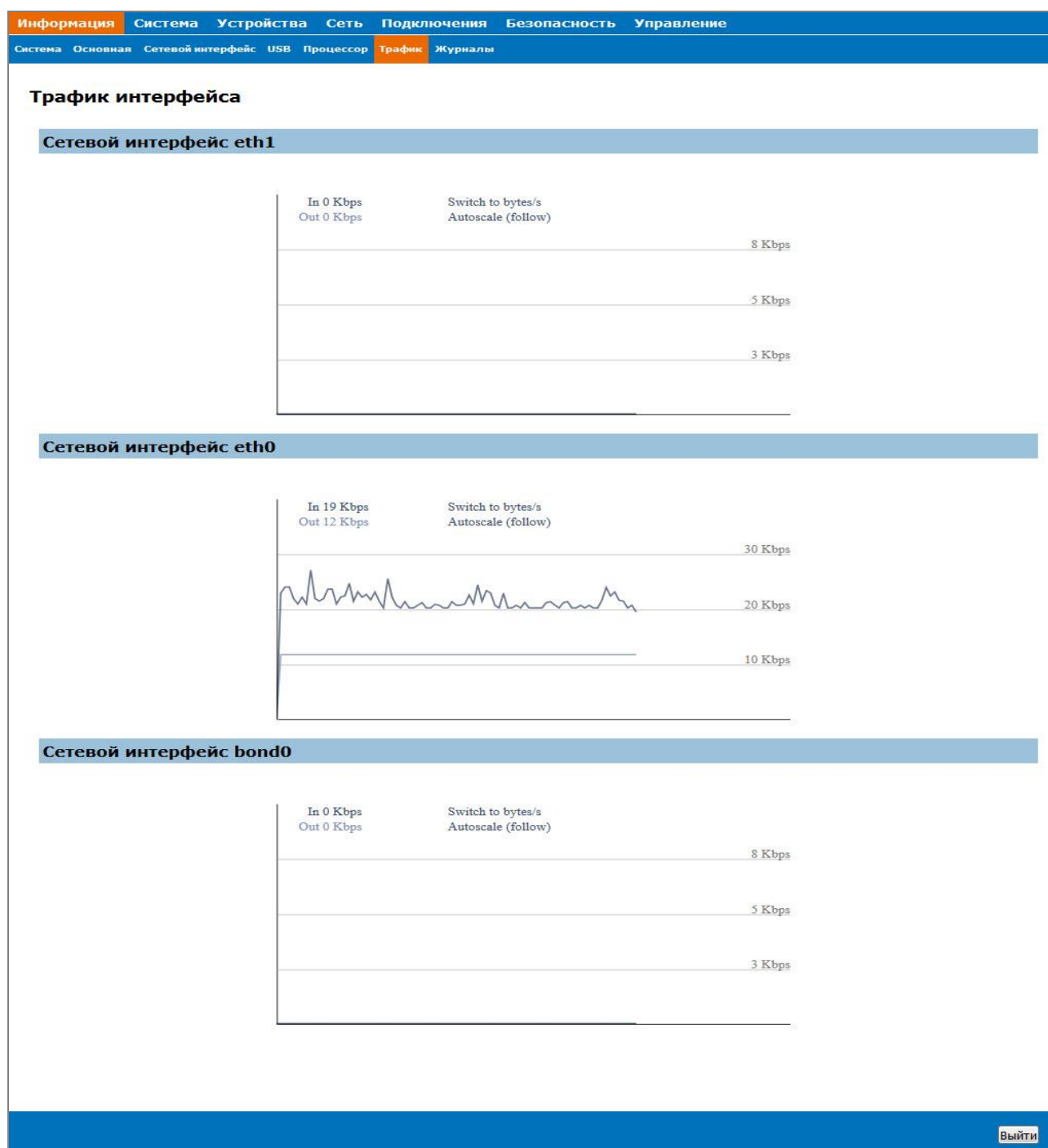


Рис. 4.10

#### 4.2.4.7. Вкладка Журналы

Для перехода на вкладку *Журналы* следует выполнить следующую последовательность действий: → пункт *Информация* → вкладка *Журналы*. На вкладке *Журналы* расположены три функциональные кнопки [Показать usermessages], [Показать лог auditd] и [Показать лог KUEFI]. Кнопка [Показать usermessages] предназначена для

вывода журналов системных процессов, авторизации, монтирования устройств, работы системы печати CUPS. Кнопка [Показать лог auditd] предназначена для вывода журналов работы приложений ОС, сетевых соединений, открытия файлов. Кнопка [Показать лог KUEFI] предназначена для вывода журнала работы антивируса Kaspersky for UEFI. Вкладка *Журналы* представлена на рис. 4.11.

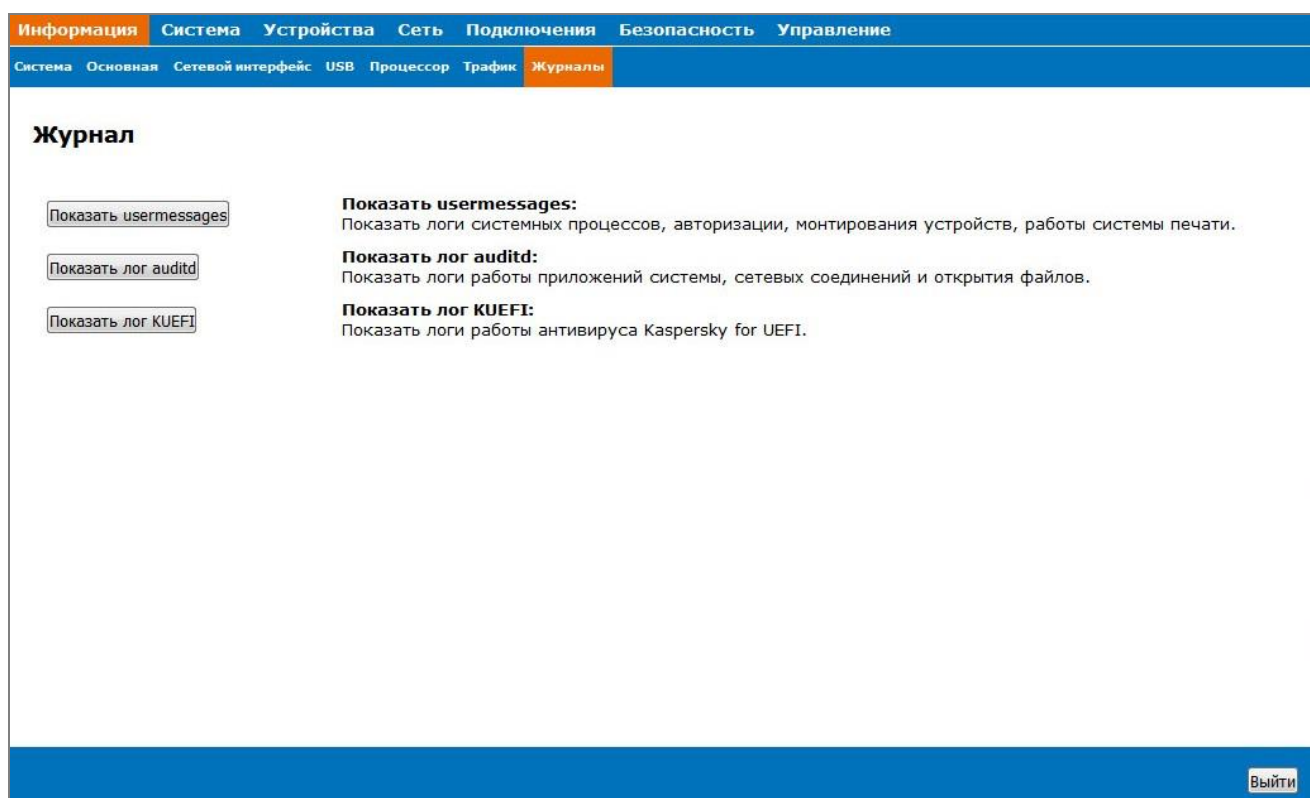


Рис. 4.11

Для вывода журналов системных процессов, авторизации, монтирования устройств, работы системы печати следует нажать на кнопку [Показать usermessages].

Для вывода журналов работы приложений системы, сетевых соединений и открытия файлов следует нажать на кнопку [Показать лог auditd].

Для вывода журнала работы антивируса Kaspersky for UEFI следует нажать на кнопку [Показать лог KUEFI].

**ВНИМАНИЕ:** ЖУРНАЛЫ СОЗДАЮТСЯ ТОЛЬКО ЕСЛИ ВЫБРАН ПАРАМЕТР ЗАПИСЫВАТЬ СОБЫТИЯ В ЖУРНАЛ РАЗДЕЛА ПАРАМЕТРОВ ЖУРНАЛИРОВАНИЕ НА ВКЛАДКЕ ПРИЛОЖЕНИЯ ПУНКТА МЕНЮ СИСТЕМА (см. п. 4.2.5.2, рисунок 4.15).

#### 4.2.5. Пункт меню Система

Пункт меню *Система* содержит 7 вкладок: *Время*, *Приложения*, *Пароль*, *VNC*, *Обновить*, *Автообновление*, *Сертификаты*.

##### 4.2.5.1. Вкладка Время

Для перехода на вкладку *Время* следует выполнить следующую последовательность действий: →пункт *Система* →вкладка *Время*. На вкладке *Время* содержатся параметры настройки времени и даты (рис. 4.12, рис. 4.13). Ниже приводится описание данных параметров.

Информация Система Устройства Сеть Подключения Безопасность Управление

Время Приложения Пароль VNC Обновить Автообновление Сертификаты

### Установка времени и даты

**Установка времени и даты**

Часовой пояс: Москва (UTC+3)

Синхронизировать дату и время по сети: ☐

**Синхронизация даты и времени:**  
Дата и время могут быть установлены с помощью протокола синхронизации времени (Network Time Protocol, NTP). NTP-сервер может быть расположен локально или в сети Интернет. Для применения данных настроек перезагрузка терминальной станции не нужна.

**Параметры**

Год: 2018  
Месяц: Март  
День: 21  
Час: 13  
Минуты: 40

Сохранить изменения Выйти

Рис. 4.12

Описание параметров:

Выбор часового пояса, времени и даты: осуществляется вручную (установлено по умолчанию), либо с помощью синхронизации даты и времени по сети с помощью протокола NTP (рис. 4.13). Network Time Protocol - сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Информация Система Устройства Сеть Подключения Безопасность Управление

Время Приложения Пароль VNC Обновить Автообновление Сертификаты

### Установка времени и даты

#### Установка времени и даты

Часовой пояс: Москва (UTC+3)

Синхронизировать дату и время по сети: ☒

**Синхронизация даты и времени:**  
Дата и время могут быть установлены с помощью протокола синхронизации времени (Network Time Protocol, NTP). NTP-сервер может быть расположен локально или в сети Интернет. Для применения данных настроек перезагрузка терминальной станции не нужна.

#### Параметры

Адрес NTP-сервера: ntp1.vniiftri.ru

Сохранить изменения Выйти

Рис. 4.13

*Адрес NTP-сервера* - для ввода адреса локального или удалённого NTP-сервера (значение «pool.ntp.org» установлено по умолчанию).

*Часовой пояс* - для выбора соответствующего часового пояса.

*Год, Месяц, День, Час, Минуты* - для выбора текущих значений даты и времени.

Для выполнения настройки на вкладке *Время* следует:

- 1) → Система → Время,
- 2) внести необходимые изменения в параметры настроек,
- 3) → [Сохранить изменения].

#### 4.2.5.2. Вкладка Приложения

На вкладке *Приложения* содержатся параметры: настройки выбора приложений, доступных пользователю в меню «Пуск», автозапуска приложений, настройка сохранения профиля браузеров Firefox и Chrome, установки разрешения непроверенных соединений, использования NLA, записи событий в журнал, отключения переключения раскладки в локальной системе (рис. 4.14 и рис. 4.15). Ниже приводится описание данных параметров.

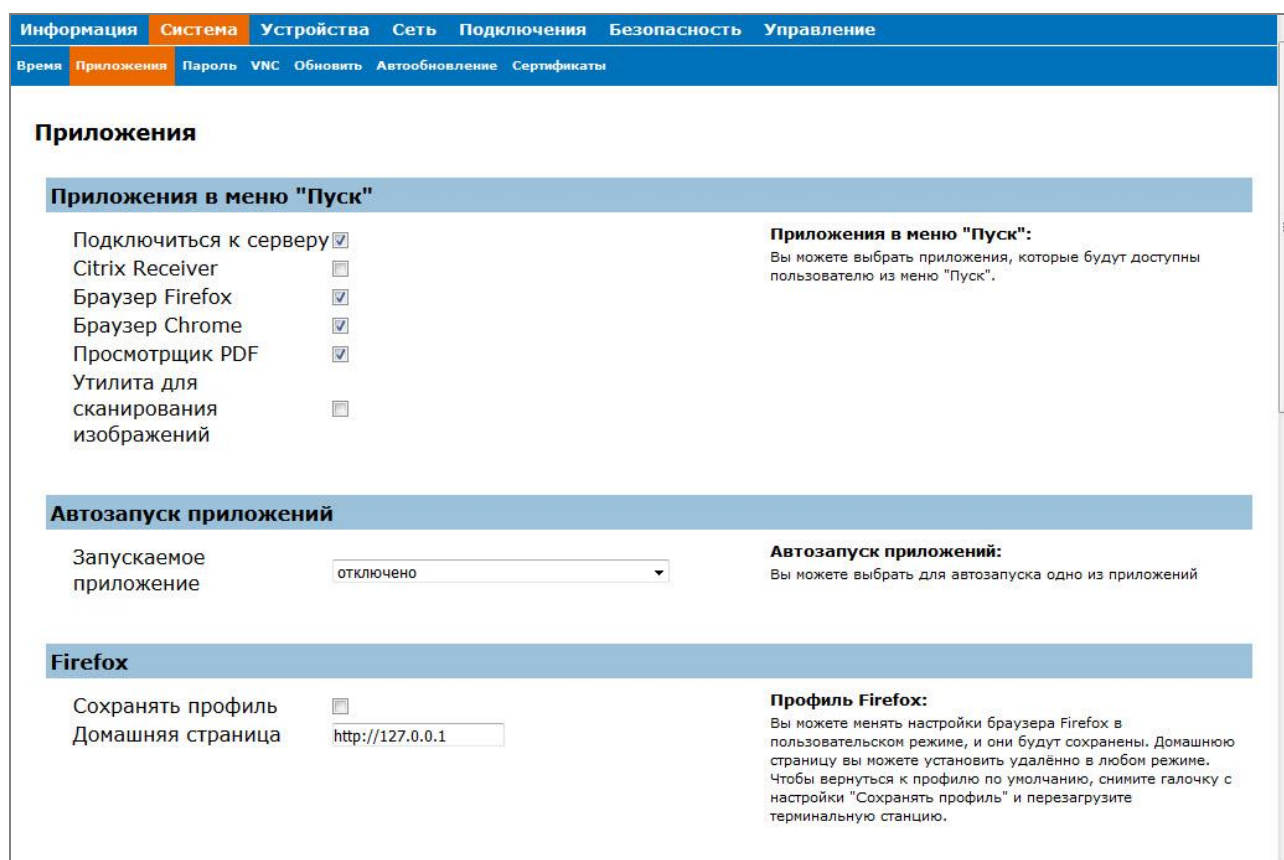


Рис. 4.14

<b>Chrome</b>	
Сохранять профиль	<input type="checkbox"/>
Домашняя страница	<input type="text"/>
<b>Профиль Chrome:</b> Вы можете менять настройки браузера Chrome в пользовательском режиме, и они будут сохранены. Домашнюю страницу вы можете установить удалённо в любом режиме. Чтобы вернуться к профилю по умолчанию, снимите галочку с настройки "Сохранять профиль" и перезагрузите терминальную станцию.	
<b>VMware</b>	
Разрешить непроверенные соединения	<input type="checkbox"/>
<b>Разрешить непроверенные соединения:</b> Пропускать соединения по ssl без проверки на достоверность сертификатов.	
<b>RDP</b>	
Использовать NLA	<input checked="" type="checkbox"/>
<b>Использовать NLA:</b> Использовать Network Level Authentication для аутентификации в FreeRDP.	
<b>Прочее</b>	
Записывать события в журнал	<input checked="" type="checkbox"/>
Отправлять логи на сервер	<input type="text"/>
Отключить переключение раскладки	<input type="checkbox"/>
<b>Записывать события в журнал:</b> Записывать в журнал события подключения внешних носителей, авторизации в системе, сетевой активности, запуска приложений и т.д.	
<b>Отключить переключение раскладки:</b> Отключить переключение раскладки в локальной системе.	
<div>Сохранить изменения Выйти</div>	

Рис. 4.15

Описание параметров:

Раздел параметров *Приложения* в меню «Пуск» - для выбора приложений, доступных пользователю из меню «Пуск». Параметры: *Подключиться к серверу*, *Браузер Firefox*, *Браузер Chrome*, *Просмотрщик PDF Evince* - выбраны по умолчанию.

*Запускаемое приложение* раздела параметров *Автозапуск приложений* - параметр, предназначенный для выбора автоматически запускаемых приложений: *Браузер Mozilla Firefox*, *Браузер Google Chrome*, *Подключиться к серверу*, *Просмотрщик PDF*, *Утилита для сканирования приложений*. По умолчанию значение параметра «отключено».

*Сохранять профиль* раздела параметров *Firefox* - параметр, для сохранения настроек браузера Firefox в пользовательском режиме. По умолчанию данный параметр не выбран. Для возврата к профилю по умолчанию, необходимо снять галочку с настройки «Сохранять профиль» и перезагрузить терминальную станцию (см.рис.4.14).

*Домашняя страница* - позволяет в любом режиме удаленно установить адрес домашней страницы.

*Сохранять профиль* раздела параметров *Chrome* - параметр, для сохранения настроек браузера Chrome в пользовательском режиме. По умолчанию данный параметр не выбран. Для возврата к профилю по умолчанию, необходимо снять галочку с настройки «Сохранять профиль» и перезагрузить терминальную станцию. (рис. 4.15).

*Домашняя страница* - позволяет в любом режиме удаленно установить адрес домашней страницы.

*Разрешить непроверенные соединения* раздела параметров *VMware* - для установки соединений терминальной станции с сервером по протоколу SSL без проверки достоверности сертификатов (только для VMWare клиента). По умолчанию данный параметр не выбран.

*Использовать NLA* раздела параметров *RDP* - для использования режима аутентификации сетевого уровня (Network Level Authentication) при подключении к терминальному серверу через FreeRDP- приложение протокола RDP. По умолчанию данный параметр выбран.

*Записывать события в журнал* раздела параметров *Прочее* - для записи в журнал событий подключения внешних носителей, авторизации в системе, запуска приложений, сетевой активности. По умолчанию данный параметр не выбран.

*Отправлять логи на сервер* - предназначен для ввода IP адреса удаленного сервера, на который следует отправлять логи.

*Отключить переключение раскладки* раздела параметров *Прочее* - для отключения переключения раскладки клавиатуры в локальной системе (если это мешает горячим клавишам на терминальном сервере). По умолчанию данный параметр не выбран.

Для выполнения настройки на вкладке *Приложения* следует:

- 1) →*Система* →*Приложения*;
- 2) внести необходимые изменения в параметры настроек;
- 3) →[Сохранить изменения].

#### 4.2.5.3. Вкладка Пароль



На вкладке *Пароль* содержатся параметры смены пароля администратора (рис. 4.16). Ниже приводится описание данных параметров.

Пароль

Смена пароля

Новый пароль:

Подтвердите пароль:

**Смена пароля:**  
Пароль для входа в веб-интерфейс и безопасный режим работы терминальной станции, а также для подключения к терминальной станции по VNC. Введите пароль дважды.

Сохранить изменения Выйти

Рис. 4.16

Описание параметров:

Раздел параметров *Смена пароля* - предназначен для установки нового пароля администратора для входа в безопасный режим и web-интерфейс консоли администратора, а также для подключения к терминальной станции по VNC.

*Новый пароль* - для ввода нового пароля администратора.

*Подтвердить пароль* - для подтверждения нового пароля администратора.

Для выполнения настройки на вкладке *Пароль* следует:

- 1) → *Система* → *Пароль*;
- 2) внести необходимые изменения в параметры настроек;
- 3) → [Сохранить изменения].

Примечание. Пароль должен состоять не менее чем из 8 символов.



#### 4.2.5.4. Вкладка VNC

На вкладке *VNC* содержится параметр настройки удаленного управления терминальной станцией через систему удаленного доступа к рабочему столу VNC (Virtual Network Computing) (рис. 4.17). Ниже приводится описание данного параметра.

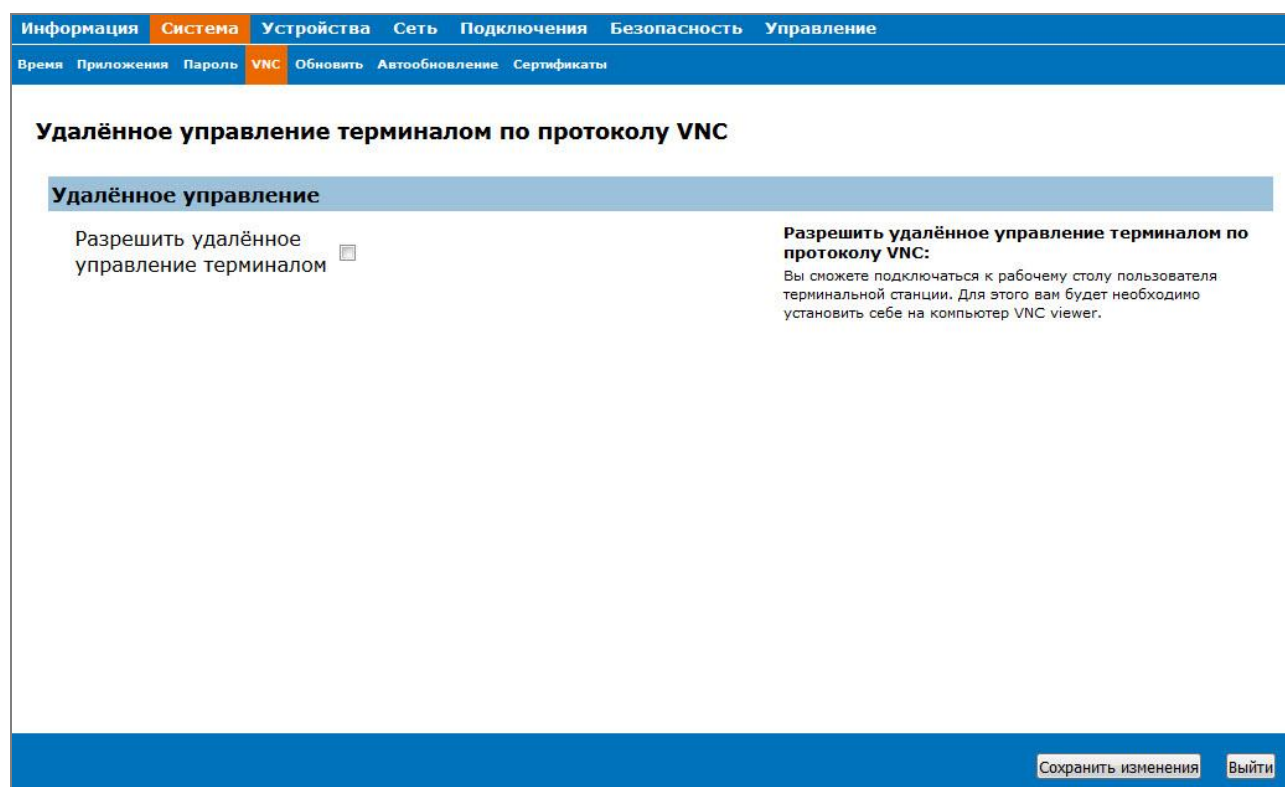


Рис. 4.17

*Разрешить удалённое управление терминалом* - для установки разрешения или запрета на удалённое управление терминальной станцией через VNC-сессию, а именно для запуска VNC-сервера терминальной станции.

Примечание. Следует помнить, что для удалённого управления терминальной станцией через VNC требуется установка программы VNC Viewer на компьютер, с которого предполагается выполнять управление (см. п. 4.3).

Для выполнения настройки на вкладке *VNC* следует:

- 1) → *Система* → *VNC*;
- 2) разрешить или запретить удалённое управление терминальной станцией через VNC;

3) →[Сохранить изменения].

#### 4.2.5.5. Вкладка Обновить

Вкладка *Обновить* содержит информацию по обновлению ПО «KTL» (рис. 4.18). Обновление ПО выполняется при включённой терминальной станции.

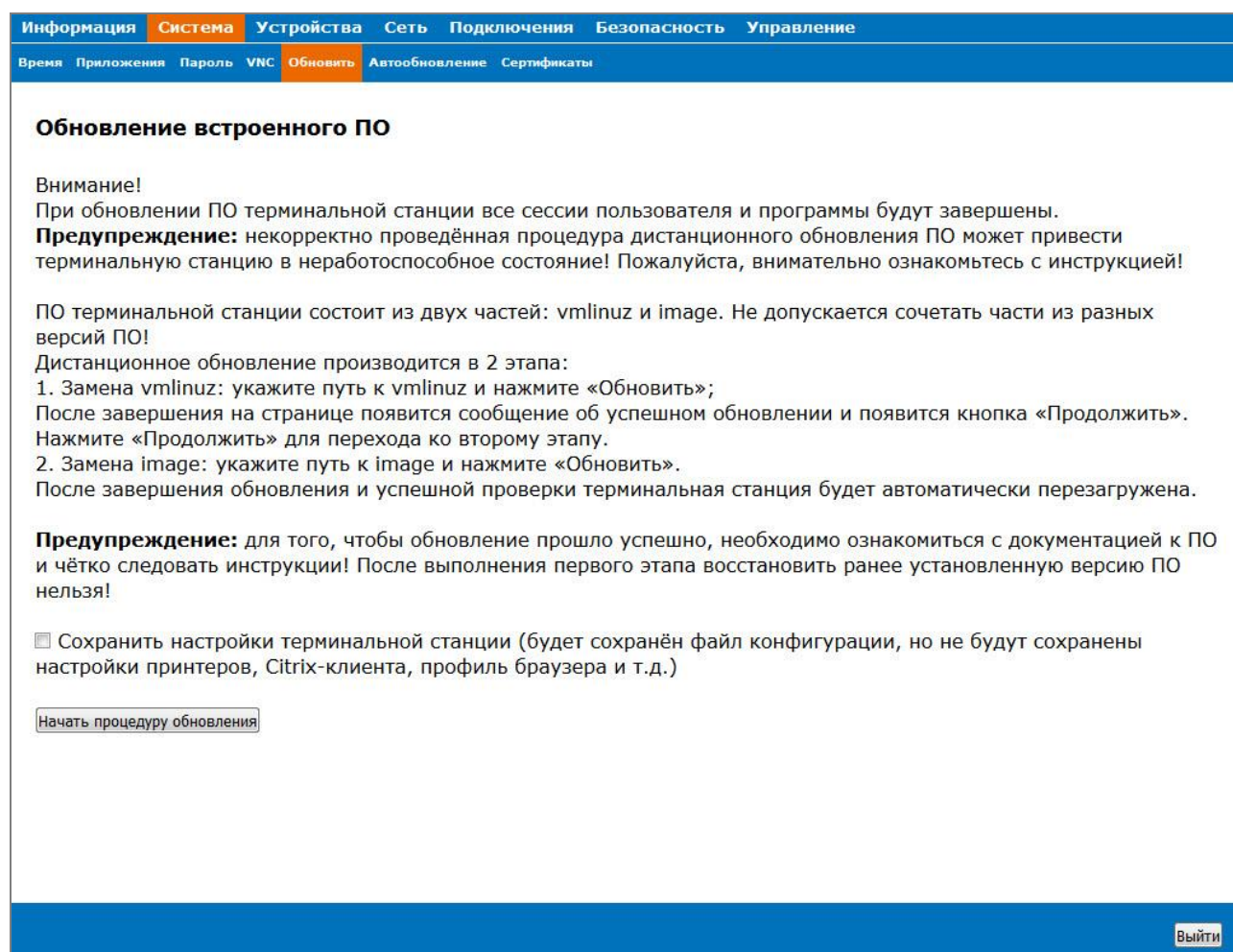


Рис. 4.18

На вкладке *Обновить* содержится подробная инструкция по обновлению ПО «Kraftway Terminal Linux», единственная кнопка [Начать процедуру обновления], предназначенная для выполнения обновления системным администратором (см. рис. 4.18)

Для выполнения настройки на вкладке *Обновить*, следует:

1) обратиться в Единый центр поддержки пользователей компании Kraftway (см. приложение 1) для получения двух файлов:

– *vtlinux* - загрузочного образа ядра KTL с базовым набором системного ПО (скриптов, конфигурационных файлов);

– *image* - образа с набором пользовательского ПО (web-браузер Mozilla Firefox, Document Viewer и т.д.).

2) скопировать полученные образы на USB-диск;

3) →*Система* →*Обновить*;

4) выбрать параметр *Сохранить настройки терминальной станции*, при необходимости;

5) →[Начать процедуру обновления], содержимое вкладки *Обновить* обновляется (рис. 4.19);

6) на вкладке *Обновить* указать место размещения файла образа ядра KTL

При размещении файла образа на локальном диске следует:

7) →[Обзор], на экран выводится окно *Выгрузка файла*, в котором следует выбрать загружаемый файл образа ядра KTL (рис. 4.20) или указать путь к образу вручную в соответствующей строке;

8) выбрать файл образа *vtlinux*;

9) →[Открыть];

10) →[Обновить] на вкладке *Обновить*, происходит распаковка и проверка файла образа *vtlinux* (на данном этапе можно отменить обновление →[Отменить]) (рис. 4.21);

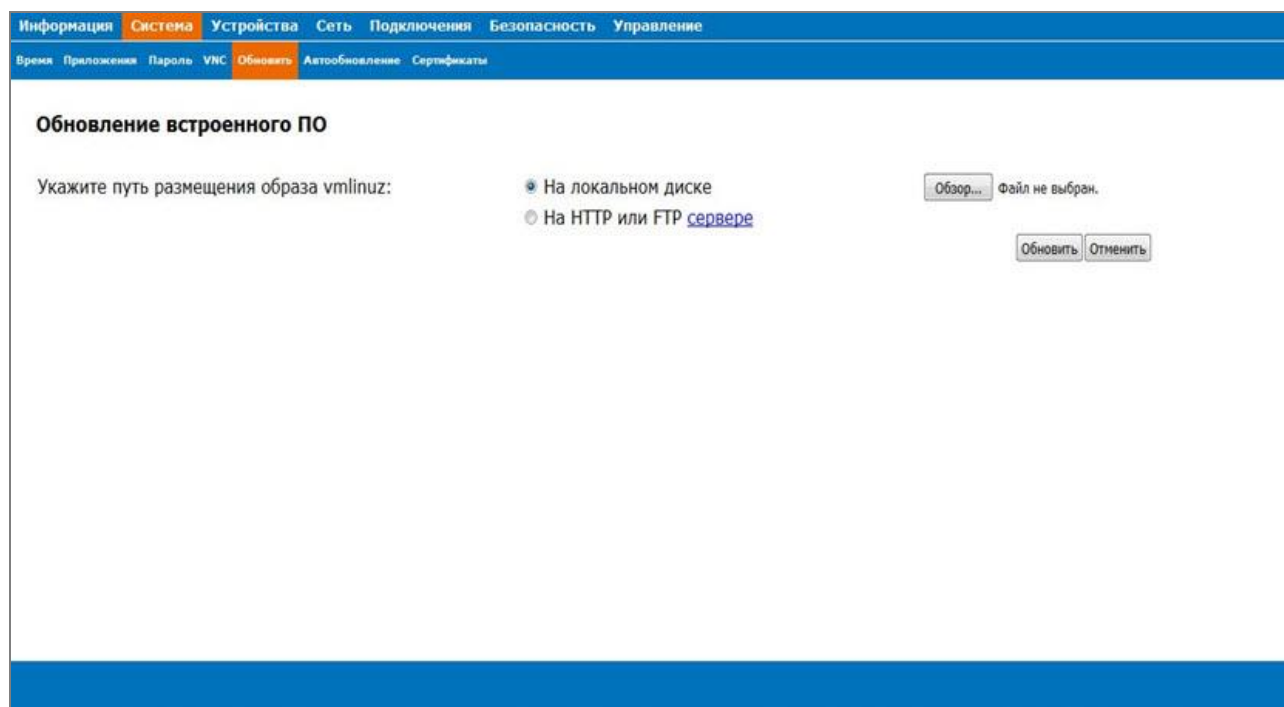


Рис. 4.19

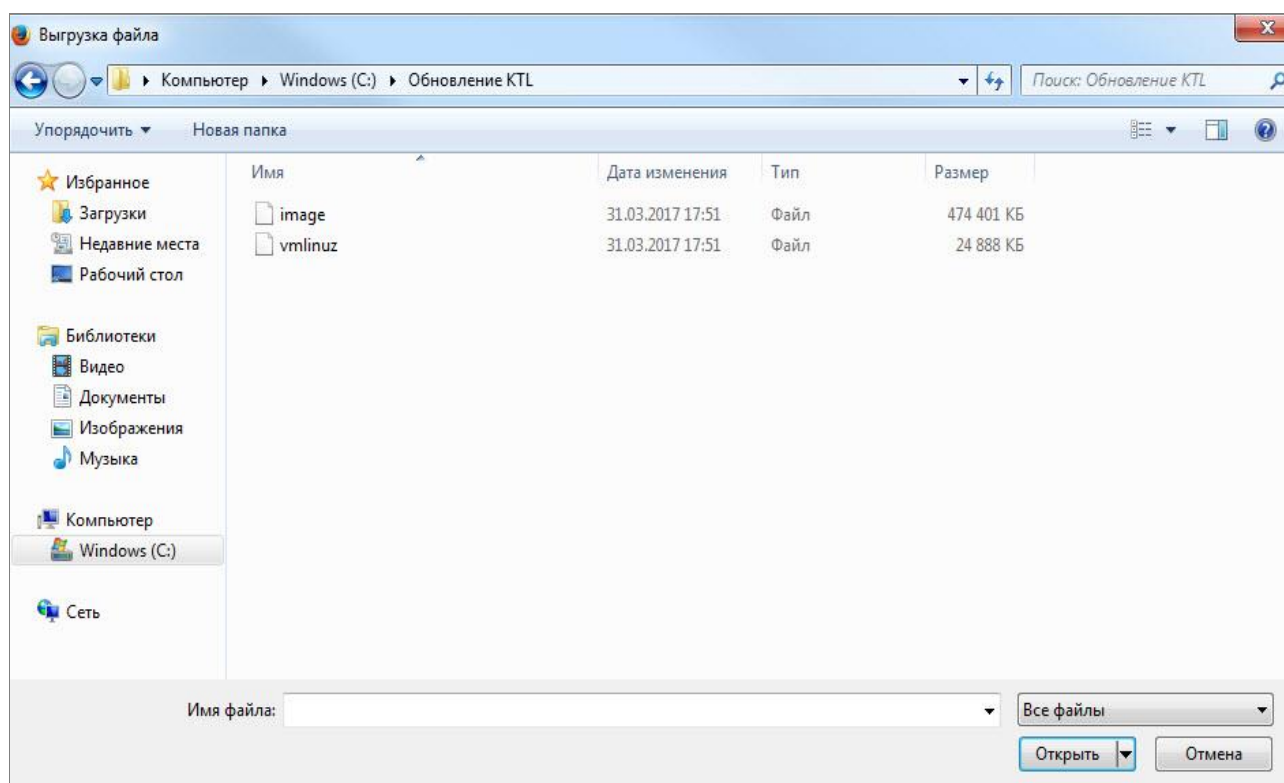


Рис. 4.20

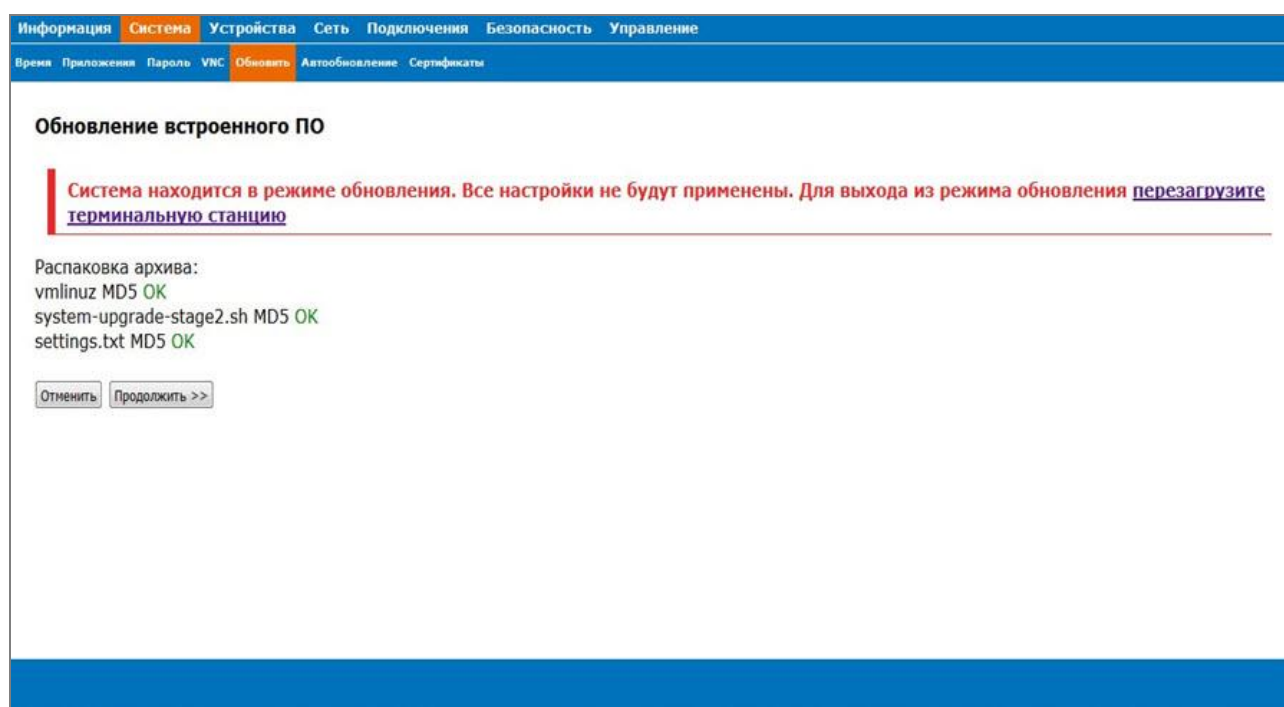


Рис. 4.21

11) →[Продолжить >>] на вкладке *Обновить*, выполняется процесс обновления системного ПО с файла образа *vmlinuz* и предлагается указать место размещения файла основного образа *image* (рис. 4.22);

12)→[Обзор], на экран выводится окно *Выгрузка файла*, в котором следует выбрать загружаемый файл образа *image* (см.рис. 4.20) или указать путь к образу вручную в соответствующей строке;

13) →[Открыть];

14) →[Обновить] на вкладке *Обновить*, выполняется процесс обновления встроенного пользовательского ПО с файла образа *image*, при этом на вкладке *Обновить* подробно выводится процесс обновления (рис. 4.23). Процесс обновления встроенного ПО завершается автоматической перезагрузкой терминальной станции;

15)при размещении файла образа на HTTP или FTP сервере : →ссылку «На HTTP или FTP сервере», на экран выводится вкладка *Автообновление* пункта меню *Система*, в котором требуется настроить параметры автоматического обновления ПО (см. рис. 4.24, п. 4.2.5.6).

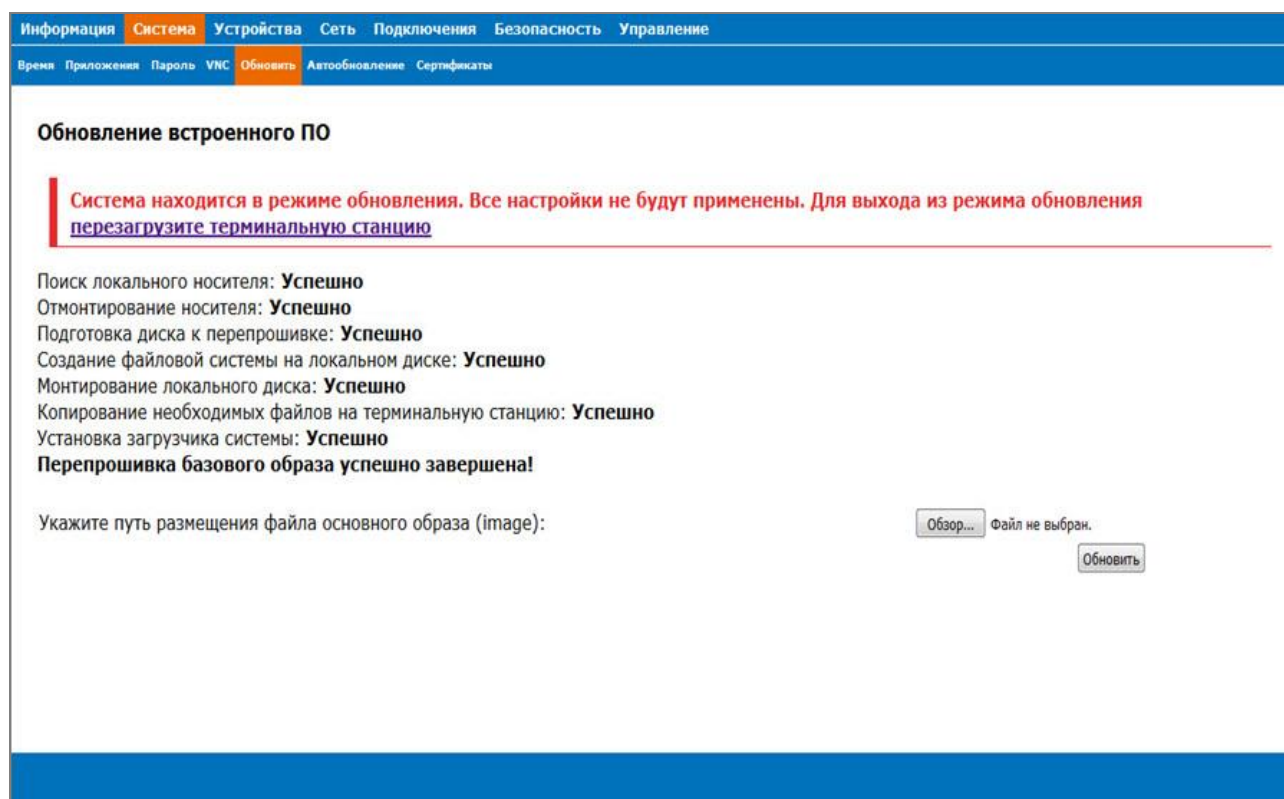


Рис. 4.22

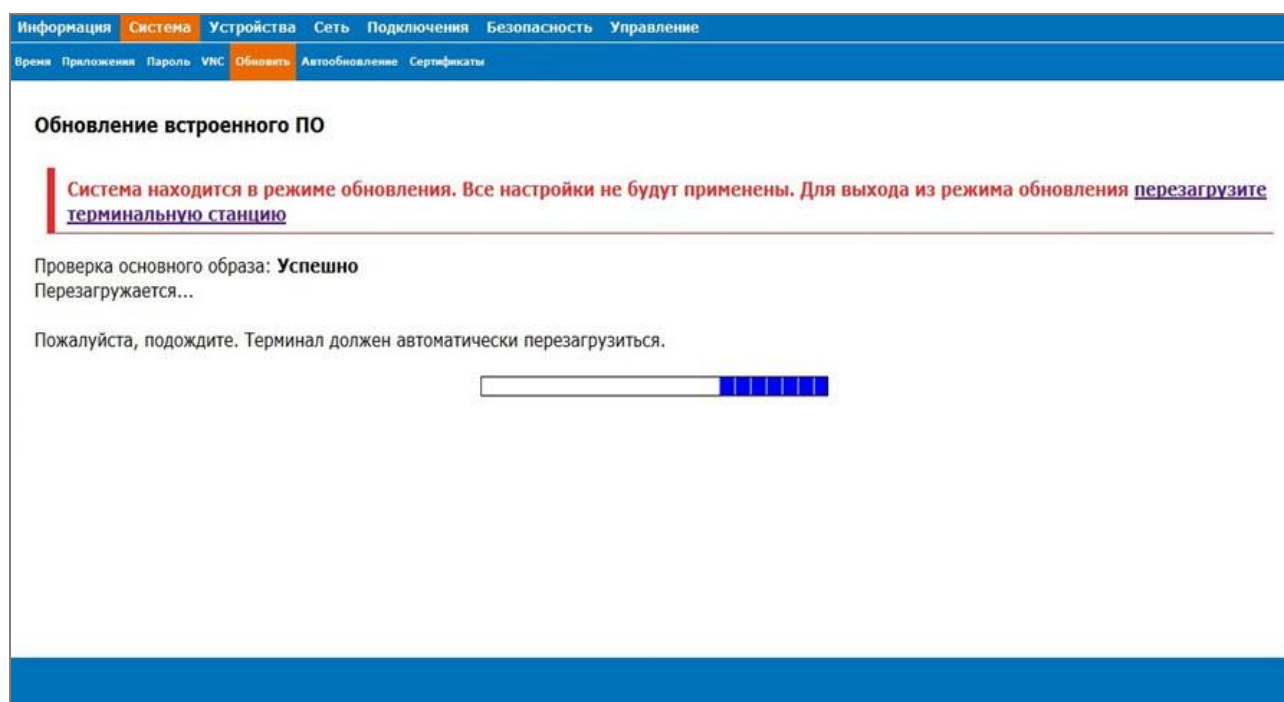


Рис. 4.23

Примечания:

1. При размещении файла образа на HTTP или FTP сервере, следует до нажатия кнопки [Обновить] настроить параметр *Адрес сервера обновлений* вкладки *Автообновление* пункта меню *Система*.
2. Следует помнить, что при обновлении ПО открытая терминальная сессия пользователя будет автоматически завершена, а запущенные программы - закрыты.
3. Есть возможность сохранить файл конфигурации терминальной станции.
4. Следует помнить, что после обновления ПО все параметры настроек клиентского окружения терминальной станции принимают значения по умолчанию, если не сохранен файл конфигурации терминальной станции.
5. ПО терминальной станции состоит из двух частей: базовой системной (*vmlinuz*) и основной пользовательской (*image*), поэтому запрещается использовать установочные образы разных версий ПО при обновлении.
6. Локальная перепрошивка осуществляется через меню *Пуск* (→[Пуск] →Обновить прошивку см. п.4.7.1).

#### 4.2.5.6. Вкладка Автообновление

На вкладке *Автообновление* содержатся параметры настройки автоматического обновления ПО «KTL» (см. рис. 4.24). Ниже приводится описание данных параметров.



Информация	<b>Система</b>	Устройства	Сеть	Подключения	Безопасность	Управление
Время	Приложения	Пароль	VNC	Обновить	<b>Автообновление</b>	Сертификаты

### Автообновление

#### Автообновление

Проверять наличие обновлений ☐  
 Спрашивать пользователя ☐  
 Получать параметры по DHCP ☐  
 Адрес сервера обновлений   
 Ограничение скорости загрузки   
 Время обновления системы

**Проверять наличие обновлений:**  
Автоматически проверять наличие обновлений при выключении или перезагрузке системы, и обновляться в случае обнаружения новых версий.

**Спрашивать пользователя:**  
Давать пользователю возможность отложить обновление.

**Получать параметры по DHCP:**  
Получать адрес сервера автообновления и скорость закачки по DHCP

**Адрес сервера обновлений:**  
HTTP или FTP адрес, на котором находятся каталоги с новыми версиями системы. Если поле оставить пустым, проверка обновлений будет производиться с серверов компании Kraftway.

**Ограничение скорости загрузки:**  
Ограничивать скорость, с которой будет загружаться новая версия системы. Пример формата: 500K, 10M, 1G, etc, подразумевая при этом скорость в формате байт/сек.

**Время обновления системы:**  
Обновление системы до или после перезагрузки терминальной станции.

**Фоновая загрузка обновления:**  
Производит загрузку обновления в фоне.

Рис. 4.24

Описание параметров:

*Проверять наличие обновлений* - для установки автоматической проверки обновлений в случае обнаружения новых версий (обновление происходит при выключении или перезагрузке системы). По умолчанию данный параметр не выбран.

*Спрашивать пользователя* - для предоставления пользователю возможности отложить обновление системы. По умолчанию данный параметр не выбран.

*Получать параметры по DHCP* - для предоставления пользователю возможности получения адреса сервера автообновления и параметров скорости закачки по DHCP. По умолчанию данный параметр не выбран.

*Адрес сервера обновлений* - поле для ввода HTTP или FTP адреса, на котором находятся каталоги с новыми версиями системы. По умолчанию данное поле не заполнено и проверка обновлений производится с серверов компании Kraftway.

*Ограничение скорости загрузки* - для ограничения скорости, с которой будет загружаться новая версия системы (пример формата: 500K, 10M, 1G и т.д., единица



измерения скорости байт/с). По умолчанию данное поле не заполнено, загрузка происходит на максимальной скорости.

*Время обновления системы* - для выбора времени обновления системы. Данный параметр имеет два состояния: «До перезагрузки», «После перезагрузки». По умолчанию установлено значение параметра «До перезагрузки».

*Фоновая загрузка обновления* - для установки обновления в фоновом режиме. Данный параметр становится доступным после выбора параметра *Получать параметры по DHCP* или присвоения параметру *Время обновления системы* значения «После перезагрузки».

Для выполнения настройки на вкладке *Автообновление* следует:

- 1) → *Система* → *Автообновление*;
- 2) внести необходимые изменения в параметры настроек;
- 3) → [Сохранить изменения].

Примечания:

1. При выборе *Получать параметры по DHCP* на сервере заранее должен быть размещен адрес сервера обновления в 40 опции внутри Vendor Specific опции 43 в виде текстовой строки (например: "<ftp://192.168.1.1/KTL/>"). Также может быть указана скорость загрузки с данного сервера, в опции 41 внутри Vendor Specific опции 43 в виде текстовой строки (например 500K).

2. Для создания собственного сервера обновлений в любую папку ftp или http сервера следует поместить:

- /ftproot/KTL/current - текстовый файл с номером текущей актуальной версии (с этой версией будет всё сравниваться и, если версия не сходится, то обновляться на неё);

- -beta, -vipnet и т.д - это отдельные ветки, они обновляются только сами на себя, либо на другую ветку вручную. Также, если у вас используется несколько веток одновременно, там можно указать актуальные версии всех веток на отдельных строках;

- /ftproot/KTL/x.x/web - папка в которую кладутся файлы vmlinuz- x.x и image и settings.txt (x.x - версия которая указана в файле current);

- на вкладке *Автообновление* пункта меню *Система* (*Система* → *Автообновление*) в поле *Адрес сервера обновлений* указать адрес:

[ftp://<сервер\\_обновлений>/KTL/](ftp://<сервер_обновлений>/KTL/) и выбрать параметр *Проверять наличие обновлений*, затем перезагрузить терминальную станцию. Тогда при перезагрузке она будет проверять наличие обновлений и в случае обнаружения выполнять обновление.

Папка с названием KTL не принципиальна и может иметь другое название или отсутствовать (все файлы могут находиться в корне диска). Главное в поле *Адрес сервера обновлений* на вкладке *Автообновление* пункта меню *Система* указать папку в которой находятся файлы.

#### 4.2.5.7. Вкладка Сертификаты

На вкладке *Сертификаты* содержатся параметры выбора цифровых сертификатов, доступных на терминальной станции, загрузки сторонних сертификатов (рис. 4.25). Ниже приводится описание данных параметров.

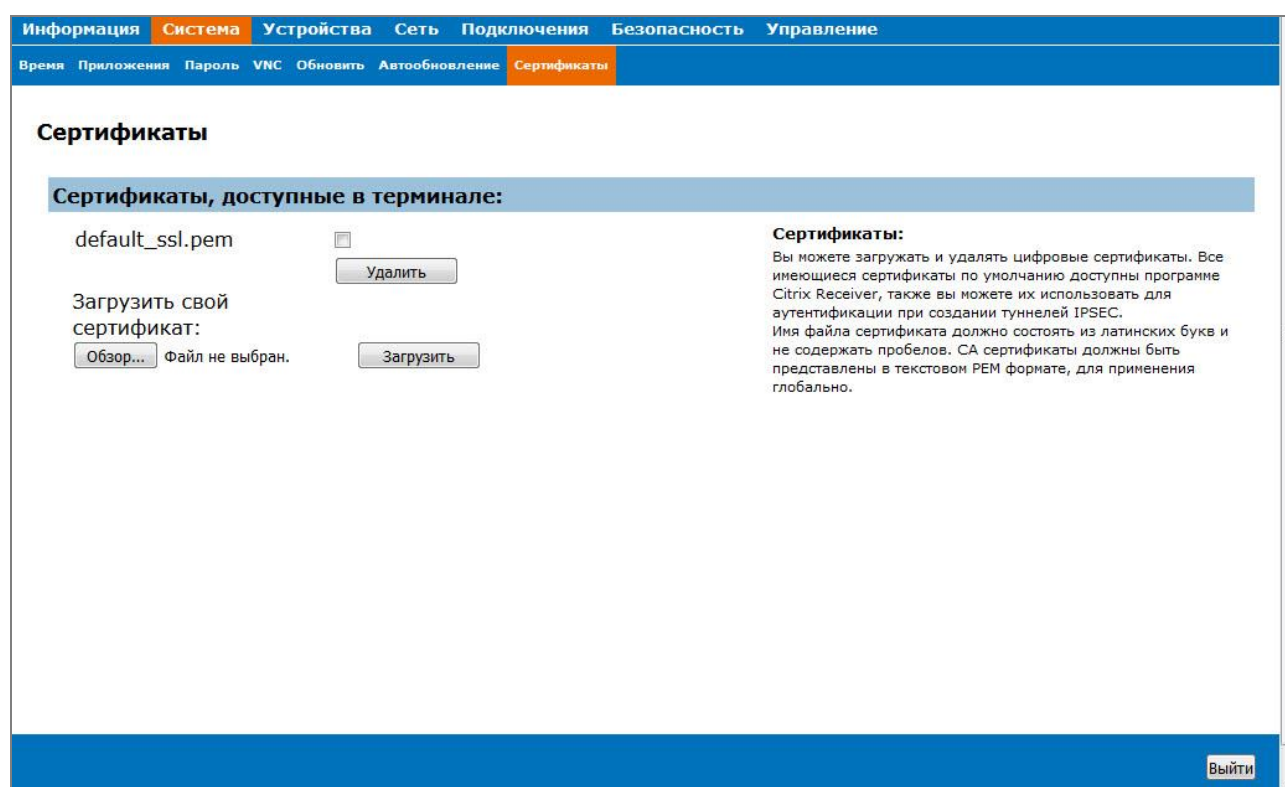


Рис. 4.25

Описание параметров:

*Сертификаты, доступные в терминале* - параметр предназначен для загрузки и удаления сертификатов, доступных на терминале. Доступны следующие сертификаты: «default\_ssl.pem» (список доступных сертификатов может отличаться от приведенного). По умолчанию сертификат не выбран.

*Загрузить свой сертификат* - параметр предназначен для загрузки сертификатов не доступных на терминале.

Примечания:

1. Все имеющиеся сертификаты по умолчанию доступны программе Citrix Receiver.

2. Все имеющиеся сертификаты можно использовать для аутентификации при создании как туннелей IPSEC, так и других VPN, требующих сертификации.

3. Следует помнить, что имя файла сертификата должно состоять из латинских букв и не содержать пробелов.

4. Следует помнить, что CA (Certification Authority - организация, обладающая правом выдачи цифровых сертификатов) сертификаты должны быть представлены в текстовом PEM формате (Privacy Enhanced Mail - расширенный сертификат электронной почты, закодированный с помощью схемы Base64 для безопасной аутентификации на веб-сайтах или цифровой подписи электронной почты), для применения глобально.

Для выполнения настройки на вкладке *Сертификаты* следует:

- 1) → *Система* → *Сертификаты*;
- 2) выбрать необходимые сертификаты из доступных на терминале;
- 3) → [Обзор...], на экран выводится окно загрузки файла сертификата, в котором следует выбрать сертификат, необходимый для добавления (см. рис. 4.26), при необходимости;
- 4) → [Открыть], при необходимости;
- 5) → [Загрузить], для начала загрузки выбранных сертификатов;
- 6) → [Удалить], для удаления сертификатов.

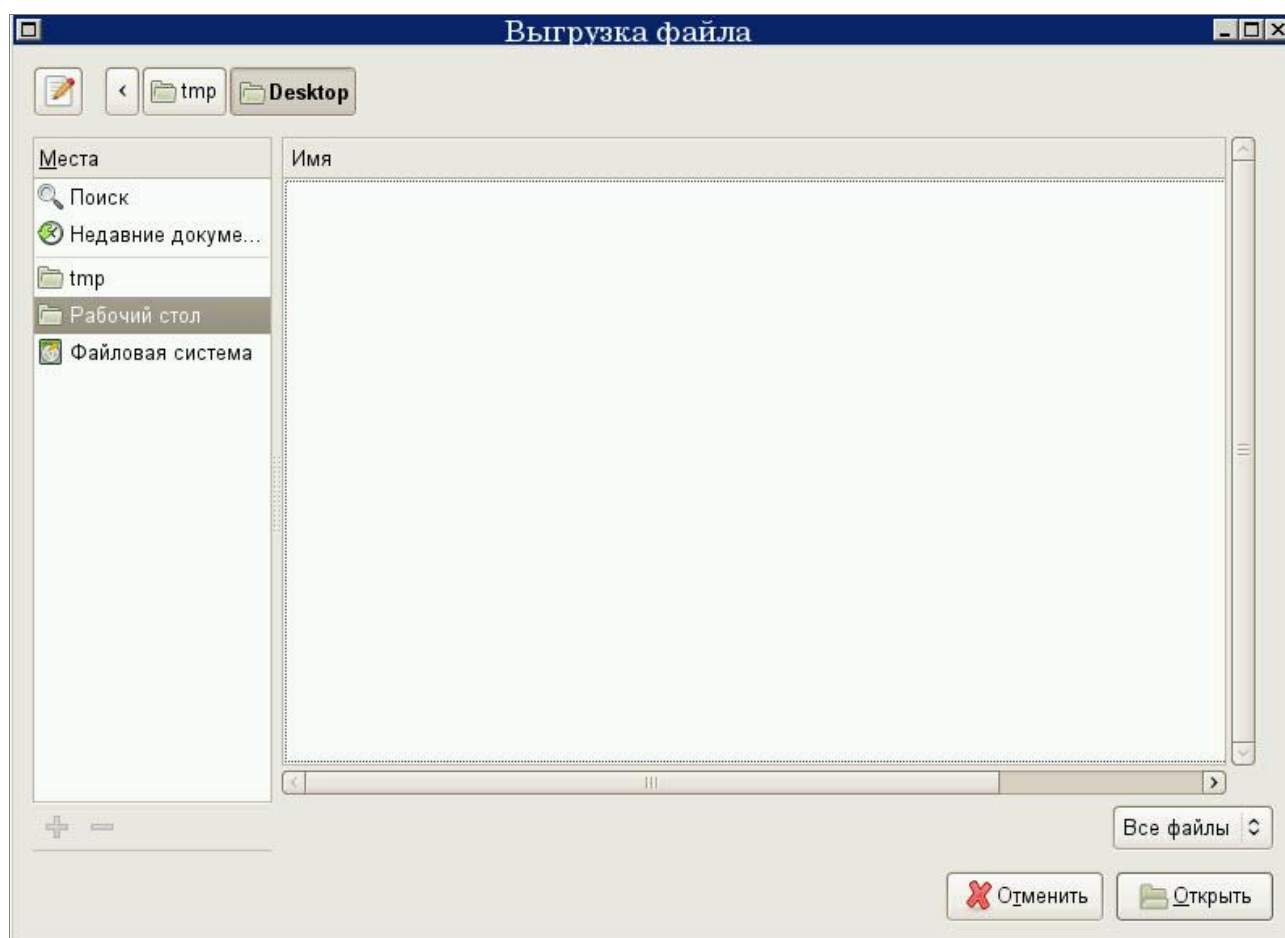


Рис. 4.26

#### 4.2.6. Пункт меню Устройства

Пункт меню *Устройства* содержит вкладки *Устройства* и *COM over IP*.

##### 4.2.6.1. Вкладка Устройства

На вкладке *Устройства* содержатся параметры настройки для настройки работы: монитора, кнопки Power, USB-дисков, принтеров, сканеров, COM/LPT-портов, сканера ШК Opticon OPR-3201, смарт-карт, USB-портов, звука (рис. 4.27, рис. 4.28, рис. 4.29). Ниже приводится описание данных параметров.

Параметры настройки мониторов (рис. 4.27):

*Использовать два монитора* - для настройки KTL для работы с двумя мониторами. По умолчанию данный параметр не выбран.

*Расположение* - для настройки расположения мониторов относительно друг друга. Данный параметр становится доступным в режиме работы с двумя мониторами.

*Основной* - для выбора основного монитора, на котором будут отображаться меню и иконки сценария. Данный параметр становится доступным в режиме работы с двумя мониторами.

*Разрешение, Глубина цвета, Частота обновления* - для выбора соответствующих значений параметров, поддерживаемых настраиваемым монитором (см. прилагаемую документацию к монитору). Значения трех параметров, установленные по умолчанию: «Авто», «Миллионы цветов (24 бита)», «Авто».

*Сенсорный экран COM* - для работы с сенсорным экраном Elotouch, подключенному к первому COM-порту. По умолчанию данный параметр не выбран.

*Сенсорный экран USB* - для работы с сенсорным экраном, подключенному к USB-порту. По умолчанию данный параметр не выбран.

*Перекалибровать* - для выполнения калибровки сенсорного экрана, подключенному к USB-порту. По умолчанию данный параметр не выбран. Данный параметр отображается в разделе настроек *Монитор* только после выбора параметра *Сенсорный экран USB*.

*Использовать драйвер Vesa* - для использования универсального Vesa-драйвера видеокарты. Обеспечивает поддержку работы большинства видеокарт с разрешениями экрана, заданными в BIOS производителем, без графического ускорения. По умолчанию данный параметр не выбран.

Параметры настройки кнопки Power (см. рис. 4.27):

*Действие при нажатии кнопки Power* - для изменения режима работы кнопки Power терминальной станции. Значения параметра: «Нет действия», «Спящий режим», «Выключение» (установлено по умолчанию).

*Не выводить запрос подтверждения перехода в спящий режим* - для отключения запроса на подтверждение перехода в спящий режим. По умолчанию данный параметр не выбран.

Параметры настройки подключения USB-дисков, настроек принтеров и сканеров (рис. 4.28):

*Монтировать USB-диски* - для установки правил использования, подключаемых к USB-портам терминальной станции USB-накопителей, значения параметра: «Нет», «Только на чтение», «На чтение и запись» (установлено по умолчанию).

Информация	Система	Устройства	Сеть	Подключения	Безопасность	Управление
Устройства COM over IP						
<b>Устройства</b>						
<b>Монитор</b>						
Использовать два монитора	<input type="checkbox"/>	<b>Использовать два монитора:</b> Настроить KTL для работы с двумя мониторами				
Разрешение	Авто	<b>Расположение Мониторов:</b> Расположение Мониторов относительно друг друга				
Глубина цвета	Миллионы цветов (24 бита)	<b>Основной монитор:</b> Монитор на котором будет отображаться меню и иконки сценария				
Частота обновления	Авто	<b>Параметры монитора:</b> При установке параметров монитора не учитываются его реальные возможности. Если после перезагрузки изображение не появится, необходимо загрузить терминальную станцию в безопасном режиме и изменить параметры монитора				
Сенсорный экран COM	<input type="checkbox"/>	<b>Сенсорный экран COM:</b> Задействовать сенсорный экран Elotouch, подключенный к первому COM-порту.				
Сенсорный экран USB	<input type="checkbox"/>	<b>Сенсорный экран USB :</b> Задействовать сенсорный экран, подключенный к USB-порту.				
Использовать драйвер Vesa	<input type="checkbox"/>	<b>Перекалибровать :</b> Перекалибровать сенсорный экран, подключенный к USB-порту при следующей загрузке.				
<b>Использовать драйвер Vesa:</b> Использовать универсальный Vesa-драйвер для видеокарты. Драйвер поддерживает только разрешения с соотношением сторон 4:3.						
<b>Кнопка Power</b>						
Действие при нажатии кнопки Power	Выключение	<b>Действие при нажатии кнопки Power:</b> Вход/выход из спящего режима производится быстрее, но на старых моделях мониторов данный режим может работать нестабильно. В этом режиме нельзя обесточивать терминальную станцию				
Не выводить запрос подтверждения перехода в спящий режим	<input type="checkbox"/>	<b>Запрос подтверждения:</b> Отключение запроса на подтверждение перехода в спящий режим				

Рис. 4.27

Параметры настройки принтеров (см. рис. 4.28)

*Перенаправлять локальный принтер* - для установки разрешения перенаправления локального принтера в сессию терминального сервера. Параметр работает для протокола RDP, при подключении по Citrix принтер перенаправляется всегда. Данный параметр выбран по умолчанию.

*Название драйвера Windows* - для ввода названия драйвера, установленного на Windows-сервере, который ассоциируется с принтером в RDP-сессии. Данный параметр используется:

- при отсутствии требуемого драйвера в списке встроенных драйверов при установке принтера;



– при необходимости использования данного конкретного драйвера для устанавливаемого принтера.

The screenshot shows a settings window with three main sections: USB-диски, Принтеры, and Сканеры. Each section has a list of options on the left and detailed descriptions on the right.

**USB-диски**

- Монтировать USB-диски: На чтение и запись (dropdown menu)
- Перенаправлять USB-диски: ☒
- Перенаправлять USB-диски по SMB протоколу: ☐

**Перенаправлять USB-диски:**  
Разрешить перенаправление USB-дисков в сессию на терминальном сервере. Параметр работает для протоколов RDP и Citrix.

**Перенаправлять USB-диски:**  
Разрешить перенаправление USB-дисков в сессию на терминальном сервере. Параметр работает для протокола NX.

**Принтеры**

- Перенаправлять локальный принтер: ☒
- Название драйвера Windows: (пока не настроено ни одного принтера)
- Включить принт-сервер: ☐
- [Настроить принтеры](#)

**Перенаправлять локальный принтер:**  
Разрешить перенаправление локального принтера в сессию на терминальном сервере. Параметр работает для протокола RDP, при подключении по Citrix принтер перенаправляется всегда.

**Название драйвера Windows:**  
Вы можете указать имя драйвера на Windows, который будет ассоциирован с принтером, проброшенным в RDP-сессию. Если вы укажете неправильный драйвер (которого нет на сервере), принтер может не отображаться в сессии. При подключении по RDP применяются все указанные драйверы, при подключении по Citrix - только для принтера по умолчанию (его можно выбрать, перейдя по ссылке "Настроить принтеры").

**Включить принт-сервер:**  
Разрешить использование терминальной станции в качестве принт-сервера

**Сканеры**

- Включить скан-сервер: ☐
- Перенаправление папки: ☐

**Включить скан-сервер:**  
Разрешить использование терминальной станции в качестве скан-сервера

**Перенаправление папки сканера:**  
Включение перенаправления папки сканирования в Citrix. Для перенаправления будет использован drive X.

Рис. 4.28

Названия доступных принтеров с полями для ввода названия драйвера выводятся на вкладке *Устройства* под параметром *Название драйвера Windows* только после установки этих устройств. Значение по умолчанию - «(пока не настроено ни одного принтера)».

*Включить принт-сервер* - для установки разрешения использования терминальной станции с подключённым к ней локальным принтером в качестве принт-сервера. По умолчанию данный параметр не выбран.

*Принтер для принт-сервера* - для выбора локального принтера, который выступает в качестве принтера для принт-сервера, т.е. установлен и настроен специально для него. Данный параметр выводится на вкладке *Устройства* только после

выбора параметра *Включить принт-сервер*. Синтаксис значений параметра: <название принтера 1>, ..., <название принтера n>.

*Настроить принтеры* - параметр-ссылка, предназначенный для установки и настройки печатающих устройств с помощью системы печати CUPS (Common UNIX Printing System, см. п. 4.4). После нажатия на него в браузере Mozilla Firefox вместо консоли администратора отображается основная страница системы печати CUPS (<http://127.0.0.1:631/> - при локальной установке и настройке печатающих устройств, <http://<IP-адрес терминальной станции>:631/> - при удалённой установке и настройке печатающих устройств).

Параметры настройки сканеров (см. рис. 4.28):

*Включить скан-сервер* - для установки разрешения использования терминальной станции с подключённым к ней локальным сканером в качестве скан-сервера. По умолчанию данный параметр не выбран.

*Перенаправление папки* - для разрешения перенаправления папки сканирования в Citrix (при установке разрешения для перенаправления используется *drive X*). По умолчанию данный параметр не выбран.

Параметры настройки портов, смарт-карт и звука (рис.4.29)

*Перенаправлять COM/LPT порты* - для установки разрешения перенаправления COM/LPT-портов в сессию на терминальном сервере (при подключении различного рода специального оборудования, при работе с которыми необходимо прямое обращение к портам, например, сканеров штрих кодов). Параметр работает для протоколов RDP и Citrix. По умолчанию данный параметр не выбран.

*Перенаправлять виртуальный COM-порт* - для установки разрешения перенаправления виртуального COM-порта сканера штрих-кодов Opticon OPR-3201 в сессию на терминальном сервере (параметр работает для протокола RDP при подключении через сценарии). По умолчанию данный параметр не выбран.

*Перенаправлять смарт-карты* - для установки разрешения перенаправления смарт-карт в сессию на терминальном сервере (параметр работает для подключений по протоколу RDP при помощи Freerdp, при подключении по Citrix смарт-карта перенаправляется всегда). Данный параметр выбран по умолчанию.

*Выбрать смарткарту по умолчанию* - для выбора модели смарткарты для авторизации в Citrix Receiver. Значение параметра по умолчанию - «Автовыбор».

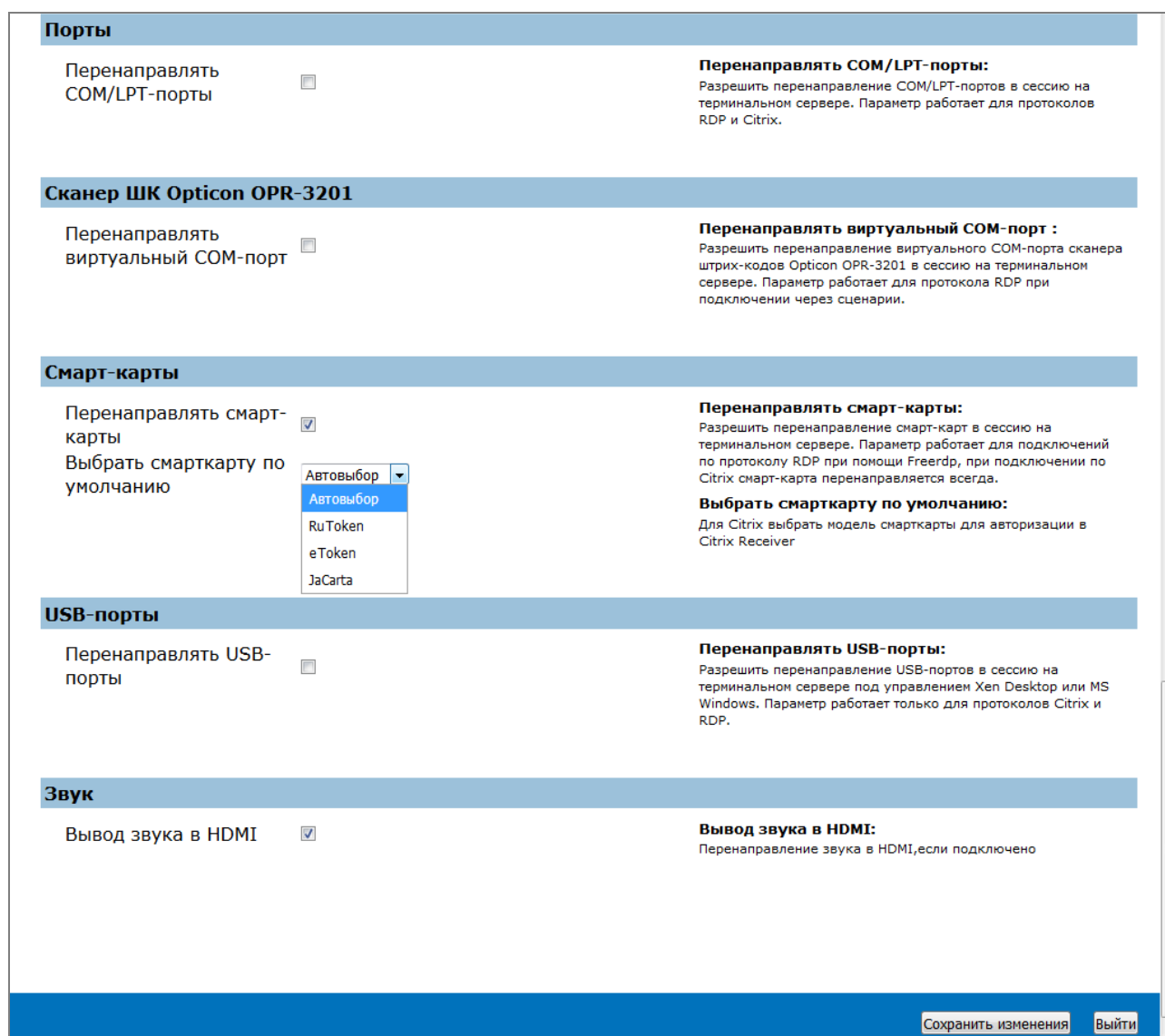


**Перенаправлять USB-порты** - для установки разрешения перенаправления USB-портов в сессию на терминальном сервере под управлением Xen Desktop или MS Windows (параметр работает только для протокола Citrix и RDP). По умолчанию данный параметр не выбран.

**Вывод звука в HDMI** - для перенаправления звука в HDMI, если подключено. По умолчанию данный параметр не выбран.

Для выполнения настройки на вкладке *Устройства* следует:

- 1) → *Устройства* → *Устройства*;
- 2) внести необходимые изменения в параметры настроек;
- 3) → [Сохранить изменения].



**Порты**

Перенаправлять COM/LPT-порты ☐

**Перенаправлять COM/LPT-порты:**  
Разрешить перенаправление COM/LPT-портов в сессию на терминальном сервере. Параметр работает для протоколов RDP и Citrix.

**Сканер ШК Opticon OPR-3201**

Перенаправлять виртуальный COM-порт ☐

**Перенаправлять виртуальный COM-порт :**  
Разрешить перенаправление виртуального COM-порта сканера штрих-кодов Opticon OPR-3201 в сессию на терминальном сервере. Параметр работает для протокола RDP при подключении через сценарии.

**Смарт-карты**

Перенаправлять смарт-карты ☒

Выбрать смарткарту по умолчанию

Автовыбор  
Автовыбор  
RuToken  
eToken  
JaCarta

**Перенаправлять смарт-карты:**  
Разрешить перенаправление смарт-карт в сессию на терминальном сервере. Параметр работает для подключений по протоколу RDP при помощи FreeRdp, при подключении по Citrix смарт-карта перенаправляется всегда.

**Выбрать смарткарту по умолчанию:**  
Для Citrix выбрать модель смарткарты для авторизации в Citrix Receiver

**USB-порты**

Перенаправлять USB-порты ☐

**Перенаправлять USB-порты:**  
Разрешить перенаправление USB-портов в сессию на терминальном сервере под управлением Xen Desktop или MS Windows. Параметр работает только для протоколов Citrix и RDP.

**Звук**

Вывод звука в HDMI ☒

**Вывод звука в HDMI:**  
Перенаправление звука в HDMI, если подключено

Сохранить изменения Выйти

Рис. 4.29

#### Примечания:

1. При установке параметров монитора следует учитывать режимы работы, которые он поддерживает. Если после перезагрузки изображение не появится, необходимо загрузить терминальную станцию в безопасном режиме и изменить параметры монитора.

2. ВНИМАНИЕ: ДРАЙВЕР VESA ПОДДЕРЖИВАЕТ ТОЛЬКО РАЗРЕШЕНИЯ С СООТНОШЕНИЕМ СТОРОН 4:3.

3. ВНИМАНИЕ: ПРИ ИСПОЛЬЗОВАНИИ СТАРЫХ МОДЕЛЕЙ МОНИТОРОВ, ВОЗМОЖНА НЕСТАБИЛЬНАЯ РАБОТА СПЯЩЕГО РЕЖИМА.

4. ВНИМАНИЕ: ПРИСВОЕНИЕ ПАРАМЕТРУ *ДЕЙСТВИЕ ПРИ НАЖАТИИ КНОПКИ POWER* ЗНАЧЕНИЯ «*СПЯЩИЙ РЕЖИМ*» НЕ ОБЕСТОЧИВАЕТ ТЕРМИНАЛЬНУЮ СТАНЦИЮ.

5. При работе со сканером штрих-кодов Opticon OPR-3201 параметр *Перенаправлять COM/LPT порты* не используется.

#### 4.2.6.2. Вкладка COM over IP

На вкладке *COM over IP* содержатся параметры настройки работы с локальными COM устройствами на удаленном сервере через IP соединение (рис. 4.30). Ниже приводится описание параметров вкладки.

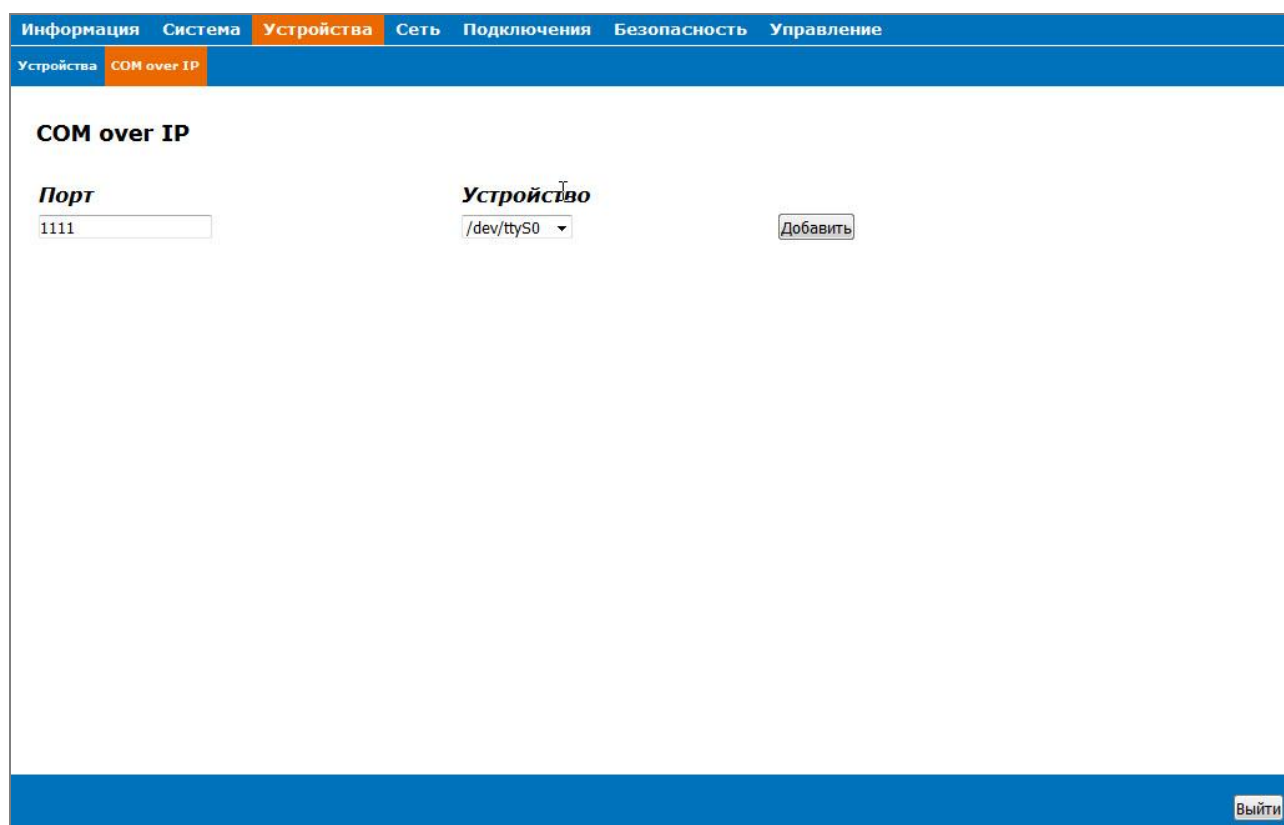


Рис. 4.30

Описание параметров:

*Порт* - поле для ввода номера используемого TCP порта.

*Устройство* - для выбора используемого COM устройства.

Для добавления новых параметров на вкладке *COM over IP* следует:

1) → *Устройства* → *COM over IP*;

2) ввести номер используемого порта и выбрать COM устройство из доступных;

3) → [ *Добавить* ], на вкладке *COM over IP* появляется строка с номером порта и названием устройства.

Для удаления требуемого соединения следует: → на ссылку *Удалить*, расположенную напротив.

#### 4.2.7. Пункт меню Сеть

Пункт меню *Сеть* содержит 8 вкладок: *TCP/IP*, *DNS*, *Routers*, *Proxy*, *Проверка*, *Active Directory*, *KSM*, *VPN*.

#### 4.2.7.1. Вкладка TCP/IP

На вкладке *TCP/IP* содержатся параметры для настройки подключения TCP/IP протокола, виртуальных сетевых интерфейсов (*eth0*, *eth1* и т.п.), устройства резервирования физических интерфейсов методом bonding balance-tlb (LAN bond0): (рис. 4.31). В графах *Текущие* и *Настроенные* на данной вкладке выводятся действующие в данный момент и установленные значения параметров соответственно. Ниже приводится описание параметров вкладки.

Информация	Система	Устройства	Сеть	Подключения	Безопасность	Управление
TCP/IP	DNS	Routes	Proxy	Проверка	Active Directory	KSM VPN

### Настройка TCP/IP

#### Общие настройки

	Текущие	Настроенные
Имя узла	ts080027187e57	ts080027187e57
Основной интерфейс	eth0	auto

[Редактировать](#)

#### LAN eth1

	Текущие	Настроенные
Интерфейс включен	Включен	Включен
Метод получения	DHCP	DHCP
IP-адрес	-	-
Маска подсети	-	-
VLAN	-	-
Шлюз	-	-

[Редактировать](#)

#### LAN eth0

	Текущие	Настроенные
Интерфейс включен	Включен	Включен
Метод получения	DHCP	DHCP
IP-адрес	10.0.154.89	-
Маска подсети	255.255.255.0	-
VLAN	-	-
Шлюз	10.0.154.1	-

[Редактировать](#)

#### LAN bond0

	Текущие	Настроенные	
Интерфейс включен	Отключен	Отключен	<b>bond0:</b> Устройство резервирования физических интерфейсов методом bonding balance-tlb. Включенные в bond0 интерфейсы не могут иметь самостоятельные IP. Они будут работать только в составе bond0.
Метод получения	Статический IP		
IP-адрес			
Маска подсети			
VLAN			
Шлюз			
Подключенные интерфейсы			

[Редактировать](#)

Рис. 4.31

Описание параметров:

*Имя узла* - для отображения и ввода имени используемого узла. По умолчанию терминальной станции присваивается имя типа «ts<MAC-адрес>», например, «ts080027058837».

*Основной интерфейс* - для отображения и выбора сетевого интерфейса, шлюз которого будет назначен в системе шлюзом по умолчанию. Значение, установленное по умолчанию - «auto».

*Интерфейс включён, включить интерфейс* - для отображения и включения /отключения виртуального сетевого интерфейса. По умолчанию данный параметр выбран.

*Метод получения* - для отображения и установки метода получения IP-адреса терминальной станцией, значения параметра: «DHCP» (установлен по умолчанию), «Статический IP-адрес».

*IP-адрес* - для отображения и ввода статического IP-адреса.

*Маска подсети* - для отображения и ввода используемой маски подсети при назначении статического IP-адреса терминальной станции.

*VLAN* - для ввода номера виртуальной подсети.

*Шлюз* - для ввода IP-адреса используемого шлюза при назначении статического IP-адреса терминальной станции. Значение параметра по умолчанию отсутствует.

*Подключенные интерфейсы* - для выбора подключенного интерфейса в разделе параметров *LAN bond0*.

Для выполнения настройки параметров раздела *Общие настройки*, представленных на вкладке *TCP/IP*, следует:

1) →*Сеть* →*TCP/IP*;

2) *Общие настройки* →[Редактировать], выводится параметры для редактирования (рис. 4.32);

3) ввести имя узла в соответствующее поле и выбрать сетевой интерфейс;

4) →[Сохранить изменения].

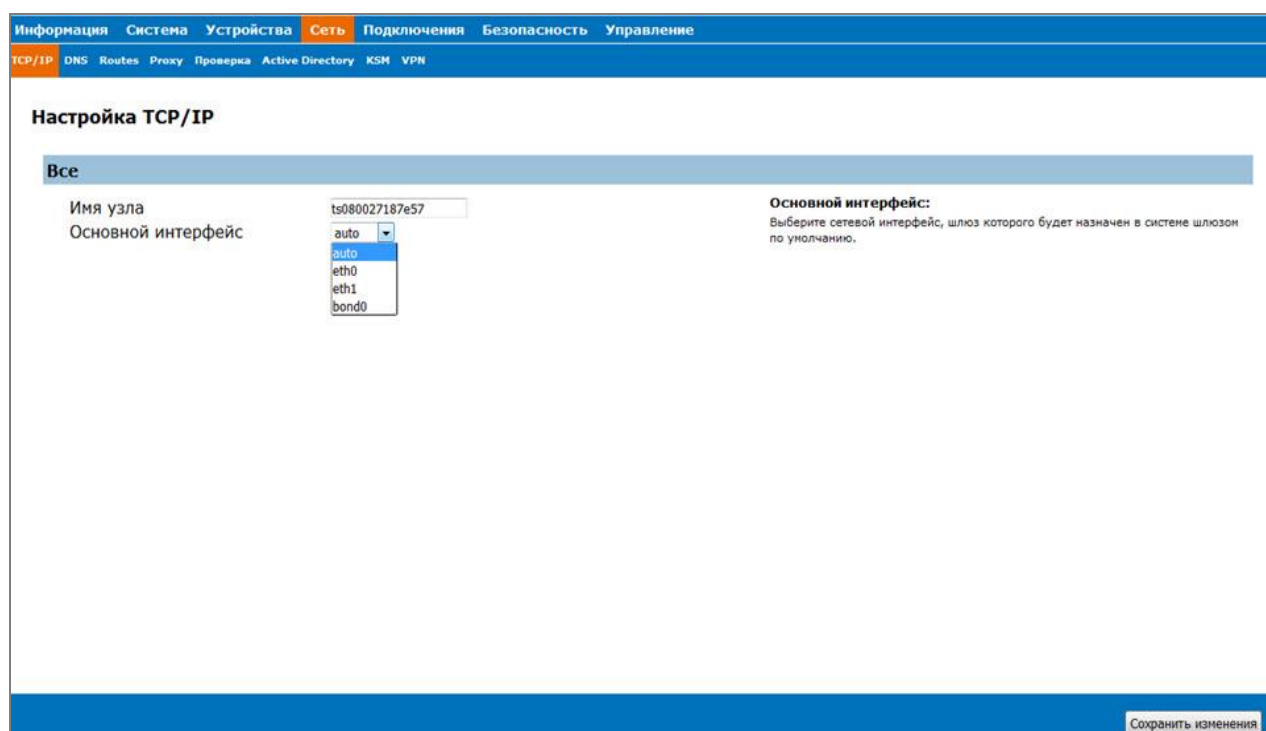


Рис. 4.32

Для выполнения настройки параметров разделов *LAN eth0* или *LAN eth1*, представленных на вкладке *TCP/IP*, следует:

- 1) → *Сеть* → *TCP/IP*;
- 2) выбрать требуемый сетевой интерфейс (*LAN eth0* или *LAN eth1*) → [Редактировать], выводятся параметры для редактирования (рис. 4.33);
- 3) определить значение параметра *Включить интерфейс*, при выключенном интерфейсе ввести номер виртуальной подсети (при необходимости);
- 4) при включенном интерфейсе выбрать метод получения IP адреса;
- 5) далее если выбран метод получения *DHCP* - ввести номер виртуальной подсети (при необходимости);
- 6) если выбран метод получения *Статический IP* - ввести в соответствующие поля статический IP адрес терминальной станции, маску подсети, номер виртуальной подсети (при необходимости), IP-адрес шлюза, при необходимости (рис. 4.34);
- 7) → [Сохранить изменения].

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка Active Directory KSM VPN

### Настройка TCP/IP

#### Настройка сетевого интерфейса eth0

Включить интерфейс ☒

Метод получения DHCP

VLAN

Сохранить изменения Выйти

Рис. 4.33

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка Active Directory KSM VPN

### Настройка TCP/IP

#### Настройка сетевого интерфейса eth0

Включить интерфейс ☒

Метод получения Статический IP

IP-адрес

Маска подсети

VLAN

Шлюз

Сохранить изменения Выйти

Рис. 4.34



Для выполнения настройки параметров раздела *LAN bond0*, представленных на вкладке *TCP/IP*, следует:

- 1) →*Сеть* →*TCP/IP*;
- 2) *LAN bond0*→[Редактировать], выводится параметры для редактирования (рис.4.35); определить значение параметра *Включить интерфейс*;
- 3) в параметре *Добавить интерфейс* выбрать интерфейс, который нужно добавить (при необходимости);
- 4) при выключенном интерфейсе ввести номер виртуальной подсети (при необходимости) (рис.4.35.);
- 5) при включенном интерфейсе выбрать метод получения IP адреса;
- 6) далее, если выбран метод получения *DHCP* - ввести номер виртуальной подсети (при необходимости) (рис.4.36);
- 7) если выбран метод получения *Статический IP* - ввести в соответствующие поля статический IP адрес терминальной станции, маску подсети, номер виртуальной подсети (при необходимости), IP-адрес шлюза, при необходимости (рис. 4.37);
- 8) →[Сохранить изменения].

Примечание. Включенные в *bond0* интерфейсы не могут иметь самостоятельные IP. Они будут работать только в составе *bond0*.

ИнформацияСистемаУстройстваСетьПодключенияБезопасностьУправление

TCP/IPDNSRoutesProxyПроверкаActive DirectoryKSMVPN

## Настройка TCP/IP

### Настройка сетевого интерфейса bond0

Включить интерфейс ☐

Добавить интерфейс:

eth1 ☐

eth0 ☐

VLAN

Сохранить измененияВыйти

Рис.4.35

ИнформацияСистемаУстройстваСетьПодключенияБезопасностьУправление

TCP/IPDNSRoutesProxyПроверкаActive DirectoryKSMVPN

## Настройка TCP/IP

### Настройка сетевого интерфейса bond0

Включить интерфейс ☒

Добавить интерфейс:

eth1 ☐

eth0 ☐

Метод получения

VLAN

Сохранить измененияВыйти

Рис.4.36

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка Active Directory KSM VPN

### Настройка TCP/IP

#### Настройка сетевого интерфейса bond0

Включить интерфейс ☒

Добавить интерфейс:

eth1 ☐

eth0 ☐

Метод получения Статический IP

IP-адрес 192.168.0.1

Маска подсети 255.255.255.0

VLAN

Шлюз

Сохранить изменения Выйти

Рис. 4.37

#### 4.2.7.2. Вкладка DNS

Вкладка *DNS* предназначена для установки и добавления DNS-серверов локальной сети (рис. 4.38).

Для добавления IP-адресов DNS-серверов локальной сети следует:

1) → *Сеть* → *DNS*;

2) ввести IP-адрес устанавливаемого DNS-сервера в соответствующее поле, например,  
10.0.0.171;

3) → [Добавить], на вкладке *DNS* выводится IP-адрес добавленного DNS-сервера.

Для удаления IP-адреса DNS-сервера локальной сети следует:

1) → *Сеть* → *DNS*;

2) выбрать из списка IP-адресов, используемых DNS-серверов, IP-адрес удаляемого DNS-сервера, например, 10.0.0.171;

3) → на ссылку *Удалить*, расположенную рядом с IP-адресом удаляемого DNS-сервера.

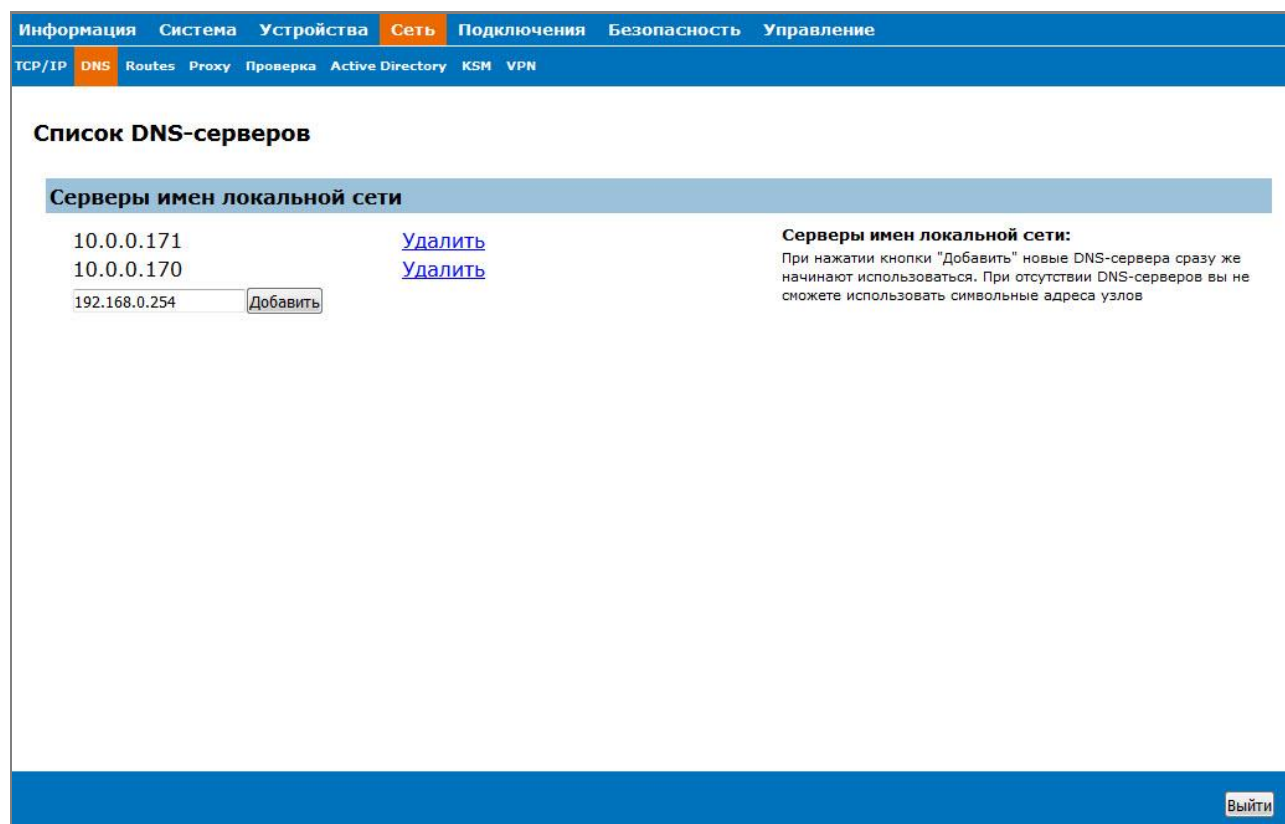


Рис. 4.38

Примечания:

1. IP-адрес DNS-сервера 192.168.0.254 введён в поле по умолчанию только для примера.
2. Только что добавленный локальный DNS-сервер сразу же начинает использоваться.
3. При отсутствии установленных локальных DNS-серверов использование символьных имён узлов невозможно.

#### 4.2.7.3. Вкладка Routes

Вкладка *Routes* предназначена для создания таблицы маршрутизации (рис. 4.39). Ниже приводится описание параметров вкладки.

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS **Routes** Proxy Проверка Active Directory KSM VPN

**Таблица роутинга**

Подсеть	Маска сети	Шлюз	Интерфейс	
<input type="text" value="192.168.0.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="eth1"/>	<input type="button" value="Добавить"/>

Выйти

Рис. 4.39

*Подсеть* - для задания адреса сети назначения.

*Маска сети* - для указания маски сети назначения.

*Шлюз* - для задания адреса шлюза сети назначения.

*Интерфейс* - для указания интерфейса терминальной станции.

Для добавления записей в таблицу маршрутизации следует:

- 1) → *Сеть* → *Routes*;
- 2) ввести IP-адрес подсети, маску сети, IP-адрес шлюза в соответствующее поле и выбрать тип интерфейса;
- 3) → [Добавить], на вкладке *Routes* выводятся параметры (рис. 4.40).

Подсеть	Маска сети	Шлюз	Интерфейс	
192.168.0.0	255.255.255.0	192.168.0.254	eth1	<a href="#">Удалить</a>
<input type="text" value="192.168.0.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="eth1"/>	<input type="button" value="Добавить"/>

Рис. 4.40

Для удаления записи из таблицы маршрутизации следует:

- 1) → *Сеть* → *Routes*;
- 2) выбрать из таблицы маршрутов, удаляемый маршрут;
- 3) → на ссылку *Удалить* (см. рис. 4.40).

Примечание: Создать запись в таблице маршрутизации с VPN интерфейсом возможно только после создания VPN соединения на вкладке VPN (см. п. 4.2.7.8).

#### 4.2.7.4. Вкладка Proxy

На вкладке *Proxy* содержатся параметры для настройки использования прокси-сервера HTTP и прокси-сервера FTP (рис. 4.41). Ниже приводится описание параметров вкладки.

Использовать http proxy ☐

Сервер

Логин

Пароль

**http proxy:**  
Для использования прокси сервера http необходимо ввести адрес сервера, вида http://адрес\_сервера, логин и пароль при необходимости

Использовать ftp proxy ☐

Сервер

Логин

Пароль

**ftp proxy:**  
Для использования прокси сервера ftp необходимо ввести адрес сервера, вида ftp://адрес\_сервера, логин и пароль при необходимости

Сохранить изменения Выйти

Рис. 4.41

*Использовать http proxy* - для выбора прокси-сервера http (по умолчанию параметр не выбран).

*Использовать ftp proxy* - для выбора прокси-сервера ftp (по умолчанию параметр не выбран).

*Сервер* - адрес сервера.

*Логин* - поле ввода логина.

*Пароль* - поле ввода пароля.

Для использования прокси-сервера HTTP следует:

- 1) →Сеть →Proxy;
- 2) выбрать параметр *Использовать http proxy*;
- 3) ввести адрес сервера, логин и пароль;
- 4) →[Сохранить изменения].

Для использования прокси-сервера FTP следует:

- 1) →Сеть →Proxy;
- 2) выбрать параметр *Использовать ftp proxy*;
- 3) ввести адрес сервера, логин и пароль;
- 4) →[Сохранить изменения].

Примечания:

1. Для использования прокси-сервера HTTP необходимо ввести адрес сервера, вида `http://адрес_сервера`.

2. Для использования прокси-сервера FTP необходимо ввести адрес сервера, вида `ftp://адрес_сервера`.

#### 4.2.7.5. Вкладка Проверка

На вкладке *Проверка* содержатся параметры для выбора тестов, которые будут выполняться перед загрузкой пользовательского интерфейса. Если тесты не будут успешно пройдены, пользовательский интерфейс не будет запущен. (рис. 4.42). Ниже приводится описание параметров вкладки.

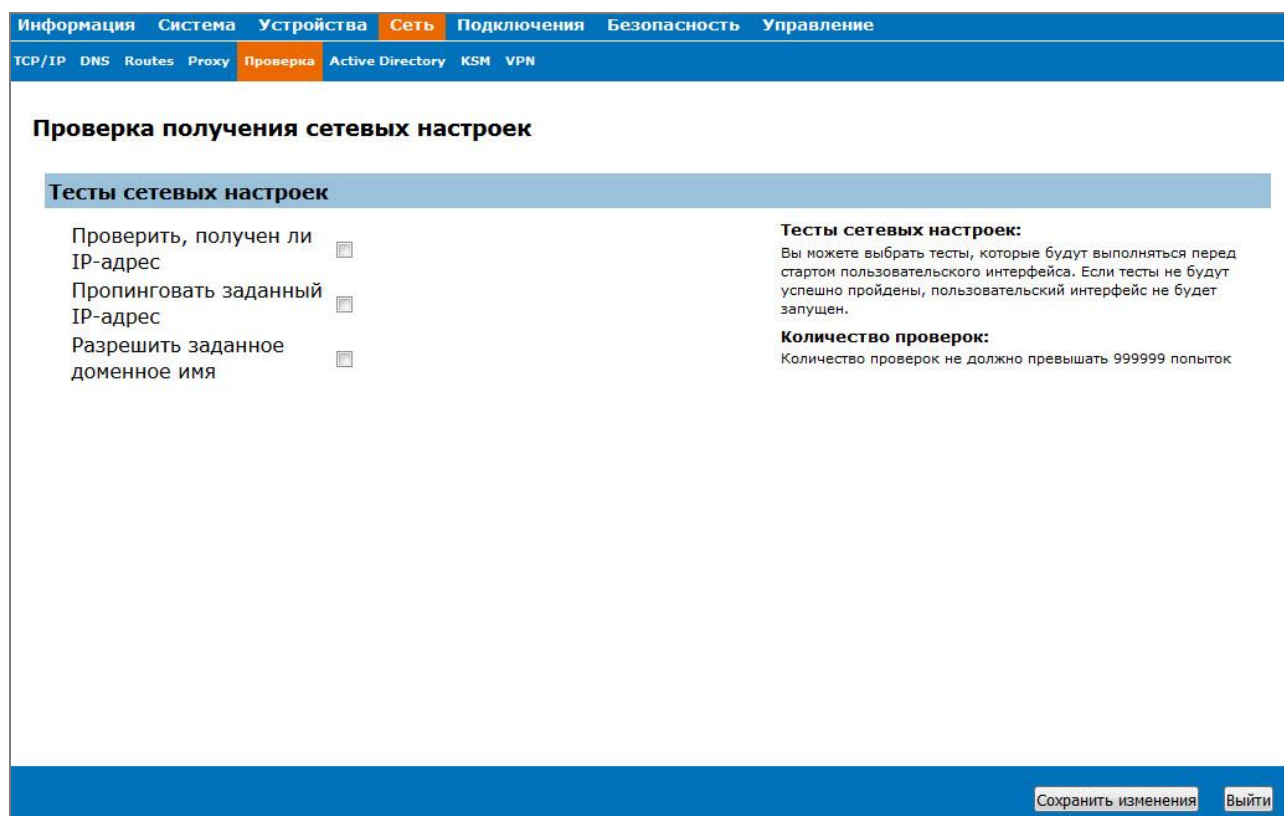


Рис. 4.42

*Проверить, получен ли IP-адрес* - для проверки получения IP-адреса терминальной станции по протоколу DHCP. По умолчанию данный параметр не выбран.

*Количество проверок* - для указания количества проверок.



*Пропинговать заданный IP-адрес* - для проверки доступности заданного IP-адреса по команде «ping». По умолчанию данный параметр не выбран.

*IP-адрес* - поле для ввода IP-адреса терминальной станции.

*Разрешить заданное доменное имя* - для проверки доступности заданного доменного имени. По умолчанию данный параметр не выбран.

*Доменное имя* - поле для ввода доменного имени.

Для включения проверки получения IP-адреса следует:

- 1) → *Сеть* → *Проверка* (рис.4.43);
- 2) выбрать соответствующий пункт *Проверить, получен ли IP-адрес*;
- 3) ввести количество проверок;
- 4) → [Сохранить изменения].

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy **Проверка** Active Directory KSM VPN

### Проверка получения сетевых настроек

#### Тесты сетевых настроек

Проверить, получен ли IP-адрес	<input checked="" type="checkbox"/>
Количество проверок	<input type="text"/>
Пропинговать заданный IP-адрес	<input checked="" type="checkbox"/>
IP-адрес	<input type="text"/>
Количество попыток	<input type="text"/>
Разрешить заданное доменное имя	<input checked="" type="checkbox"/>
Доменное имя	<input type="text"/>

**Тесты сетевых настроек:**  
Вы можете выбрать тесты, которые будут выполняться перед стартом пользовательского интерфейса. Если тесты не будут успешно пройдены, пользовательский интерфейс не будет запущен.

**Количество проверок:**  
Количество проверок не должно превышать 999999 попыток.

Сохранить изменения Выйти

Рис.4.43

Для включения проверки доступности заданного IP-адреса следует:

- 1) → *Сеть* → *Проверка*;
- 2) выбрать соответствующий пункт *Пропинговать заданный IP-адрес*;

3) ввести статический IP-адрес, который необходимо проверить на доступность по команде «ping»;

4) ввести количество попыток;

5) →[Сохранить изменения].

Для включения проверки доступности заданного доменного имени следует:

1) →*Сеть* →*Проверка*;

2) выбрать соответствующий пункт *Разрешить заданное доменное имя*;

3) ввести доменное имя, доступность которого необходимо проверить;

4) →[Сохранить изменения].

#### 4.2.7.6. Вкладка Active Directory

На вкладке *Active Directory* содержатся параметры для настройки подключения терминальной станции к домену Active Directory (см. рис. 4.44). В разделе параметров *Текущий статус* отображаются текущие значения параметров: *Имя*, *Домен*, выводится действующий в данный момент статус терминальной станции. Ниже приводится описание параметров вкладки.

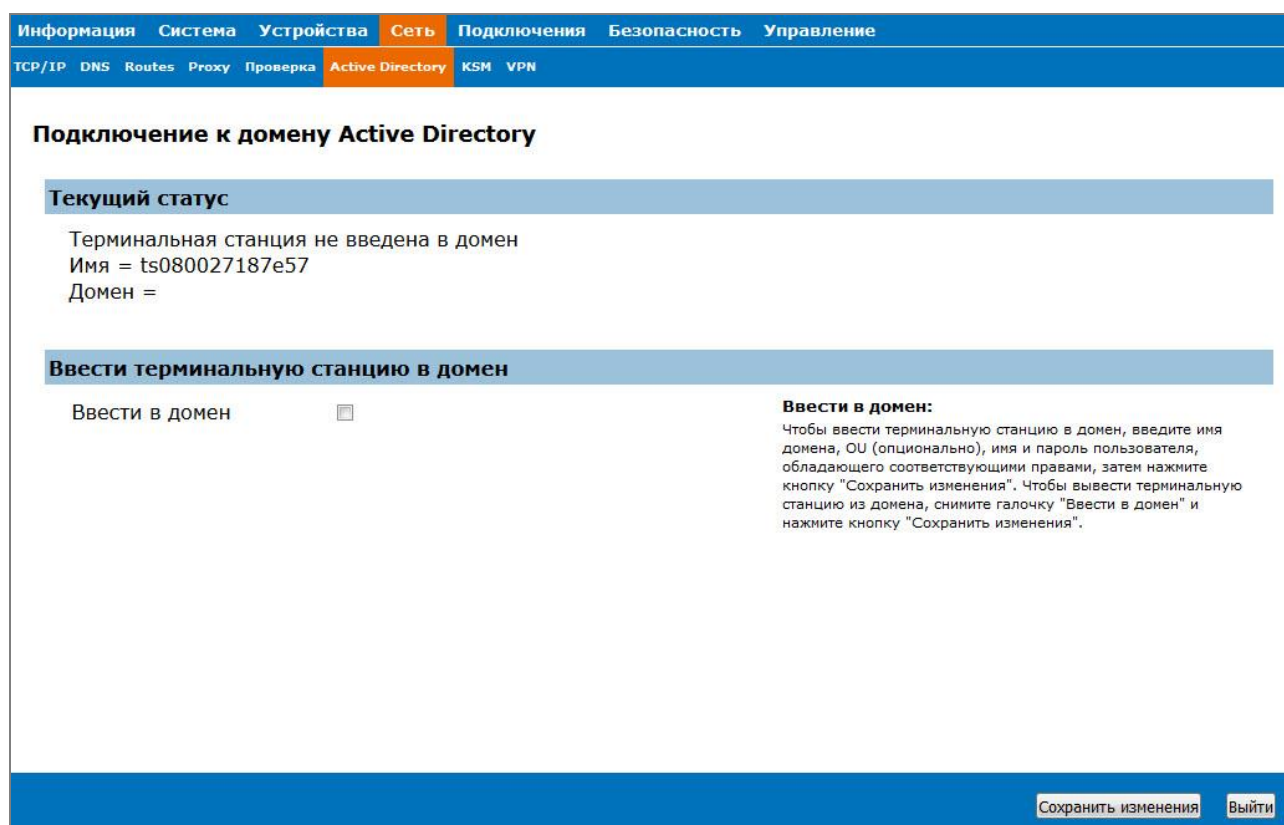


Рис. 4.44

*Ввести в домен* - для ввода терминальной станции в домен. По умолчанию данный параметр не выбран.

*Имя домена* - для ввода имени домена, к которому требуется подключить терминальную станцию.

*Organizational Unit* - для ввода организационного подразделения в домене Active Directory.

*Пользователь* - для ввода имени пользователя домена.

*Пароль* - для ввода пароля пользователя домена.

Для подключения терминальной станции к домену следует:

- 1) → *Сеть* → *Active Directory*;
- 2) выбрать *Ввести в домен* (рис. 4.45);
- 3) ввести имя домена, Organization Unit, имя и пароль пользователя;
- 4) → [Сохранить изменения].

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка **Active Directory** KSM VPN

### Подключение к домену Active Directory

#### Текущий статус

Терминальная станция не введена в домен  
Имя = ts080027187e57  
Домен =

#### Ввести терминальную станцию в домен

Ввести в домен ☒

Имя домена

Organizational Unit

Пользователь

Пароль

**Ввести в домен:**  
Чтобы ввести терминальную станцию в домен, введите имя домена, OU (опционально), имя и пароль пользователя, обладающего соответствующими правами, затем нажмите кнопку "Сохранить изменения". Чтобы вывести терминальную станцию из домена, снимите галочку "Ввести в домен" и нажмите кнопку "Сохранить изменения".

Сохранить изменения Выйти

Рис. 4.45

Для вывода терминальной станции из домена следует:

- 1) → *Сеть* → *Active Directory*;
- 2) снять галочку с пункта *Ввести в домен*;
- 3) → [Сохранить изменения].

Примечание. Параметр *Organizational Unit* задается опционально.

#### 4.2.7.7. Вкладка KSM

Вкладка *KSM* предназначена для разрешения подключения к серверу Kraftway System Manager. (рис. 4.46). Ниже приводится описание параметров вкладки.

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка Active Directory **KSM** VPN

### Подключение к серверу Kraftway System Manager

#### Kraftway System Manager

Использовать DHCP ☒

Использовать DHCP:  
Получать адрес KSM по DHCP

Использовать https: ☐

Использовать https:  
Убедитесь, что версия Kraftway System Manager поддерживает данную функцию

Kraftway System Manager:  
Авторизация в Kraftway System Manager. Убедитесь, что Ваша версия KSM требует авторизацию.

#### Обновление ip адресов в KSM

Обновлять ip адрес ☒

Выбор сетевой карты: По умолчанию ▼

Обновлять ip адрес:  
Терминальная станция будет отправлять текущий ip адрес KSM-серверу.

Сохранить изменения Выйти

Рис. 4.46

*Использовать DHCP* - для разрешения безопасного соединения с сервером по протоколу DHSP. По умолчанию данный параметр выбран.

*Обновлять ip адрес* - для разрешения отправления текущего IP-адреса терминальной станции KSM-серверу. Необходимо для автоматического обновления IP-адреса ТС в БД сервера KSM, т.к. при автоматическом методе получения IP-адреса ТС с помощью DHCP-сервера (см. п. 4.2.7.1) IP-адрес ТС может меняться, т.е. может назначаться DHCP-сервером новый IP-адрес ТС. По умолчанию данный параметр выбран.

*Выбор сетевой карты* - для выбора сетевой карты. Значение параметра по умолчанию: «По умолчанию».

*Использовать https* - для разрешения безопасного соединения с сервером по протоколу HTTPS. По умолчанию данный параметр не выбран.

*Сервер Kraftway System Manager* - для ввода имени или IP-адреса сервера KSM, к которому требуется подключить терминальную станцию. Параметр становится доступным при соединении с сервером по протоколу HTTPS (т.е. выбран параметр *Использовать https*).

*Порт KSM шлюз* - для ввода номера порта KSM шлюза. По умолчанию данный параметр имеет значение «80». Параметр становится доступным если выбран параметр *Использовать https*.

*Логин* - для ввода логина для подключения к KSM. Этот параметр появляется если выбран параметр *Использовать https*.

*Пароль* - для ввода пароля для подключения к KSM. Этот параметр появляется если выбран параметр *Использовать https*.

По умолчанию терминальная станция подключается к серверу KSM по протоколу DHCP. Для изменения параметров соединения следует (см. рис. 4.46):

- 1) →*Сеть* →*KSM*;
- 2) выбрать сетевую карту;
- 3) →[Сохранить изменения].

Для подключения терминальной станции к серверу KSM по протоколу HTTPS следует:

- 1) →*Сеть* →*KSM*;
- 2) снять галочку у параметра *Использовать DHCP* (рис.4.47);
- 3) выбрать пункт *Использовать https*;
- 4) ввести адрес сервера KSM, номер порта KSM шлюз;
- 5) ввести логин и пароль;
- 6) выбрать пункт *Обновлять ip адрес*, при необходимости;
- 7) выбрать сетевую карту;
- 8) →[Сохранить изменения].

#### Примечания:

1. При выборе параметра *Использовать DHCP* на сервере заранее должен быть размещен адрес сервера KSM-gate в опции 152 в виде текстовой строки (например: "<https://login@password:KSM-gate.address:8888/>"), не забывайте указывать порт.

2. Для использования https протокола необходимо убедиться, что версия KSM поддерживает данную функцию.

3. Для авторизации в KSM, убедитесь, что Ваша версия KSM требует авторизацию.

Информация Система Устройства **Сеть** Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка Active Directory **KSM** VPN

### Подключение к серверу Kraftway System Manager

#### Kraftway System Manager

Использовать DHCP ☐

Использовать https ☒

Сервер Kraftway System Manager

Порт KSM шлюза

Логин

Пароль

**Использовать DHCP:**  
Получать адрес KSM по DHCP

**Использовать https:**  
Убедитесь, что версия Kraftway System Manager поддерживает данную функцию

**Kraftway System Manager:**  
Авторизация в Kraftway System Manager. Убедитесь, что Ваша версия KSM требует авторизацию.

#### Обновление ip адресов в KSM

Обновлять ip адрес ☒

Выбор сетевой карты

**Обновлять ip адрес:**  
Терминальная станция будет отправлять текущий ip адрес KSM-серверу.

Сохранить изменения Выйти

Рис.4.47

#### 4.2.7.8. Вкладка VPN

Вкладка *VPN* предназначена для установки VPN-соединения. На вкладке *VPN* расположена одна функциональная кнопка [Добавить новое vpn соединение]. Кнопка предназначена для задания параметров настройки VPN соединения (рис.4.48). Ниже приводится описание параметров вкладки.

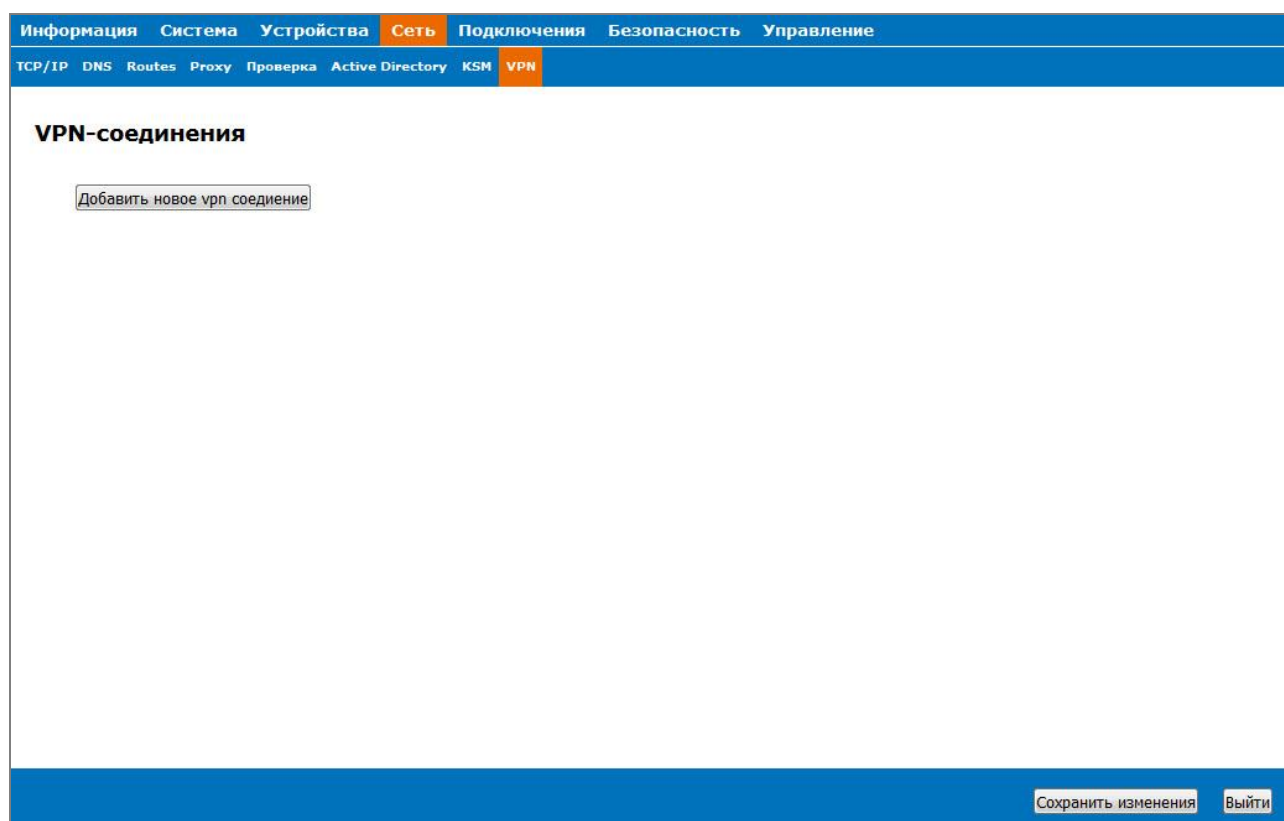


Рис. 4.48

В зависимости от выбора протокола VPN соединения, изменяются параметры настройки.

Параметры VPN соединения по протоколу *IPSec* (рис. 4.49, рис. 4.50):

*Название подключения* - для ввода названия подключения.

*Протокол* - для выбора протокола соединения.

*Сервер* - для ввода IP адреса сервера, который будет выступать в роли шлюза VPN соединения.

*Тип авторизации* - для выбора типа авторизации. Значения, принимаемые данным параметром: *Сертификат* (по умолчанию), *PSK* (Pre-Shared-Key - авторизация по ключу).

*Сертификат* - данный параметр отображается на вкладке *VPN* только после выбора типа авторизации *Сертификат* и используется для выбора сертификата авторизации. Список доступных сертификатов расположен на вкладке *Сертификаты* меню *Система* (см. п. 4.2.5.7).

*Пароль* - для ввода пароля, по которому происходит доступ к VPN соединению.



Получить виртуальный IP адрес - для получения виртуального IP адреса терминальной станции, внутри VPN.

**VPN-соединения**

**Параметры нового vpn соединения**

Название подключения	<input type="text" value="Новый"/>
Протокол	<input type="text" value="IPsec"/>
Сервер	<input type="text" value="192.168.1.1"/>
Тип авторизации	<input type="text" value="Сертификат"/>
Сертификат	<input type="text" value="default_ssl.pem"/>
Пароль	<input type="password"/>
Получить виртуальный IP адрес	<input type="checkbox"/>

**Новое соединение VPN:**  
Пробелы в названии будут вырезаны.

**Сертификаты:**  
Выберите сертификат из списка. Загрузить сертификат можно [здесь](#). Для авторизации по сертификатам используйте сертификат в формате PKCS12. Для авторизации OpenVPN по пользователю используйте сертификат CA.

**Шифрование:**  
Для pptp и l2tp : использовать MPPE  
Для OpenVPN: включить шифрование и выбрать алгоритмы.

**Шлюз по умолчанию:**  
Направлять весь трафик в данный тоннель.

Рис. 4.49

ИнформацияСистемаУстройстваСетьПодключенияБезопасностьУправление

TCP/IPDNSRoutesProxyПроверкаActive DirectoryKSMVPN

### VPN-соединения

Параметры нового vpn соединения

Название подключения

Протокол

Сервер

Тип авторизации

Пароль

Получить виртуальный IP адрес

Новый

IPsec

192.168.1.1

PSK

☐

**Новое соединение VPN:**  
Пробелы в названии будут вырезаны.

**Сертификаты:**  
Выберите сертификат из списка. Загрузить сертификат можно [здесь](#). Для авторизации по сертификатам используйте сертификат в формате PKCS12. Для авторизации OpenVPN по пользователю используйте сертификат CA.

**Шифрование:**  
Для pptp и l2tp : использовать MPPE  
Для OpenVPN: включить шифрование и выбрать алгоритмы.

**Шлюз по умолчанию:**  
Направлять весь трафик в данный тоннель.

Сохранить изменения

Выйти

Рис. 4.50

Параметры VPN соединения по протоколу *PPTP* (рис. 4.51):

ИнформацияСистемаУстройстваСетьПодключенияБезопасностьУправление

TCP/IPDNSRoutesProxyПроверкаActive DirectoryKSMVPN

### VPN-соединения

Параметры нового vpn соединения

Название подключения

Протокол

Сервер

Тип авторизации

Имя пользователя

Пароль

Шифрование

Шлюз по умолчанию

Новый

PPTP

192.168.1.1

Пользователь

☐

☐

**Новое соединение VPN:**  
Пробелы в названии будут вырезаны.

**Сертификаты:**  
Выберите сертификат из списка. Загрузить сертификат можно [здесь](#). Для авторизации по сертификатам используйте сертификат в формате PKCS12. Для авторизации OpenVPN по пользователю используйте сертификат CA.

**Шифрование:**  
Для pptp и l2tp : использовать MPPE  
Для OpenVPN: включить шифрование и выбрать алгоритмы.

**Шлюз по умолчанию:**  
Направлять весь трафик в данный тоннель.

Сохранить изменения

Выйти

Рис. 4.51

*Название подключения* - для ввода названия подключения.

*Протокол* - для выбора протокола соединения.

*Сервер* - для ввода IP адреса сервера, который будет выступать в роли шлюза VPN соединения.

*Тип авторизации* - для выбора типа авторизации. Единственное значение данного параметра при соединении по протоколу PPTP - *Пользователь*.

*Имя пользователя* - для ввода имени пользователя для подключения к VPN;

*Пароль* - для ввода пароля пользователя для подключения к VPN;

*Шифрование* - для разрешения использования шифрования при VPN соединении.

*Шлюз по умолчанию* - для передачи всего трафика в VPN соединение.

Параметры VPN соединения по протоколу *OpenVPN* (рис. 4.52 , рис. 4.53):

*Название подключения* - для ввода названия подключения.

*Протокол* - для выбора протокола соединения.

*Сервер* - для ввода IP адреса сервера, который будет выступать в роли шлюза VPN соединения.

*Тип авторизации* - для выбора типа авторизации. Значения, принимаемые данным параметром при соединении по протоколу Open VPN: *Сертификат* и *Пользователь* (по умолчанию),

*Сертификат* - для выбора сертификата авторизации. Список доступных сертификатов расположен на вкладке *Сертификаты* меню *Система* (см. п. 4.2.5.7).

*Пароль сертификата* - для ввода пароля сертификата.

*Имя пользователя* - для ввода имени пользователя для подключения к VPN. Данный параметр отображается на вкладке VPN при выборе типа авторизации *Пользователь*.

*Пароль* - для ввода пароля, по которому происходит подключение к VPN соединению. Если выбран тип авторизации *Сертификат*, то параметр *Пароль* - это пароль сертификата (рис. 4.53). Если выбран тип авторизации *Пользователь*, то параметр *Пароль* - это пароль пользователя (рис. 4.52).

*Шифрование* - основной параметр для разрешения использования шифрования при VPN соединении. По умолчанию данный параметр не выбран.

*Шифрование Авторизации* - для выбора алгоритма шифрования авторизации при VPN соединении. Данный параметр отображается на вкладке *VPN* только после выбора параметра *Шифрование*.

*Шифрование* - для выбора алгоритма шифрования при VPN соединении. Данный параметр отображается на вкладке *VPN* только после выбора основного параметра *Шифрование*.

*Защита SSL/TLS через 'HMAC firewall'* - для отключения защиты SSL/TLS через HMAC а также для выбора файла ключа HMAC. Список доступных для выбора файлов ключа появляется после загрузки сертификата (см. п. 4.2.5.7). Данный параметр отображается на вкладке *VPN* только после выбора основного параметра *Шифрование*.

Информация Система Устройства Сеть Подключения Безопасность Управление

TCP/IP DNS Routes Proxy Проверка Active Directory KSM VPN

### VPN-соединения

#### Параметры нового vpn соединения

Название подключения	Новый
Протокол	OpenVPN
Сервер	192.168.1.1
Тип авторизации	Пользователь
Сертификат	default_ssl.pem
Пароль Сертификата	
Имя пользователя	
Пароль	
Шифрование	<input checked="" type="checkbox"/>
Шифрование	SHA1
Автризации	BF-CBC
Шифрование	
Защита SSL/TLS через 'HMAC firewall'	Отключить

**Новое соединение VPN:**  
Пробелы в названии будут вырезаны.

**Сертификаты:**  
Выберите сертификат из списка. Загрузить сертификат можно [здесь](#). Для авторизации по сертификатам используйте сертификат в формате PKCS12. Для авторизации OpenVPN по пользователю используйте сертификат CA.

**Шифрование:**  
Для pptp и l2tp : использовать MPPE  
Для OpenVPN: включить шифрование и выбрать алгоритмы.

**Шлюз по умолчанию:**  
Направлять весь трафик в данный тоннель.

Сохранить изменения Выйти

Рис. 4.52

ИнформацияСистемаУстройстваСетьПодключенияБезопасностьУправление

TCP/IPDNSRoutesProxyПроверкаActive DirectoryKSMVPN

### VPN-соединения

Параметры нового vpn соединения

Название подключения

Новый

Протокол

OpenVPN

Сервер

192.168.1.1

Тип авторизации

Сертификат

Сертификат

default\_ssl.pem

Пароль

Шифрование

☒

Шифрование Автризации

SHA1

Шифрование

BF-CBC

Защита SSL/TLS через 'HMAC firewall'

Отключить

**Новое соединение VPN:**  
Пробелы в названии будут вырезаны.

**Сертификаты:**  
Выберите сертификат из списка. Загрузить сертификат можно [здесь](#). Для авторизации по сертификатам используйте сертификат в формате PKCS12. Для авторизации OpenVPN по пользователю используйте сертификат CA.

**Шифрование:**  
Для pptp и l2tp : использовать MPPE  
Для OpenVPN: включить шифрование и выбрать алгоритмы.

**Шлюз по умолчанию:**  
Направлять весь трафик в данный тоннель.

Сохранить изменения

Выйти

Рис. 4.53

Параметры VPN соединения по протоколу L2TP (рис. 4.54):

ИнформацияСистемаУстройстваСетьПодключенияБезопасностьУправление

TCP/IPDNSRoutesProxyПроверкаActive DirectoryKSMVPN

### VPN-соединения

Параметры нового vpn соединения

Название подключения

Новый

Протокол

L2TP

Сервер

192.168.1.1

Тип авторизации

Пользователь

Имя пользователя

Пароль

Шифрование

☐

Шлюз по умолчанию

☐

**Новое соединение VPN:**  
Пробелы в названии будут вырезаны.

**Сертификаты:**  
Выберите сертификат из списка. Загрузить сертификат можно [здесь](#). Для авторизации по сертификатам используйте сертификат в формате PKCS12. Для авторизации OpenVPN по пользователю используйте сертификат CA.

**Шифрование:**  
Для pptp и l2tp : использовать MPPE  
Для OpenVPN: включить шифрование и выбрать алгоритмы.

**Шлюз по умолчанию:**  
Направлять весь трафик в данный тоннель.

Сохранить изменения

Выйти

Рис. 4.54

*Название подключения* - для ввода названия подключения.

*Протокол* - для выбора протокола соединения.

*Сервер* - для ввода IP адреса сервера, который будет выступать в роли шлюза VPN соединения.

*Тип авторизации* - для выбора типа авторизации. Значения, принимаемые данным параметром: *Пользователь* (установлено по умолчанию).

*Имя пользователя* - для ввода имени пользователя для подключения к VPN.

*Пароль* - для ввода пароля пользователя для подключения к VPN.

*Шифрование* - для разрешения использования шифрования при VPN соединении.

*Шлюз по умолчанию* - для передачи всего трафика в VPN соединение.

Для установки нового соединения VPN по протоколу *IPSec* следует:

- 1) →*Сеть* →*VPN*;
- 2) →[Добавить новое vpn соединение] ;
- 3) ввести название VPN соединения, выбрать протокол *IPSec*;
- 4) ввести IP адрес сервера;
- 5) выбрать тип авторизации;
- 6) выбрать сертификат;
- 7) ввести пароль;
- 8) выбрать пункт *Получить виртуальный IP адрес*, при необходимости;
- 9) →[Сохранить изменения].

Для установки нового соединения VPN по протоколу *PPTP* следует:

- 1) →*Сеть* →*VPN*;
- 2) →[Добавить новое vpn соединение];
- 3) ввести название VPN соединения, выбрать протокол *PPTP*;
- 4) ввести IP адрес сервера;
- 5) ввести имя пользователя;
- 6) ввести пароль;
- 7) выбрать пункт *Шифрование*, при необходимости;
- 8) выбрать пункт *Шлюз по умолчанию*, при необходимости;
- 9) →[Сохранить изменения].

Для установки нового соединения VPN по протоколу *OpenVPN* следует:

- 1) →*Сеть* →*VPN*,
- 2) →[Добавить новое vpn соединение];

- 3) ввести название VPN соединения, выбрать протокол *OpenVPN*;
- 4) ввести IP адрес сервера;
- 5) выбрать тип авторизации;
- 6) выбрать сертификат;
- 7) ввести пароль сертификата (для типа авторизации *Пользователь*);
- 8) ввести имя пользователя (для типа авторизации *Пользователь*);
- 5) ввести пароль (для типа авторизации *Пользователь* - пароль пользователя, для типа авторизации *Сертификат* - пароль сертификата);
- 9) выбрать пункт *Шифрование*, при необходимости;
- 10) →[Сохранить изменения].

Для установки нового соединения VPN по протоколу *L2TP* следует:

- 1) →*Сеть* →*VPN*;
- 2) →[Добавить новое vpn соединение];
- 3) ввести название VPN соединения, выбрать протокол *L2TP*;
- 4) ввести IP адрес сервера;
- 5) ввести имя пользователя;
- 6) ввести пароль;
- 7) выбрать пункт *Шифрование*, при необходимости;
- 8) выбрать пункт *Шлюз по умолчанию*, при необходимости;
- 9) →[Сохранить изменения].

Примечания:

1. При установлении нового VPN соединения пробелы в названии будут вырезаны.
2. Загрузить свой сертификат можно по ссылке «здесь», расположенной в правой части вкладки *VPN* (см. рис. 4.54 Вкладка *VPN*). При переходе по данной ссылке загружается меню *Система* вкладка *Сертификаты* (см. п. 4.2.5.7).
3. Для авторизации по сертификатам используйте сертификат в формате PKCS12.
4. Для авторизации с использованием протокола *OpenVPN* по пользователю используйте сертификат *CA*.
5. Для протоколов *PPTP* и *L2TP* используется *MPPE* шифрование.
6. Для протокола *OpenVPN* предусмотрена возможность включения и выбора алгоритмов шифрования.



#### 4.2.8. Пункт меню Подключения

Пункт меню *Подключения* содержит 2 вкладки: *Автоподключение*, *Сценарии*.

##### 4.2.8.1. Вкладка Автоподключение

Вкладка *Автоподключение* предназначена для: установки и выбора сценария для автоматического подключения к необходимому терминальному серверу, выполнения проверки системы для запуска сценария (рис. 4.55, рис. 4.56). Ниже приводится описание параметров вкладки.



Информация	Система	Устройства	Сеть	Подключения	Безопасность	Управление
Автоподключение	Сценарии					

### Автоматическое подключение

#### Выбор подключения по умолчанию

Подключение по умолчанию	<input type="text" value="отключено"/>	<b>Подключение по умолчанию:</b> Выбрать сценарий для автоматического подключения возможно только после его создания на вкладке "Сценарии".
		<b>Проверить получение IP :</b> Прежде чем попробовать запустить сценарий авто подключения, проверить получен ли IP.
		<b>Количество проверок:</b> По умолчанию IP проверяется 3 раза с паузой в 3 секунды. Количество проверок можно увеличить.
		<b>Прочие проверки :</b> Для проверки что всё готово для запуска сценария вы можете использовать <a href="#">другие проверки</a> .

Сохранить изменения Выйти

Рис.4.55

Информация	Система	Устройства	Сеть	Подключения	Безопасность	Управление
Автоподключение	Сценарии					

### Автоматическое подключение

#### Выбор подключения по умолчанию

Подключение по умолчанию	<input type="text" value="Подключение 1 - Новый"/>	<b>Подключение по умолчанию:</b> Выбрать сценарий для автоматического подключения возможно только после его создания на вкладке "Сценарии".
Действие после окончания сессии	<input type="text" value="Перезагрузить"/>	
Проверить, получен ли IP-адрес	<input type="checkbox"/>	
Количество проверок	<input type="text"/>	

Сохранить изменения

Рис. 4.56

Описание параметров:

*Подключение по умолчанию* - для установки запрета на использование автоматического подключения к серверу, а также - разрешения при выборе заранее созданных сценариев для автоматических подключений. Значения параметра: «отключено» (установлено по умолчанию), «<Название сценария 1>, ..., <Название сценария n>».

*Действие после окончания сессии* - для выбора реакции терминальной станции на выход пользователя из терминальной сессии при автоматическом подключении. Значения параметра: «Перезагрузить» (установлено по умолчанию), «Выключить».

*Проверить, получен ли IP-адрес* - для проверки получения IP-адреса ТС.

*Количество проверок* - для установки количества проверок получения IP-адреса ТС.

Для установки и выбора сценария для автоматического подключения к необходимому серверу следует:

- 1) →Подключения →Автоподключение;
- 2) выбрать в списке требуемый сценарий для автоматического подключения;
- 3) выбрать в списке требуемое действие после закрытия сессии;
- 4) выполнить проверку получения IP-адреса ТС, при необходимости;
- 5) установить количество проверок получения IP-адреса ТС, при необходимости;
- 6) →[Сохранить изменения].

Примечания:

1. Для выбора необходимого сценария для автоматического подключения вначале следует создать хотя бы один сценарий на вкладке *Сценарии* (→Подключения →Сценарии).

2. Перед запуском сценария автоматического подключения необходимо проверить получен ли IP-адрес терминальной станцией.

3. Проверка получения IP-адреса ТС по умолчанию выполняется 3 раза с интервалом 3 секунды.

4. Провести дополнительные тесты сетевых настроек можно по ссылке «*другие проверки*», расположенной в правой части вкладки *Автоподключение* (см. рис. 4.56 Вкладка VPN). После выбора данной ссылки открывается вкладка *Проверка консоли*

администратора (см. п. 4.2.7.5), (→Сеть →Проверка), в которой администратору предлагается задать дополнительные проверки, которые будут всегда выполняться перед запуском пользовательского интерфейса.

#### 4.2.8.2. Вкладка Сценарии

Вкладка *Сценарии* предназначена для создания сценариев подключения к необходимым терминальным серверам (рис. 4.57). Ниже приводится описание параметров вкладки.

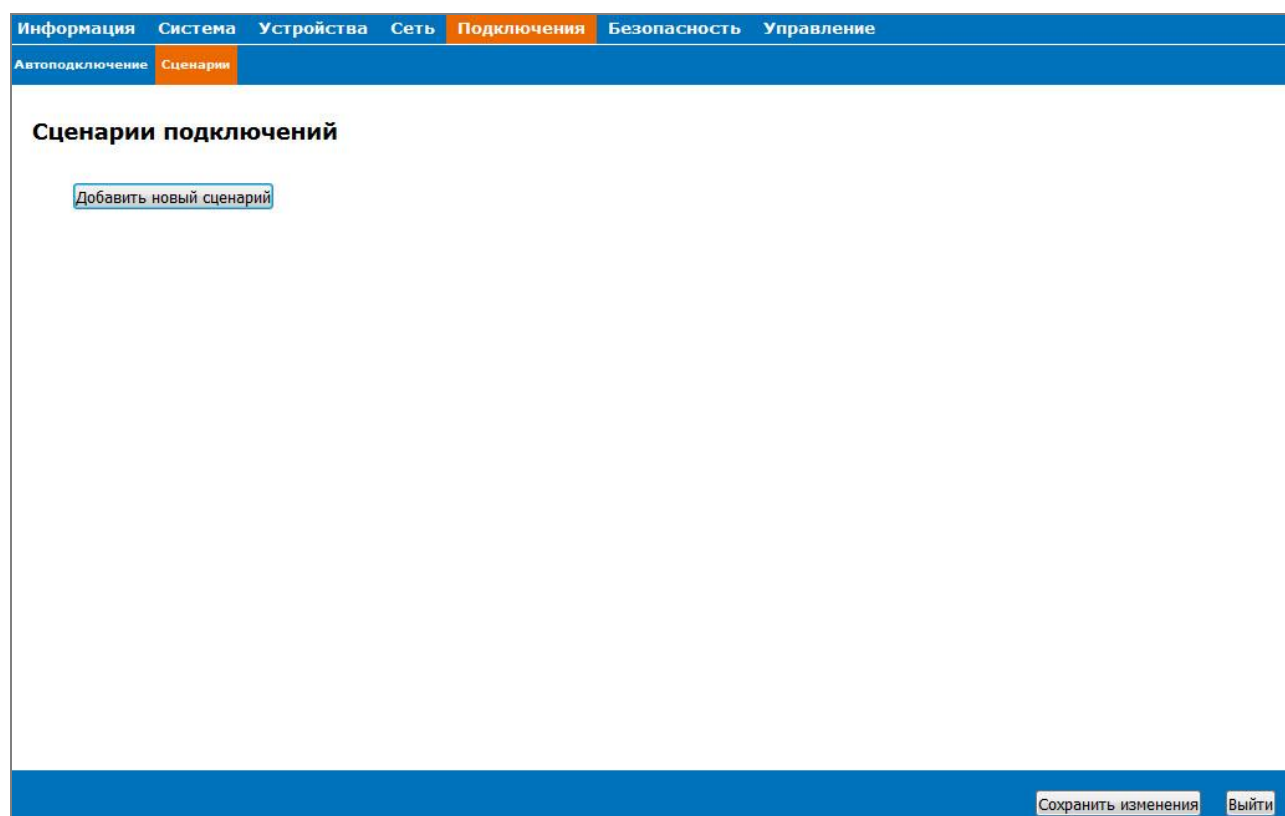


Рис. 4.57

В зависимости от выбора протокола сценария, изменяются параметры настройки.

Параметры сценария для создания сессии со значением параметра *протокол*: «Windows terminal server (freerdp)» и «Windows terminal server (rdesktop)» (рис. 4.58, рис. 4.59):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Имя пользователя* - для ввода имени пользователя.

*Пароль* - для ввода пароля пользователя.

*Спрашивать пароль* - для установки необходимости запроса пароля. Данный параметр по умолчанию не выбран.

*Глубина цвета* - для выбора глубины цвета в открываемой терминальной сессии. Значения параметра: «256 цветов (8 бит)», «Тысячи цветов (16 бит)» (установлено по умолчанию), «Миллионы цветов (24 бита)», «Реальные цвета (32 бита)».

*Раскладка клавиатуры* - для выбора раскладки клавиатуры. Значения параметра: «Английская», «Русская». Данный параметр выводится при создании сценария подключения по RDP протоколу.

Рис. 4.58

**Звук** - для включения входящего звукового потока в терминальной сессии. Параметр по умолчанию не выбран. Данный параметр выводится при создании сценария подключения со значением параметра *протокол*: «Windows terminal server (freerdp)».

**Видео** - для использования ресурсов видеоадаптера терминальной станции. Параметр по умолчанию не выбран. Данный параметр выводится при создании сценария подключения со значением параметра *протокол*: «Windows terminal server (freerdp)».

**RemoteFX** - для использования ресурсов видеоадаптера терминального сервера. Параметр по умолчанию не выбран. Данный параметр выводится при создании сценария подключения со значением параметра *протокол*: «Windows terminal server (freerdp)».

**Сжатие** - для установки поддержки сжатия данных.

**Программа** - для автоматического запуска требуемой программы в RDP сессии. Синтаксис значения - «полный путь к исполняемому файлу программы», например, C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE. Данный параметр выводится при создании сценария подключения по RDP протоколу.

Информация Система Устройства Сеть **Подключения** Безопасность Управление

Автоподключение **Сценарии**

### Сценарии подключений

#### Параметры нового сценария

Название сценария	Новый
Протокол	Windows terminal server (rdesktop)
Сервер	192.168.1.1
Имя пользователя	
Пароль	
Спрашивать пароль	<input type="checkbox"/>
Глубина цвета	Тысячи цветов (16 бит)
Раскладка клавиатуры	Английская
Сжатие	<input type="checkbox"/>
Программа	

**Новый сценарий:**  
Пробелы в именах сценариев будут вырезаны.

Сохранить изменения Выйти

Рис. 4.59

Параметры сценария для создания сессии со значением параметра *протокол*: «Сервер Citrix» (рис. 4.60):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Имя пользователя* - для ввода имени пользователя.

*Пароль* - для ввода пароля доступа к терминальному серверу.

*Шифрование* - для выбора алгоритма шифрования с различной длиной ключа. Значения параметра: «Basic» (установлено по умолчанию), «RC5 (128 bit - Login only)», «RC5 (40 bit)», «RC5 (56 bit)», «RC5 (128 bit)».

Рис. 4.60

Параметры сценария для создания сессии со значением параметра *протокол*: «Сервер X Window (Unix)» (рис. 4.61):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

Информация Система Устройства Сеть **Подключения** Безопасность Управление

Автоподключение **Сценарии**

### Сценарии подключений

#### Параметры нового сценария

Название сценария	<input type="text" value="Новый"/>	<b>Новый сценарий:</b> Пробелы в именах сценариев будут вырезаны.
Протокол	<input type="text" value="Сервер X Window (UNIX)"/>	
Сервер	<input type="text" value="192.168.1.1"/>	

Сохранить изменения Выйти

Рис. 4.61

Параметры сценария для создания сессии со значением параметра *протокол*: «Сервер NX» и «Сервер SSH» и (рис. 4.62, рис. 4.63):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Имя пользователя* - для ввода имени пользователя.

Информация	Система	Устройства	Сеть	Подключения	Безопасность	Управление
Автоподключение	Сценарии					

### Сценарии подключений

#### Параметры нового сценария

Название сценария	<input type="text" value="Новый"/>	<b>Новый сценарий:</b> Пробелы в именах сценариев будут вырезаны.
Протокол	<input type="text" value="Сервер NX"/>	
Сервер	<input type="text" value="192.168.1.1"/>	
Имя пользователя	<input type="text"/>	

Рис. 4.62

Информация	Система	Устройства	Сеть	Подключения	Безопасность	Управление
Автоподключение	Сценарии					

### Сценарии подключений

#### Параметры нового сценария

Название сценария	<input type="text" value="Новый"/>	<b>Новый сценарий:</b> Пробелы в именах сценариев будут вырезаны.
Протокол	<input type="text" value="Сервер SSH"/>	
Сервер	<input type="text" value="192.168.1.1"/>	
Имя пользователя	<input type="text"/>	

Рис. 4.63



Параметры сценария для создания сессии со значением параметра *протокол*: «X2Go server» (рис. 4.64):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Имя пользователя* - для ввода имени пользователя.

*Тип сессии* - для выбора типа сессии. Параметр определяет какой оконный менеджер будет открыт со стороны сервера.

Рис. 4.64

Параметры сценария для создания сессии со значением параметра *протокол*: «Сервер VNC» (рис 4.65):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Пароль* - для ввода пароля доступа к терминальному серверу.

Информация Система Устройства Сеть **Подключения** Безопасность Управление

Автоподключение **Сценарии**

**Сценарии подключений**

**Параметры нового сценария**

Название сценария Новый

Протокол Сервер VNC

Сервер 192.168.1.1

Пароль

**Новый сценарий:**  
Пробелы в именах сценариев будут вырезаны.

Сохранить изменения Выйти

Рис. 4.65

Параметры сценария для создания сессии со значением параметра *протокол*: «Web-приложение (будет открыто в Firefox)» (рис. 4.66):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*URL* - для автоматического открытия требуемого ресурса сети Интернет по заданному URL-адресу. Синтаксис значения - «URL-адрес требуемого ресурса», например, [www.kraftway.ru](http://www.kraftway.ru).

*Режим киоска* - для функционирования браузера Firefox в полноэкранном режиме. Данный параметр по умолчанию не выбран.

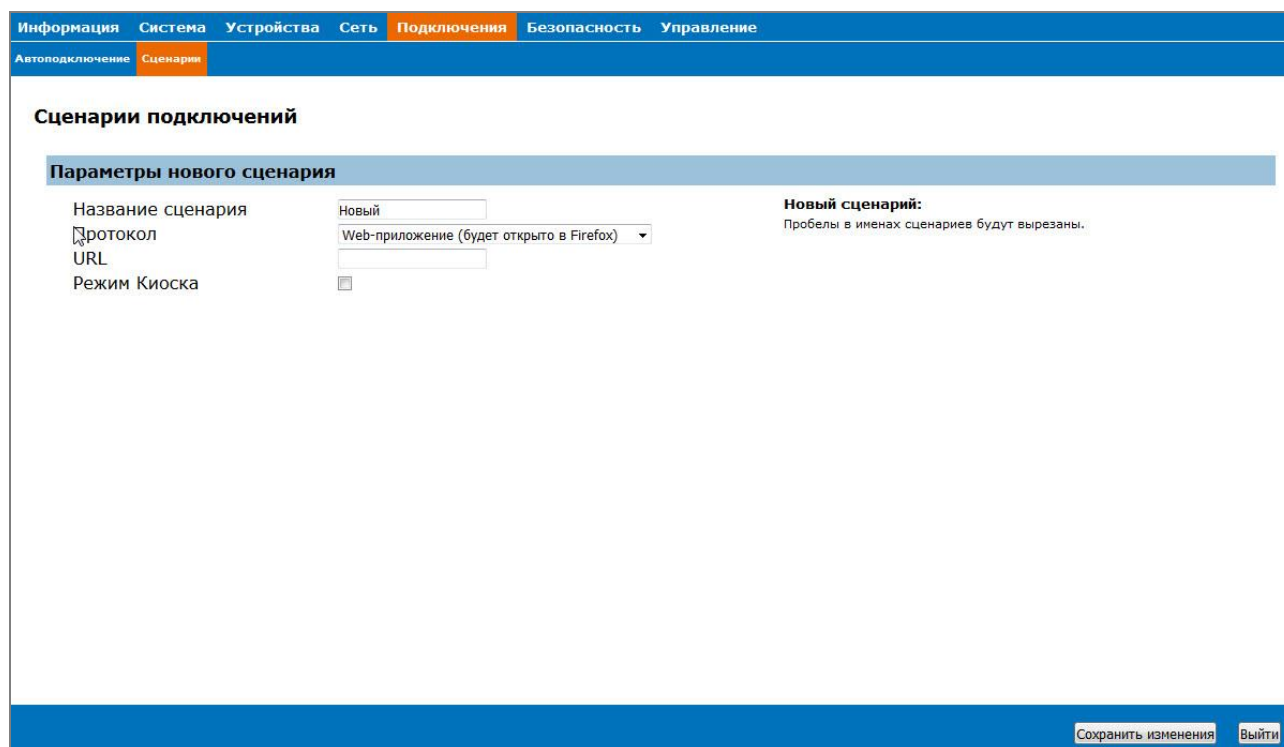


Рис. 4.66

Параметры сценария для создания сессии со значением параметра *протокол*: «Web-приложение (будет открыто в Chrome)» (рис. 4.67):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*URL* - для автоматического открытия требуемого ресурса сети Интернет по заданному URL-адресу. Синтаксис значения - «URL-адрес требуемого ресурса», например, [www.kraftway.ru](http://www.kraftway.ru).

*Режим киоска* - для функционирования браузера Chrome в полноэкранный режиме. Данный параметр по умолчанию не выбран.

*Отключение правой клавиши мыши и горячих клавиш* - для отключения горячих клавиш и правой клавиши мыши. Данный параметр по умолчанию не выбран.

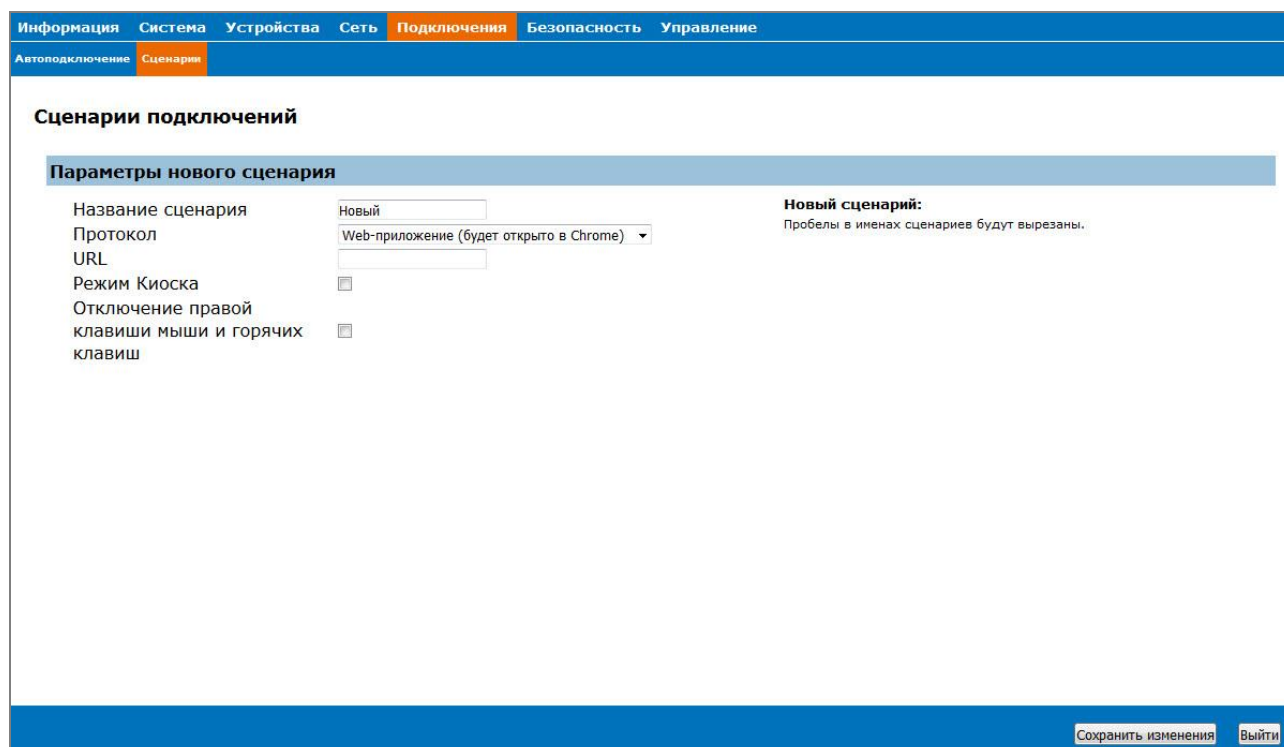


Рис. 4.67

Параметры сценария для создания сессии со значением параметра *протокол*: «VMWare View (RDP)» и «VMWare View (PCOIP)» (рис. 4.68, рис. 4.69):

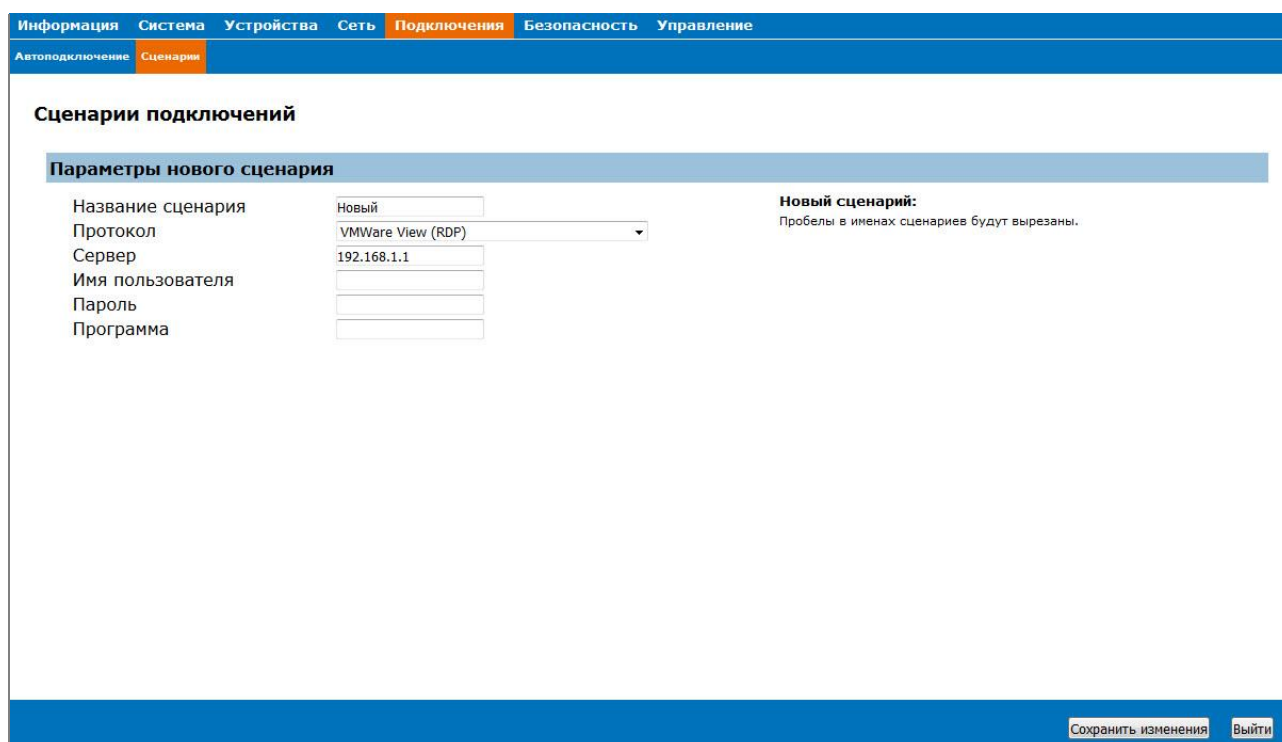
*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Имя пользователя* - для ввода имени пользователя.

*Пароль* - для ввода пароля пользователя.



Информация Система Устройства Сеть **Подключения** Безопасность Управление

Автоподключение **Сценарии**

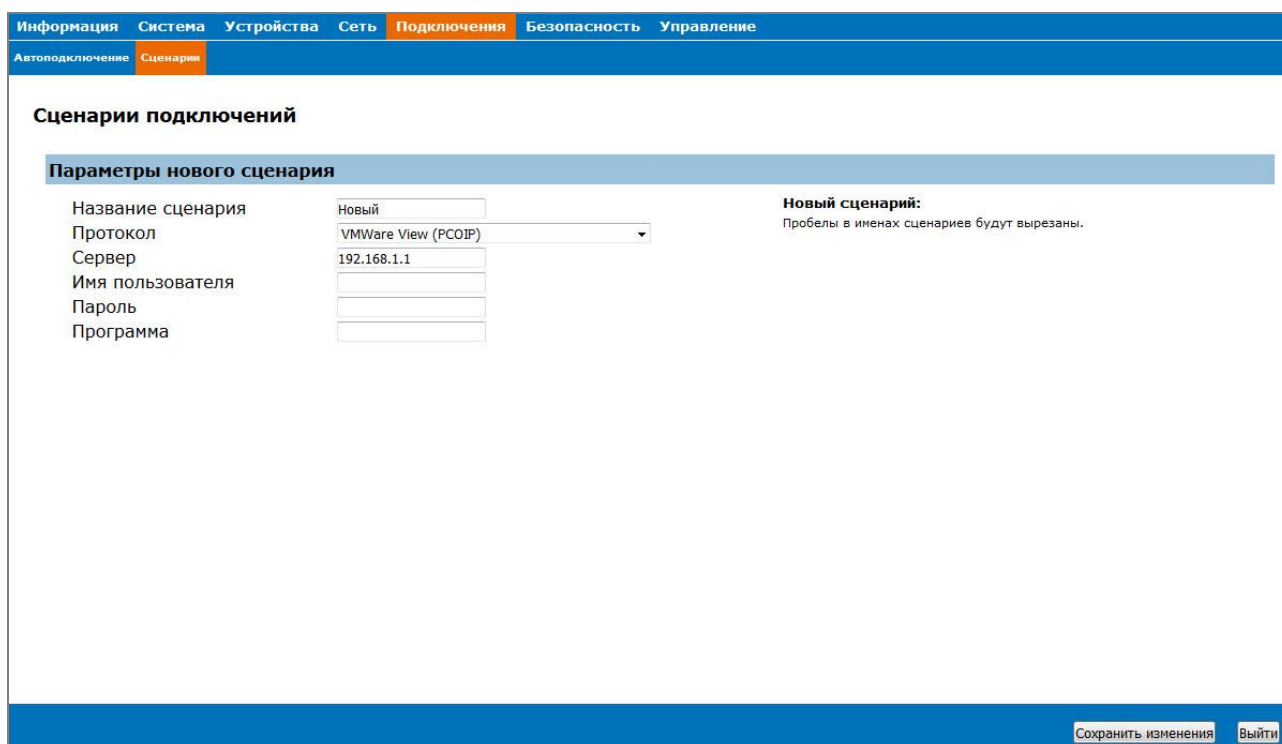
### Сценарии подключений

#### Параметры нового сценария

Название сценария	Новый	<b>Новый сценарий:</b> Пробелы в именах сценариев будут вырезаны.
Протокол	VMWare View (RDP)	
Сервер	192.168.1.1	
Имя пользователя		
Пароль		
Программа		

Сохранить изменения Выйти

Рис. 4.68



Информация Система Устройства Сеть **Подключения** Безопасность Управление

Автоподключение **Сценарии**

### Сценарии подключений

#### Параметры нового сценария

Название сценария	Новый	<b>Новый сценарий:</b> Пробелы в именах сценариев будут вырезаны.
Протокол	VMWare View (PCOIP)	
Сервер	192.168.1.1	
Имя пользователя		
Пароль		
Программа		

Сохранить изменения Выйти

Рис. 4.69

Параметры сценария для создания сессии со значением параметра *протокол*: «Spice (SPICE)» (рис. 4.70):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

*Сервер* - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

*Пароль* - для ввода пароля доступа к терминальному серверу.

*Звук* - для включения входящего звукового потока в терминальной сессии. Параметр по умолчанию не выбран.

*Порт* - для ввода порта терминального сервера.

Информация Система Устройства Сеть Подключения Безопасность Управление

Автоподключение Сценарии

**Сценарии подключений**

**Параметры нового сценария**

Название сценария	Новый	<b>Новый сценарий:</b> Пробелы в именах сценариев будут вырезаны.
Протокол	Spice (SPICE)	
Сервер	192.168.1.1	
Пароль		
Звук	<input type="checkbox"/>	
Порт	5900	

Сохранить изменения Выйти

Рис. 4.70

Параметры сценария для создания сессии со значением параметра *протокол*: «OVDC (Oracle Virtual Desktop Client)» (рис. 4.71):

*Название сценария* - для ввода названия сценария подключения (вводится без пробелов).

*Протокол* - для выбора протокола открываемой терминальной сессии пользователя.

**Сервер** - для ввода IP-адреса или имени терминального сервера, используемого при подключении.

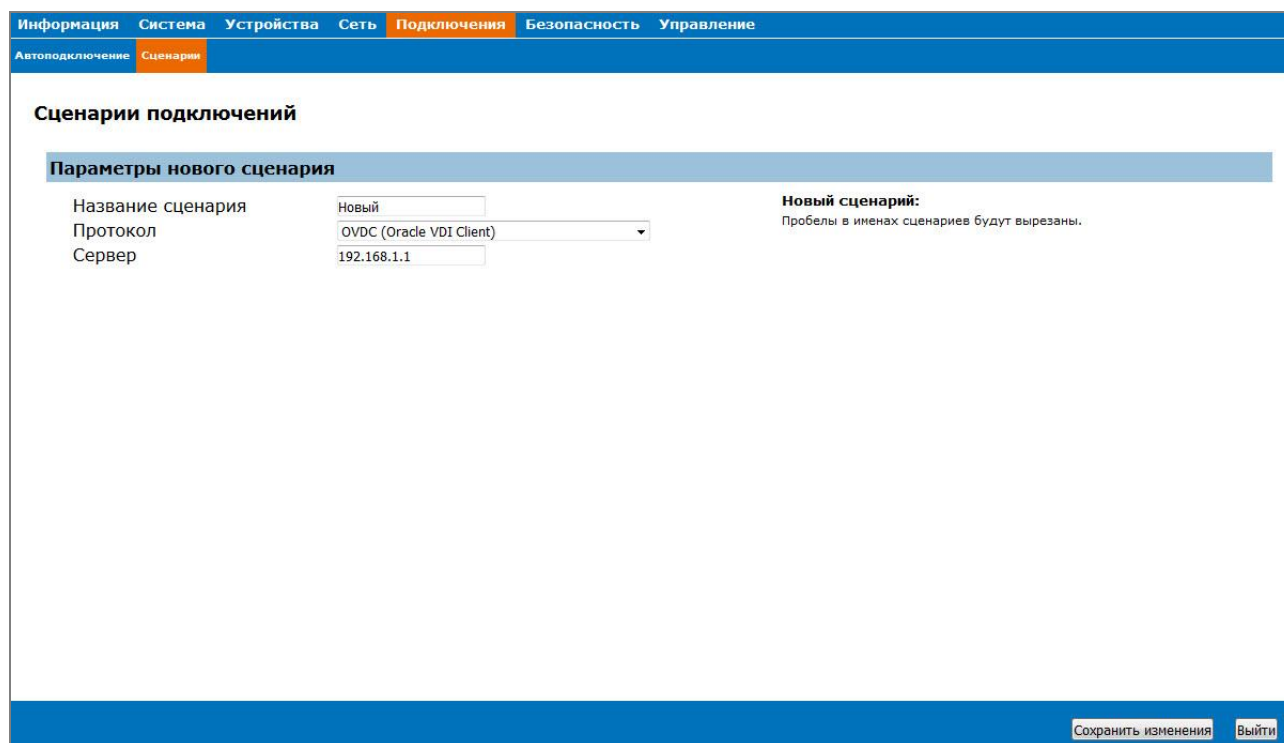


Рис. 4.71

**Примечания:**

1. Следует помнить, что пробелы в названии сценария подключения после его создания удаляются, например: введенное название - Windows (RDP), название сценария после его создания - Windows(RDP).

2. Следует помнить, что в том случае, когда в качестве сценария для автоматического подключения выбран сценарий, при создании которого использовалось значение «Web-приложение (будет открыто в Firefox)», после включения терминальной станции пользователю предоставляется возможность работы только в web-браузере Mozilla Firefox. Для значения «Web-приложение (будет открыто в Chrome)» - возможность работы только в web-браузере Google Chrome, соответственно.

Для создания сценария подключения к терминальному серверу следует:

- 1) → *Подключения* → *Сценарии*;
- 2) → [Добавить новый сценарий], на вкладку *Сценарии* выводятся параметры для настройки подключения;
- 3) внести необходимые значения в соответствующие поля;

- 4) →[Сохранить изменения], на вкладке *Сценарии* обновляется информация и выводится дополнительная функциональная кнопка [Удалить сценарий] (рис.4.72);
- 5) →[Добавить новый сценарий] при необходимости;
- 6) →[Удалить сценарий] при необходимости;
- 7) внести изменения в только что созданный сценарий подключения при необходимости;
- 8) →[Сохранить изменения] при условии выполнения каких-либо новых операций на вкладке *Сценарии* после создания первого сценария подключения.

Информация Система Устройства Сеть Подключения Безопасность Управление

Автоподключение Сценарии

**Сценарии подключений: Настройки сохранены. Для применения большинства настроек необходима перезагрузка.**

[Добавить новый сценарий](#)

**Параметры сценария 1**

Название сценария	Новый
Протокол	Windows terminal server (freerdp)
Сервер	192.168.1.1
Имя пользователя	
Пароль	
Спрашивать пароль	<input type="checkbox"/>
Глубина цвета	Тысячи цветов (16 бит)
Раскладка клавиатуры	Английская
Сжатие	<input type="checkbox"/>
Звук	<input type="checkbox"/>
Видео	<input type="checkbox"/>
RemoteFX	<input type="checkbox"/>
Программа	

[Удалить сценарий](#)

**Изменения:**  
После изменения параметров сценария не забудьте нажать кнопку "Сохранить изменения" внизу страницы.

[Сохранить изменения](#) [Выйти](#)

Рис. 4.72

#### 4.2.9. Пункт меню Безопасность

Пункт меню *Безопасность* содержит 3 вкладки: *Ограничение доступа*, *Kaspersky*, *SSL*.

##### 4.2.9.1. Вкладка Ограничение доступа



Вкладка *Ограничение доступа* предназначена для разрешения доступа к веб-интерфейсу терминальной станции (рис.4.73).

Для ограничения доступа к веб-интерфейсу терминальной станции следует:

- 1) → *Безопасность* → *Ограничение доступа*;
- 2) ввести IP-адреса, для которых будет разрешен доступ к веб-интерфейсу ТС;
- 3) → [Добавить].

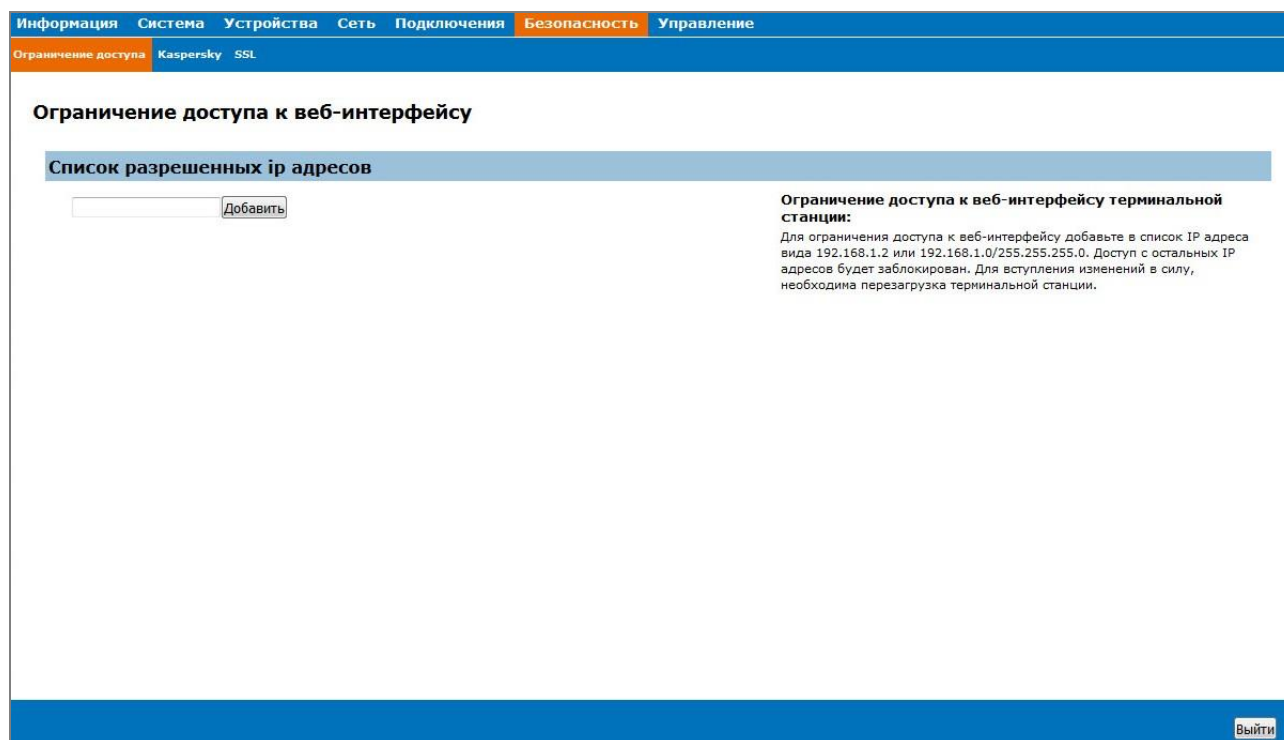


Рис. 4.73

#### 4.2.9.2. Вкладка Kaspersky

Вкладка *Kaspersky* предназначена для настройки работы Агента Антивируса Касперского (рис. 4.74). Ниже приводится описание параметров вкладки.

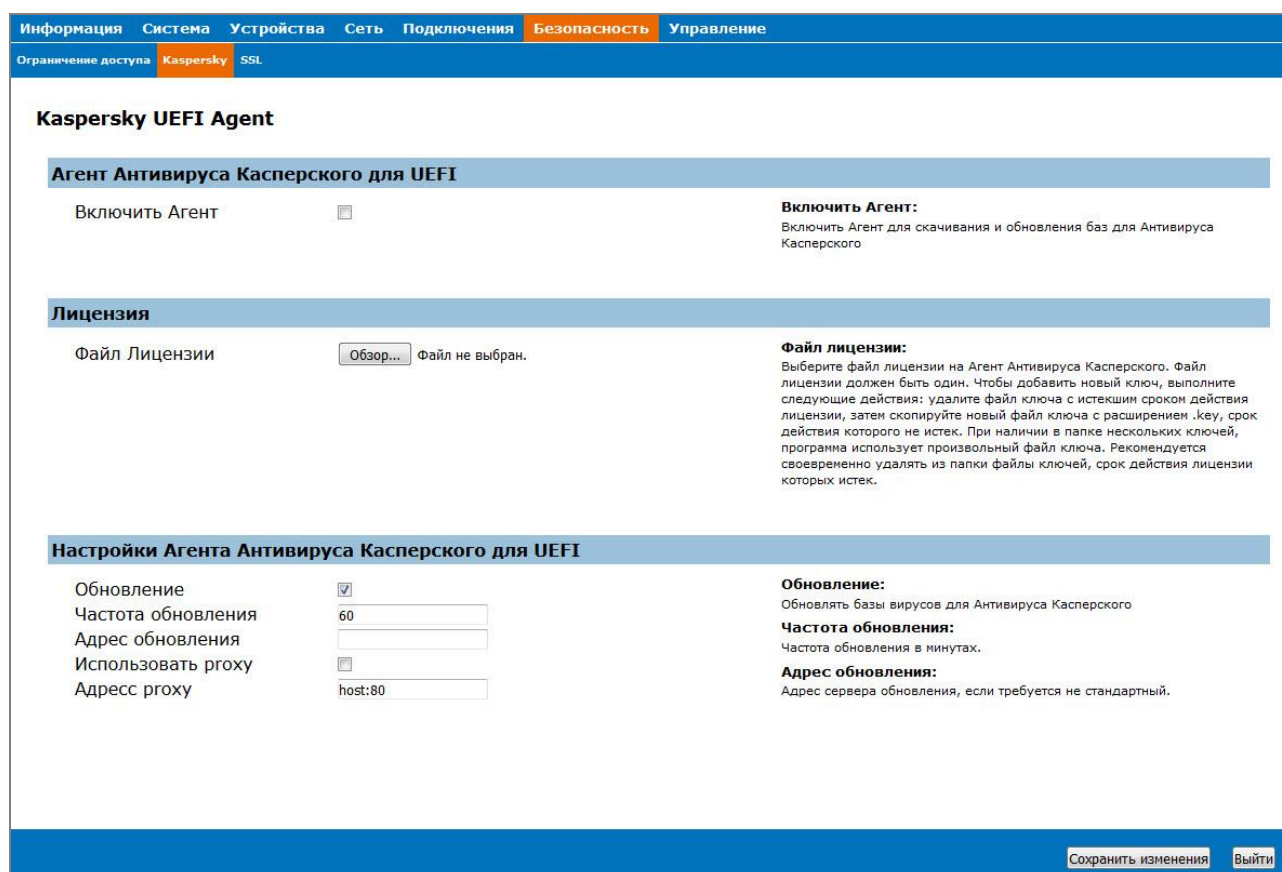


Рис. 4.74

*Включить Агент* - для включения/выключения Агента Антивируса Касперского. Данный параметр по умолчанию не выбран.

*Файл лицензии* - для подключения файла лицензии Агента Антивируса Касперского.

*Обновление* - для включения обновления базы вирусов Антивируса Касперского. Данный параметр выбран по умолчанию.

*Частота обновления* - для задания периода обновления базы вирусов (в минутах).

*Адрес обновления* - для задания адреса сервера обновления, если требуется не стандартный. *Использовать проху* - для разрешения использования прокси-сервера. Данный параметр по умолчанию не выбран.

*Адрес проху* - для ввода IP-адреса или имени прокси-сервера.

Для включения Агента Антивируса Касперского следует:

- 1) → *Безопасность* → *Kaspersky*;
- 2) выбрать параметр *Включить Агент*;
- 3) указать расположение файла лицензии;

4) выполнить настройки Агента Антивируса Касперского;

5) →[Сохранить изменения], в разделе параметров *Лицензия* отобразится описание текущей лицензии Агента Kaspersky (рис.4.75).

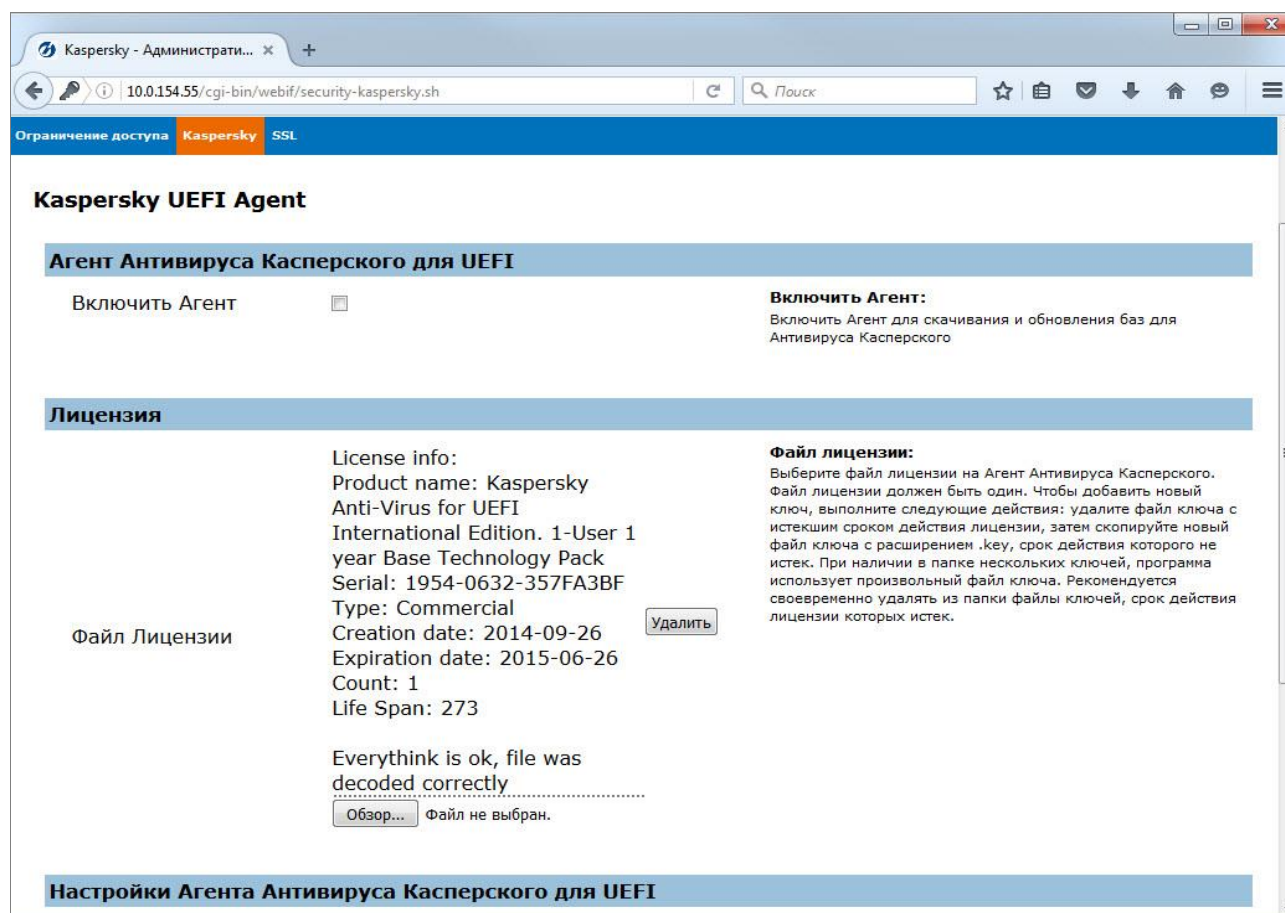


Рис.4.75

Примечания:

1. Для добавления нового ключа лицензии, выполните следующие действия: удалите файл ключа с истекшим сроком действия лицензии, затем скопируйте новый файл ключа с расширением .key, срок действия которого не истек.

2. При наличии в папке нескольких ключей, программа использует произвольный файл ключа.

3. ВНИМАНИЕ: РЕКОМЕНДУЕТСЯ СВОЕВРЕМЕННО УДАЛЯТЬ ФАЙЛЫ КЛЮЧЕЙ, СРОК ДЕЙСТВИЯ КОТОРЫХ ИСТЕК.

#### 4.2.9.3. Вкладка SSL

Вкладка *SSL* предназначена для разрешения использования защищенного соединения с терминальной станцией (рис. 4.76). Ниже приводится описание параметров вкладки.

Информация Система Устройства Сеть Подключения **Безопасность** Управление

Ограничение доступа Kaspersky SSL

### Защищенное соединение по протоколу SSL

#### Протокол SSL

Активировать защищенное соединение ☒

Запретить незащищенное соединение ☐

**Активировать защищенное соединение:**  
Рекомендуется запретить незащищенное соединение. В этом случае войти в интерфейс терминальной станции будет возможно только по протоколу https

#### Выбор сертификата

Выбор сертификата default\_ssl.pem

**Сертификат:**  
По умолчанию используется самоподписанный сертификат с 1024-битным шифрованием. Для использования стороннего сертификата, необходимо загрузить сертификат на [странице загрузки сертификатов](#). Сертификат должен иметь расширение .pem или p12. Файл сертификата должен содержать в себе ключ.

Сохранить изменения Выйти

Рис. 4.76

*Активировать защищенное соединение* - для разрешения защищенного соединения с терминальной станцией. Данный параметр выбран по умолчанию.

*Запретить незащищенное соединение* - для запрета незащищенного соединения с терминальной станцией. После выбора данного параметра войти в интерфейс терминальной станции будет возможно только по протоколу HTTPS. Данный параметр по умолчанию не выбран. Выводится на вкладку *SSL* только после выбора параметра *Активировать защищенное соединение*.

*Выбор сертификата* - для выбора цифрового сертификата. По умолчанию выбран самоподписанный сертификат с 1024-битным шифрованием «default\_ssl.pem».

Примечания:

1. Для загрузки стороннего сертификата нужно перейти по ссылке «*на странице загрузки сертификатов*», расположенной в правой части вкладки *SSL* (рис. 4.76). При переходе по данной ссылке загружается меню *Система* вкладка *Сертификаты* (см. рис. 4.25).

2. Сертификат должен иметь расширение *.pem* или *.p12*.

3. Файл сертификата должен содержать в себе ключ.

Для настройки защищенного соединения по протоколу *SSL* следует:

1) →*Безопасность* →*SSL*;

2) выполнить необходимые настройки;

3) →[*Сохранить изменения*].

#### 4.2.10. Пункт меню *Управление*

Пункт меню *Управление* содержит вкладки: *Управление* и *Настройки*.

##### 4.2.10.1. Вкладка *Управление*

На вкладке *Управление* содержатся три функциональные кнопки управления питанием терминальной станции: [*Перезагрузить терминал*] - кнопка, предназначенная для выполнения программной перезагрузки терминальной станции, [*Перезагрузить терминал в безопасный режим*] - кнопка, предназначенная для выполнения программной перезагрузки терминальной станции в безопасный режим, [*Выключить терминал*] - кнопка, предназначенная для выполнения программного выключения терминальной станции (рис. 4.77).

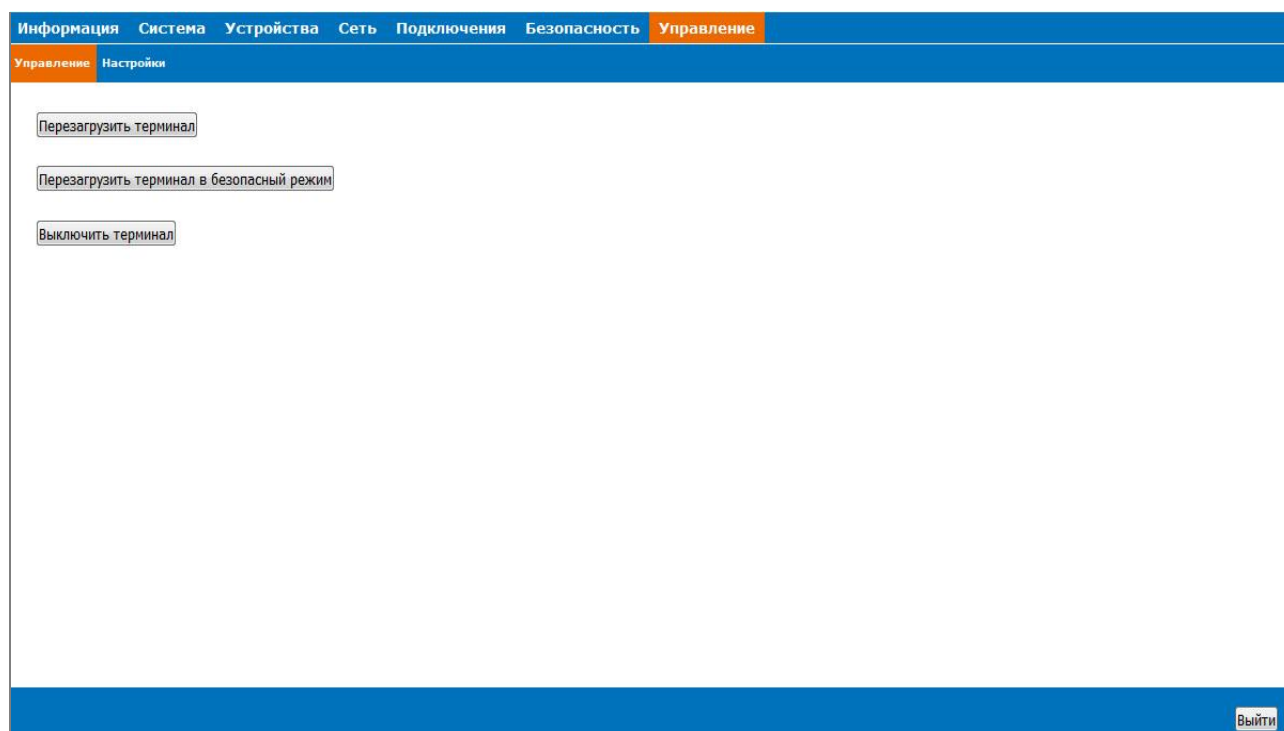


Рис. 4.77

Для выполнения настройки на вкладке *Управление* следует:

- 1) → *Управление*→*Управление*;
- 2) →[Перезагрузить терминал] при необходимости;
- 3) →[Перезагрузить терминал в безопасном режиме] при необходимости;
- 4) →[Выключить терминал] при необходимости.

#### 4.2.10.2. Вкладка Настройки

На вкладке *Настройки* содержатся параметры восстановления и сброса настроек терминальной станции (рис. 4.78).

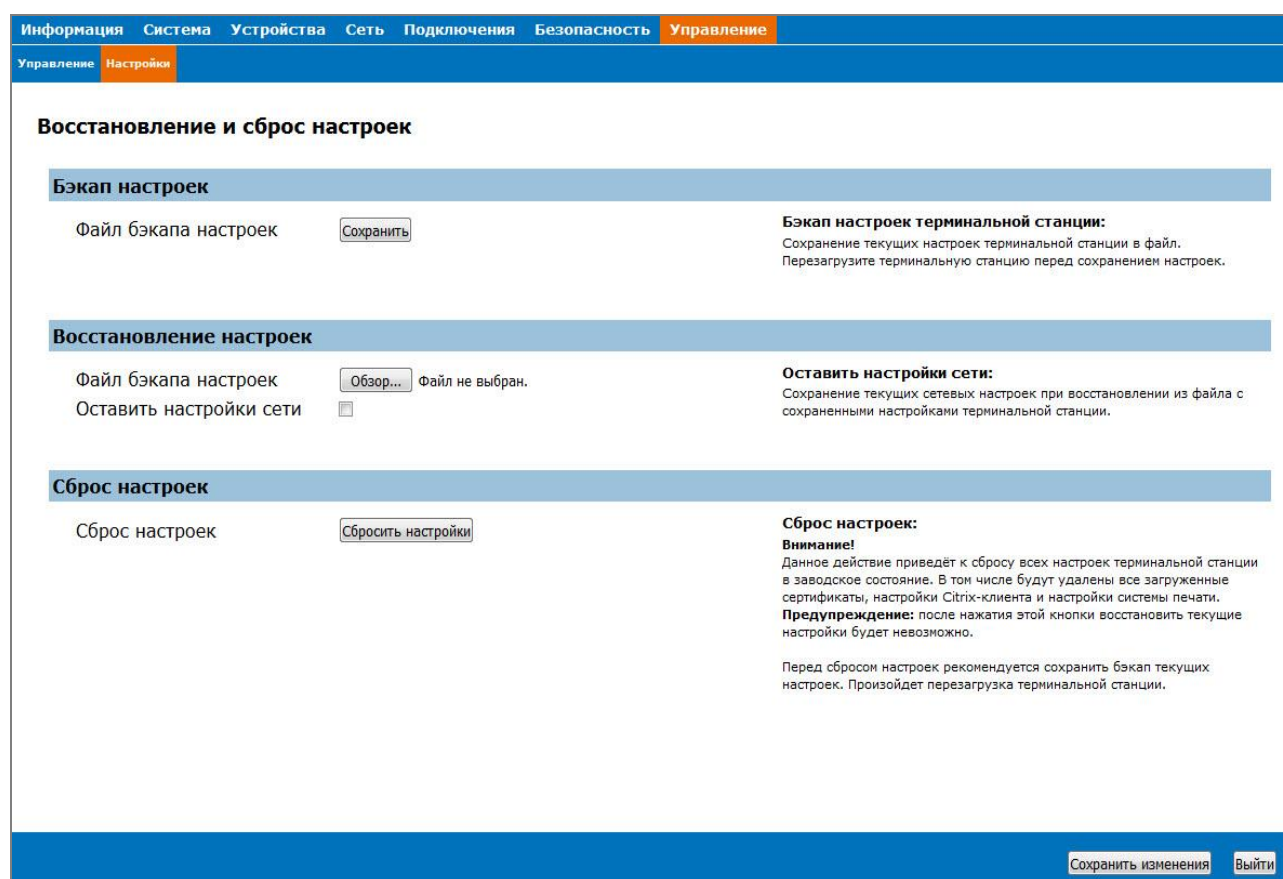


Рис. 4.78

Описание параметров:

*Файл бэкапа настроек* (бэкап настроек) - параметр предназначен для сохранения текущих настроек терминальной станции.

*Файл бэкапа настроек* (восстановление настроек) - параметр предназначен для восстановления настроек из файла с сохраненными настройками терминальной станции.

*Оставить настройки сети* - параметр предназначен для сохранения текущих сетевых настроек при восстановлении из файла с сохраненными настройками терминальной станции.

*Сброс настроек* - параметр предназначен для сброса всех настроек терминальной станции до заводских установок.

Для создания и сохранения настроек в файл backup следует:

1) → *Управление* → *Настройки*;

2) → [Сохранить] происходит сохранение файла и на экран выводится окно *Открытие backup\_имя файла бэкапа* (рис.4.79);



3) →[Сохранить файл].



Рис. 4.79

После завершения сохранения на вкладку выводится информация об успешном сохранении настроек (рис.. 4.80).

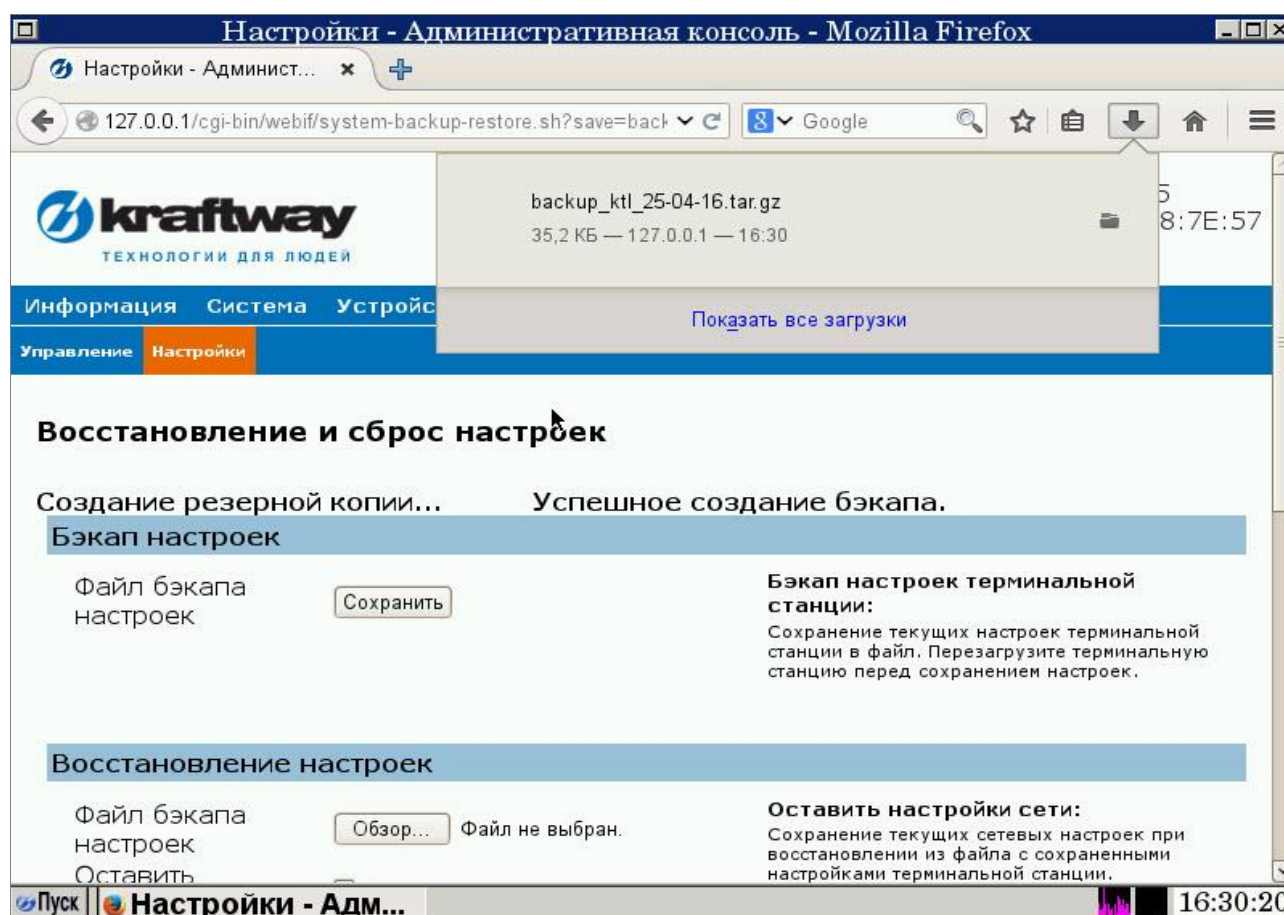


Рис. 4.80

4) →[Сбросить настройки], при необходимости сброса настроек;

5) →[Сохранить изменения].



Для восстановления настроек из файла backup следует:

- 1) → *Управление* → *Настройки*;
- 2) → [Обзор], выбрать файл (рис. 4.81);
- 3) → [Открыть], на вкладке появится строка с названием выбранного файла;
- 4) выбрать параметр *Оставить настройки сети* (при необходимости);
- 5) → [Сохранить изменения].

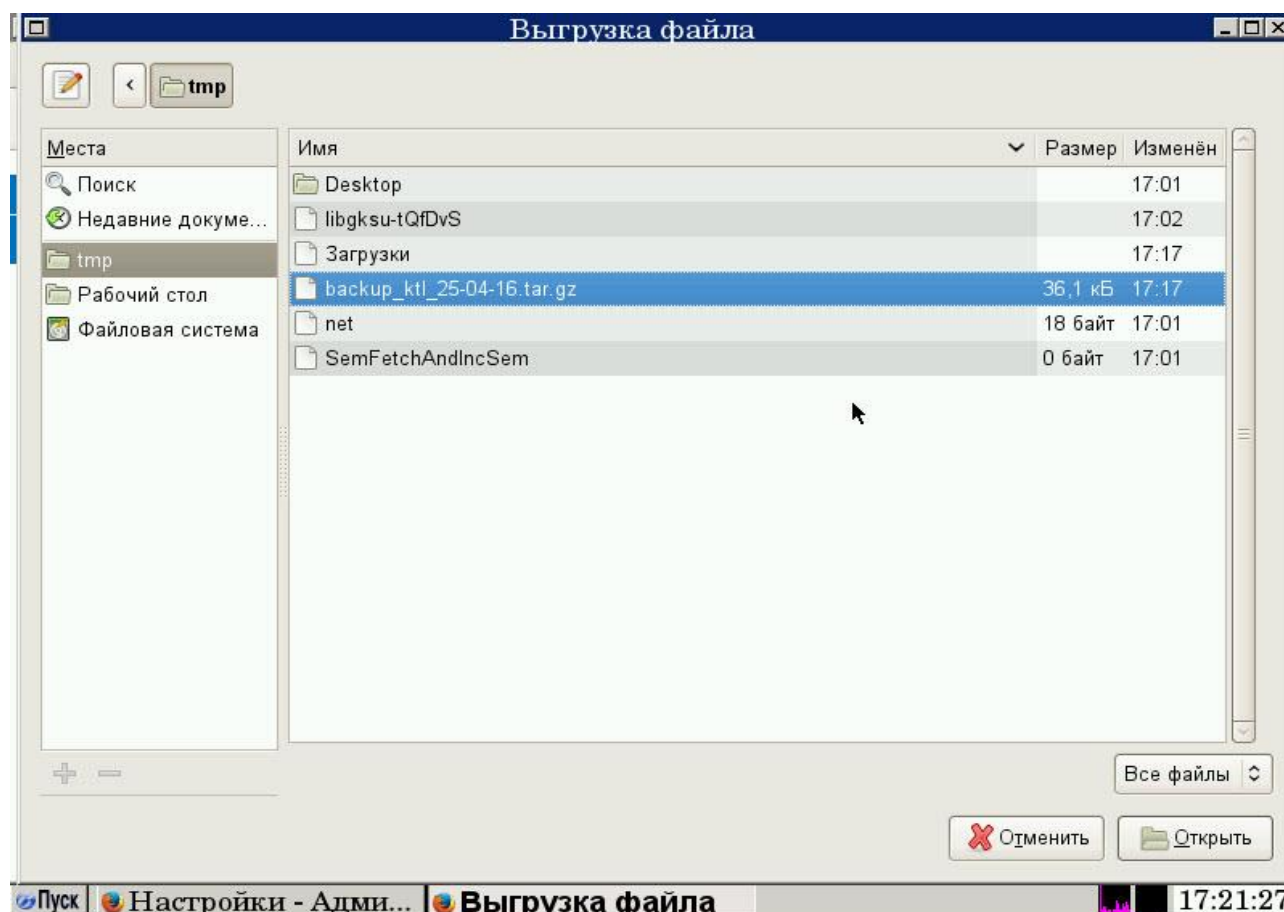


Рис. 4.81

После сохранения настроек терминал автоматически перезагрузится.

Примечания:

1. Перед сохранением текущих настроек терминальной станции требуется перезагрузка терминальной станции.

2. Следует помнить, что при сбросе настроек терминальной станции будут удалены все загруженные сертификаты, настройки Citrix-клиента и настройки системы печати.

3. ВНИМАНИЕ: ПОСЛЕ СБРОСА НАСТРОЕК ВОССТАНОВИТЬ ТЕКУЩИЕ НАСТРОЙКИ БУДЕТ НЕВОЗМОЖНО, ПРИ ОТСУТСТВИИ ФАЙЛА БЭКАПА НАСТРОЕК.

4. ВНИМАНИЕ: ПЕРЕД СБРОСОМ НАСТРОЕК РЕКОМЕНДУЕТСЯ СОХРАНИТЬ РЕЗЕРВНУЮ КОПИЮ ТЕКУЩИХ НАСТРОЕК ТЕРМИНАЛЬНОЙ СТАНЦИИ.

5. Файл бэкапа настроек можно применять в качестве шаблона при установке ПО «KTL» с USB-диска (файл бэкапа настроек копируется на USB-диск, во время установки ПО он будет распакован и установлен в качестве настроек для новой терминальной станции или при обновлении прошивки ПО терминальной станции).

4.3. Настройка клиентского окружения терминальной станции с удалённого компьютера через VNC сессию

Администратору предоставляется возможность настройки клиентского окружения терминальной станции через VNC сессию. Для данного вида настройки требуется установка на компьютер, с которого предполагается выполнять настройки терминальной станции, VNC-клиента (VNC Viewer). VNC-сервер входит в состав ПО терминальной станции.

Далее по тексту приводится описание настройки клиентского окружения терминальной станции через VNC-сессию. Для установки VNC-сессии с терминальной станцией используется VNC-клиент VNC Viewer for Windows версий 5.2.2 и выше для ОС Windows, разработанный компанией RealVNC Ltd. Исполняемый файл данного VNC-клиента можно скачать с сайта <http://www.realvnc.com/download/viewer>.

Для выполнения настройки клиентского окружения терминальной станции с удалённого компьютера через VNC сессию следует:

- 1) разрешить удалённое управление терминалом на вкладке VNC в консоли администратора (см. п. 4.2.5.4);
- 2) перезагрузить терминальную станцию в безопасный режим (см. п. 3.1.2);
- 3) запустить VNC-клиент VNC Viewer с удалённого компьютера, нажав два раза левой клавишей мыши на исполняемом файле *VNC-Viewer-5.2.2-Windows-32bit.exe*, на экран выводится окно VNC Viewer (рис. 4.82);
- 4) ввести IP-адрес терминальной станции в поле *VNC Server*;
- 5) →[Connect], на экран вводится окно VNC Viewer: Authentication (рис.4.83);

6) ввести пароль администратора в поле *Password*: (пароль администратора - admin, значение, используемое по умолчанию);

7) →[OK], на экран вводится окно *ts080027058837:0 - VNC Viewer* VNC-клиента (см. рис. 4.84), где «ts080027058837» - имя терминальной станции типа «ts<MAC-адрес>»;

8) выполнить требуемые настройки с помощью пунктов системного меню рабочего стола пользователя.

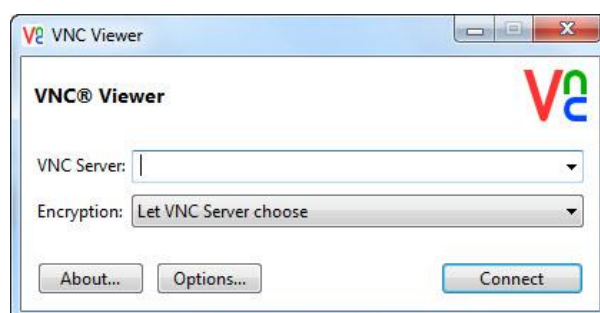


Рис. 4.82

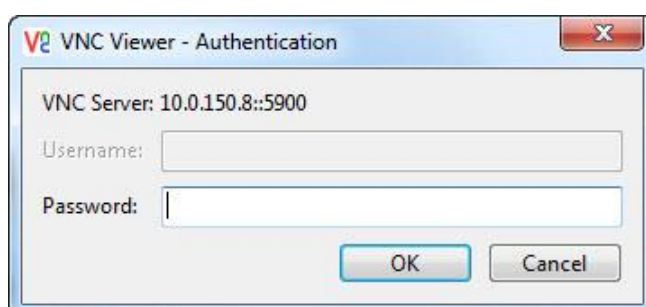


Рис. 4.83

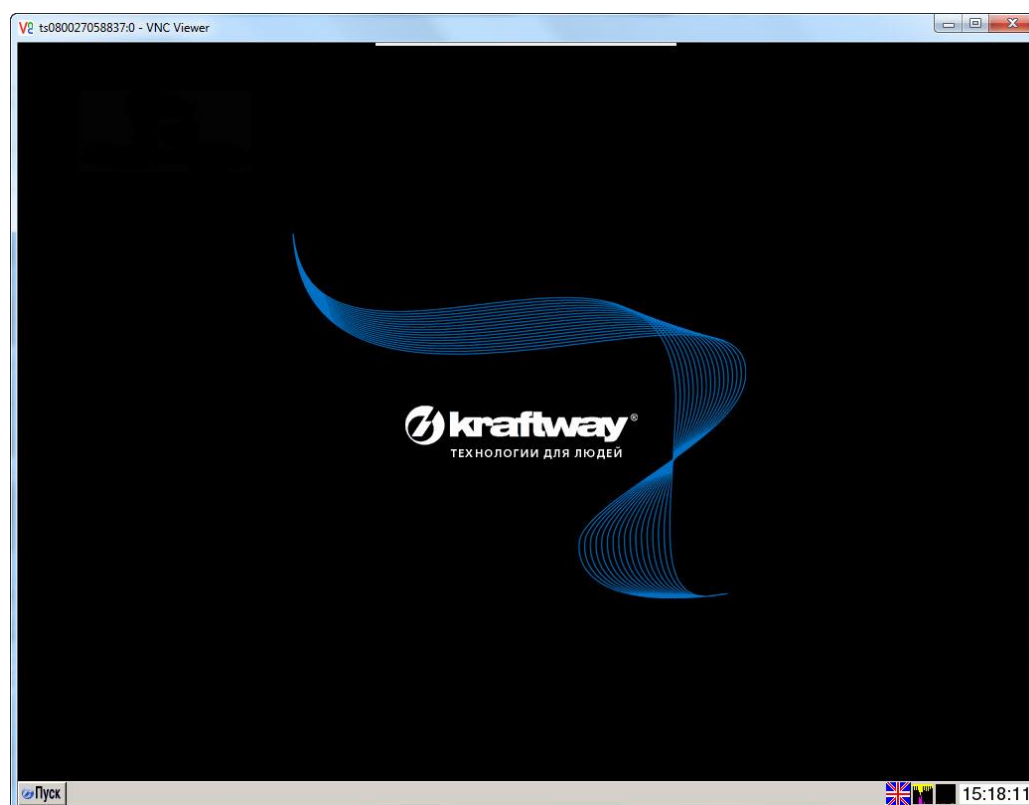


Рис. 4.84

#### 4.4. Установка и настройка печатающих устройств

Пользователю предоставляется возможность использования сетевых и локальных USB-, LPT-принтеров в RDP и Citrix сессиях ОС Windows, при работе с программами, входящими в пользовательское ПО терминальной станции, а также терминальной станции и подключённого к ней принтера в качестве принт-сервера. Работа с печатающими устройствами в перечисленных сессиях идентична работе с ними в Windows среде. Установка и настройка печатающих устройств в основном выполняется с помощью системы печати CUPS 1.7.5 (Common UNIX Printing System).

Примечания:

1. Следует помнить, что использование локальных USB/LPT-принтеров, подключённых к терминальной станции, при установке терминальных RDP сессий возможно только при разрешении перенаправления локального принтера в терминальную сессию (см. п. 4.2.6.1).

2. В Windows сессиях локальный принтер становится доступным при условии наличия у пользователя прав на перенаправление принтера в сессию на терминальном сервере.

3. Предоставляется возможность для уже установленных печатающих устройств использование конкретно определённого драйвера, установленного на Windows-сервере. Для того, чтобы воспользоваться данной возможностью, следует ввести в строку параметра *Название драйвера Windows* на вкладке *Устройства* пункта меню *Устройства* (см.рис. 4.28, п. 4.2.6.1) графической консоли администратора название требуемого драйвера. Название драйвера можно выбрать из списка драйверов параметра *Драйвер:* окна *<Название принтера> Свойства* (см. рис. 4.85). Название драйвера вводится в строку параметра *Название драйвера Windows* без изменений, т.е. так, как оно представлено в списке параметра *Драйвер*.

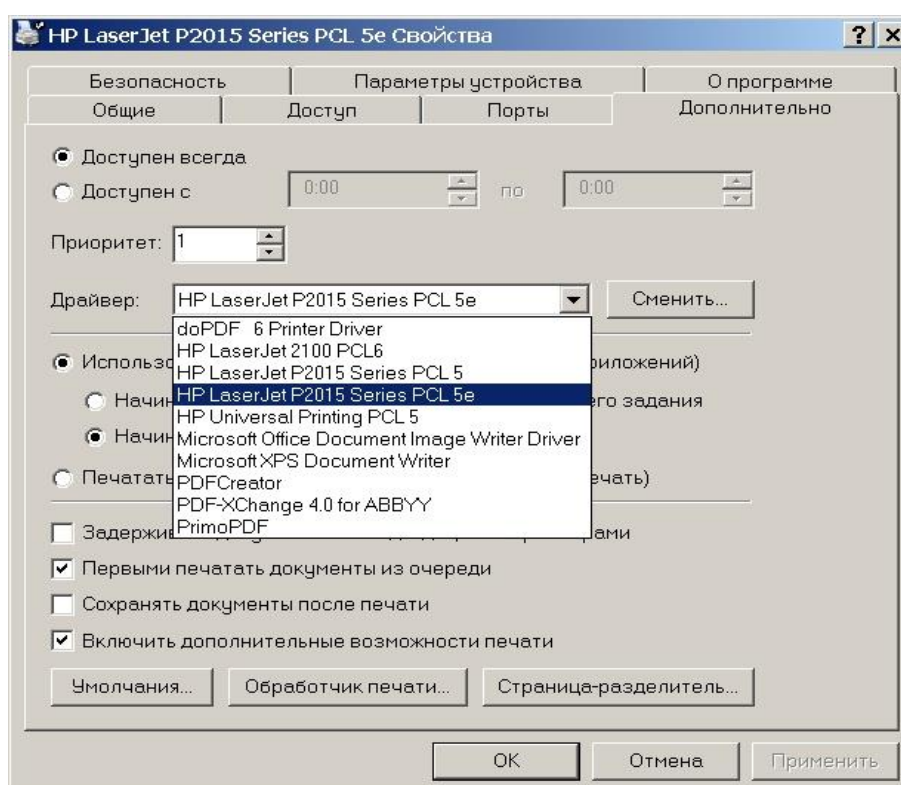


Рис. 4.85

#### 4.4.1. Установка локального принтера

Перед выполнением данного этапа необходимо подключить устанавливаемый принтер к порту (USB/LPT) терминальной станции и включить его.

Для выполнения установки нового локального принтера следует:

- 1) →[Пуск] на панели задач;
- 2) выбрать пункт *Настроить принтеры* в появившемся системном меню, на экран выводится окно *Home - CUPS 2.0.1 - Mozilla Firefox* (рис.4.86) или перейти по ссылке «Настроить принтеры» на вкладке «Устройства» (см. рис. 4.28);
- 3) →[Администрирование], на экран выводится окно *Администрирование* (см. рис.4.87);

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## CUPS 2.0.1

CUPS — поддерживающая большинство стандартов, свободная подсистема печати, разрабатываемая компанией [Apple Inc.](#) для операционной системы Mac OS® X и других UNIX®-подобных операционных систем.

### CUPS для пользователей

- [Введение в CUPS](#)
- [Печать из командной строки](#)
- [Форум пользователей](#)

### CUPS для администраторов

- [Добавление принтеров и групп](#)
- [Управление доступом](#)
- [Использование сетевых принтеров](#)
- [Справочник по cupsd.conf](#)

### CUPS для разработчиков

- [Введение в разработку CUPS](#)
- [CUPS API](#)
- [Разработка фильтров и модулей](#)
- [API доступа по HTTP и IPP](#)
- [Форум разработчиков](#)

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис.4.86

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Администрирование

### Принтеры

- [Добавить принтер](#)
- [Найти новый принтер](#)
- [Управление принтерами](#)

### Сервер

- [Редактировать конфигурационный файл](#)
- [Показать журнал заданий](#)
- [Показать журнал ошибок](#)
- [Показать журнал страниц](#)

### Группы

- [Добавить группу](#)
- [Управление группами](#)

### Параметры сервера:

[Дополнительные параметры ►](#)

- ☒ Разрешить совместный доступ к принтерам, подключенным к этой системе
  - ☒ Разрешить печать из интернет
- ☒ Разрешить удаленное администрирование
- ☐ Разрешить пользователям отменять любое задание(не только их собственные)
- ☐ Сохранять отладочную информацию в журнале

[Сохранить](#)

### Задания

- [Управление заданиями](#)

### Подписка по RSS

- [Добавить подписку по RSS](#)

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.



Рис. 4.87

- 4) →[Добавить принтер], на экран выводится окно *Добавление принтера* (рис. 4.88);
- 5) выбрать из списка порт, к которому подключен принтер, если принтер определился автоматически - выбрать соответствующий пункт;
- 6) →[Продолжить];
- 7) На вкладке выводятся новые параметры (рис.4.89);
- 8) ввести имя принтера в поле *Название* в соответствии с приведёнными правилами (поля *Расположение*, *Описание* заполнять необязательно);
- 9) если необходимо, поставить галочку в поле *Разрешить совместный доступ к этому принтеру*;
- 10) →[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.90);

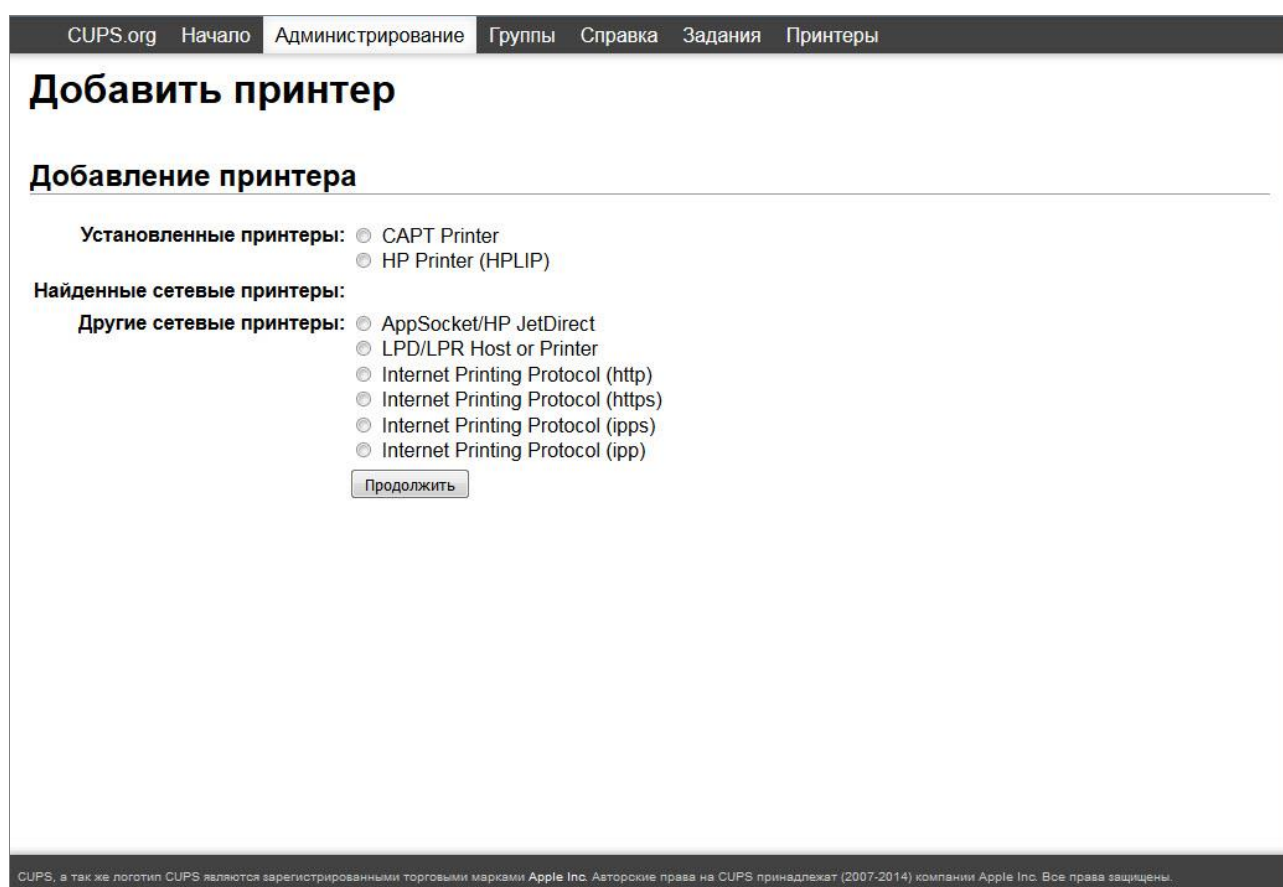


Рис. 4.88



CUPS.org Начало Администрирование Группы Справка Задания Принтеры

## Добавить принтер

### Добавление принтера

**Название:**   
(может содержать любые символы, кроме "/", "# и пробела)

**Описание:**   
(расширенное описание, например, "HP LaserJet с дуплексной печатью")

**Расположение:**   
(месторасположение принтера, например, "Кабинет 55")

**Подключение:**

**Совместный доступ:** ☐ Разрешить совместный доступ к этому принтеру

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.89

CUPS.org Начало Администрирование Группы Справка Задания Принтеры

## Добавить принтер

### Добавление принтера

**Название:** HP\_LaserJet\_1200

**Описание:**

**Расположение:**

**Подключение:**

**Совместный доступ:** Нет совместного доступа к этому принтеру

**Создать:** HP

**Модель:**   
HP LaserJet 1200 Foomatic/lj5gray (en)  
HP LaserJet 1200 Foomatic/ljet4 (en)  
HP LaserJet 1200 Foomatic/Postscript (en)  
HP LaserJet 1200 Foomatic/pxlmono (en)  
HP LaserJet 1200 pci3, hpcups 3.14.10 (en)  
HP LaserJet 1200n, hpcups 3.14.10 (en)  
HP LaserJet 1220 Foomatic/lj4dith (en)  
HP LaserJet 1220 Foomatic/lj5gray (en)  
HP LaserJet 1220 Foomatic/ljet4 (en)  
HP LaserJet 1220 Foomatic/Postscript (en)

**или использовать файл PPD:**

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.90

- 11) выбрать драйвер для принтера в списке параметра *Модель*;
- 12) →[Добавить принтер], на экран выводится окно *Требуется аутентификация* (рис. 4.91);

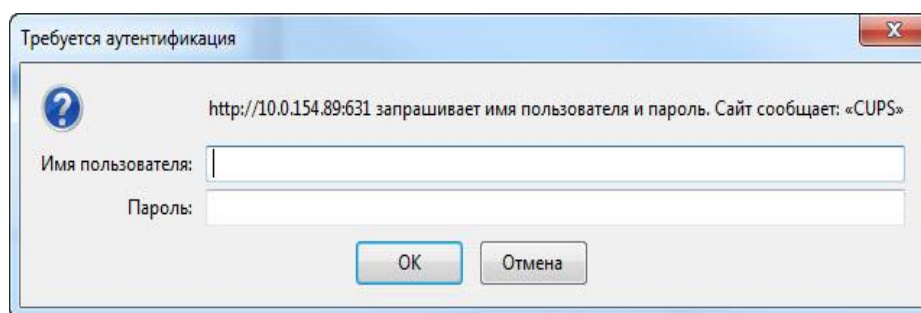


Рис. 4.91

- 13) ввести имя и пароль администратора в соответствующие поля (имя администратора CUPS - admin, пароль - admin, значения, используемые по умолчанию), на вкладке *Администрирование* выводятся новые параметры (рис. 4.92);
- 14) нажать левой клавишей мыши на кнопку [*Сохранить параметры*] название нового принтера, на экран выводится окно *<Название принтера>* (рис.4.93);
- 15) →[Обслуживание] →[Печатать пробную страницу] для распечатки тестовой страницы;
- 16) проверить визуально выполнение распечатки тестовой страницы и её качества, что подтверждает правильную установку, и работу добавленного принтера;
- 17) →[x], расположенную в верхнем правом углу окна web-браузера Mozilla Firefox для закрытия системы печати CUPS.

CUPS.org Начало Администрирование Группы Справка Задания Принтеры

## Настроить параметры принтера

### Установить параметры по умолчанию для HP\_LaserJet\_1200

[General](#) [Параметры установлены](#) [Баннеры](#) [Политики](#)

**General**

Media Size: A4 210x297mm

Double-Sided Printing: Off

Media Source: Auto-Select

Print Quality: Normal

CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.92

CUPS.org Начало Администрирование Группы Справка Задания **Принтеры**

## HP\_LaserJet\_1200

**HP\_LaserJet\_1200 (ожидает, принимает задания, нет совместного доступа )**

Обслуживание Администрирование

**Описание:**

**Расположение:**

**Драйвер:** HP LaserJet 1200 pcl3, hpcups 3.14.10 (цветной, дуплексная печать)

**Подключение:** http://hostname:631/ipp/

**По умолчанию:** job-sheets=none, none media=iso\_a4\_210x297mm sides=one-sided

### Задания

Поиск HP\_LaserJet\_1200:

Нет заданий.

CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.93

#### 4.4.2. Настройка локального принтера

Для выполнения настройки установленного локального принтера в системе CUPS следует:

- 1) выполнить действия 1, 2, описанные в пункте 4.4.1.;
- 2) выбрать вкладку *Принтеры* (рис.4.94);
- 3) выбрать принтер, который необходимо настроить;
- 4) →[<Название принтера>], на экран выводится окно состояния и настройки принтера (рис. 4.95);
- 5) →[Администрирование] →[Установить параметры по умолчанию] для вывода страницы настройки принтера (рис. 4.96);

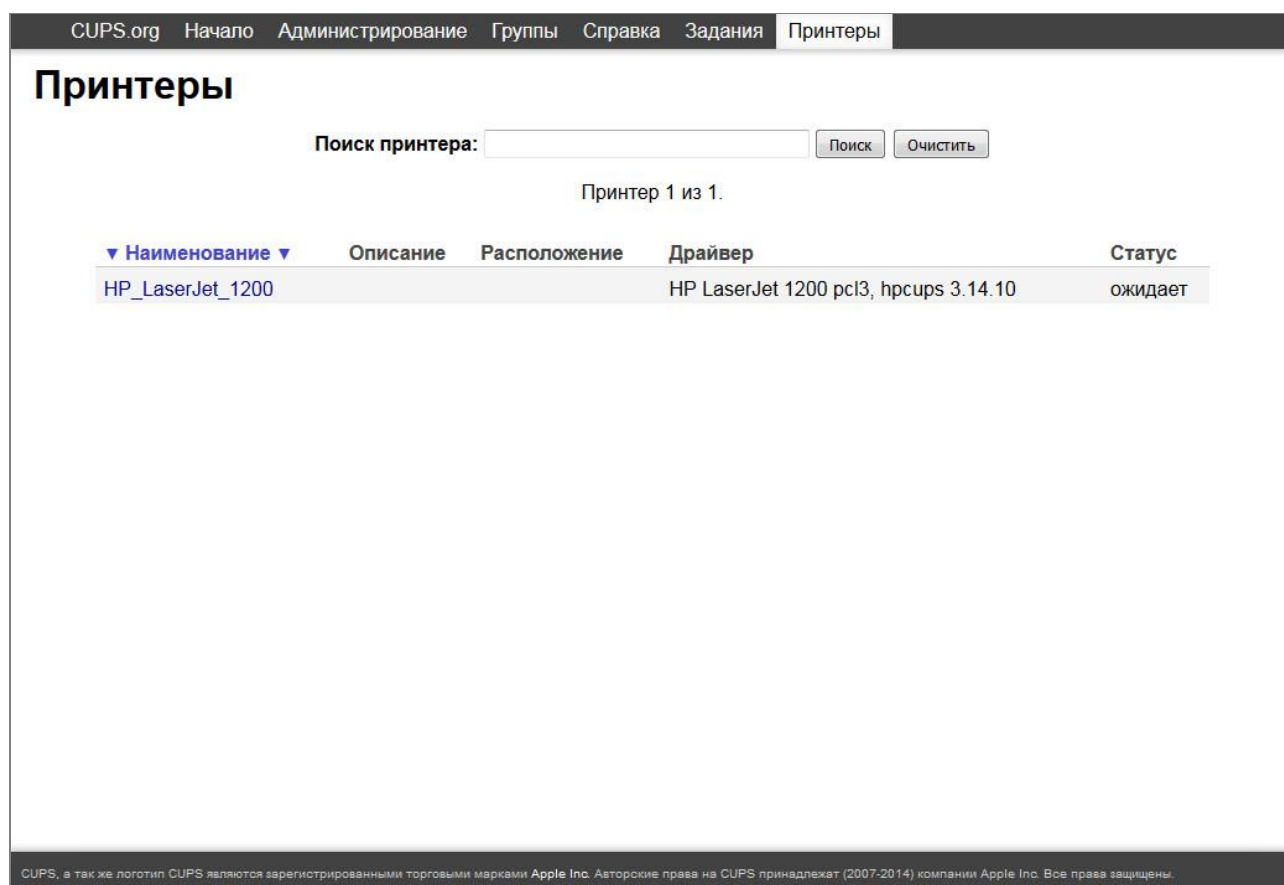


Рис. 4.94

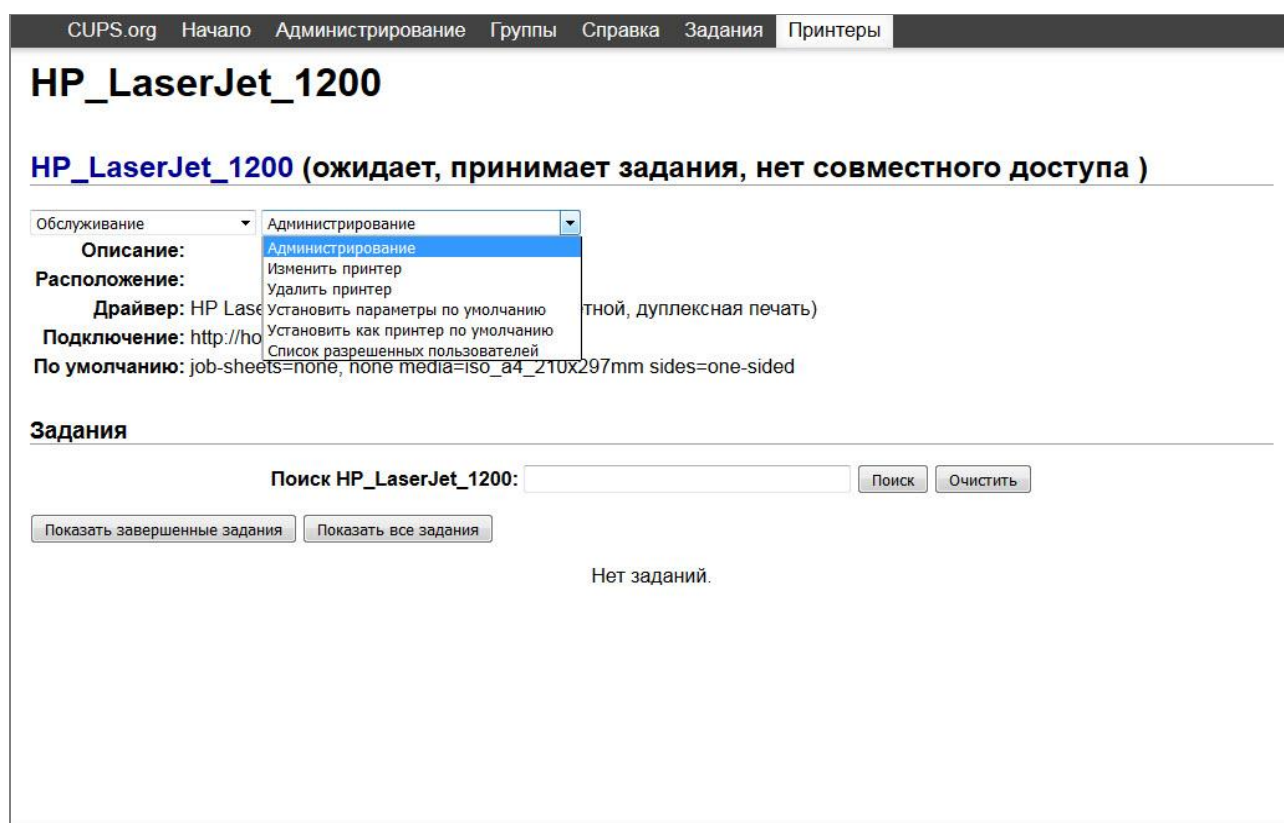


Рис. 4.95

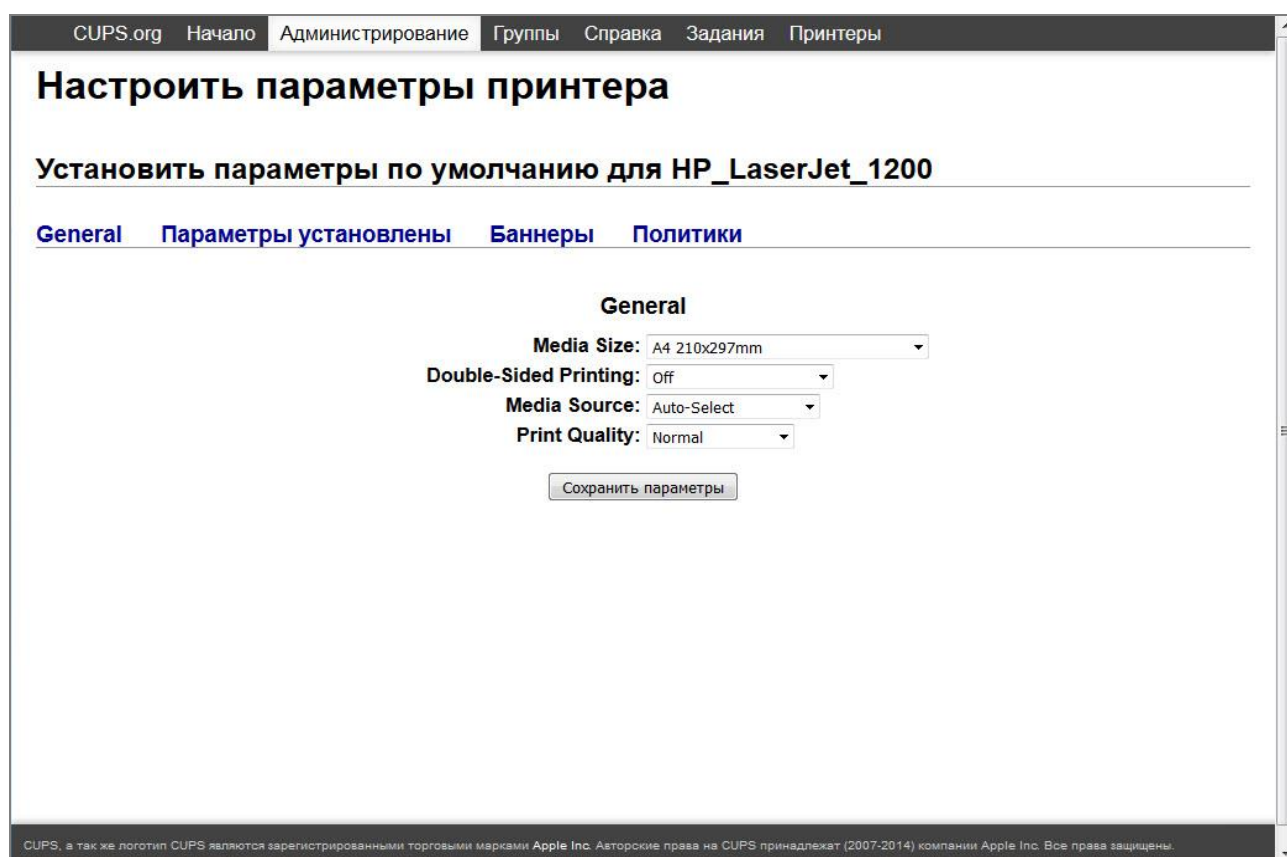


Рис. 4.96

- 6) выполнить необходимые настройки в разделах: *<Название принтера>: General*, *<Название принтера>: Параметры установлены*, *<Название принтера>: Баннеры*, *<Название принтера>: Политики* (для сохранения выбранных значений параметров настроек следует нажать на кнопку [Сохранить параметры принтера по умолчанию] в каждом разделе);
- 7) выбрать вкладку *Принтеры*, выбрать *<Название принтера>*;
- 8) →[Обслуживание] →[Печатать пробную страницу] настраиваемого принтера для распечатки тестовой страницы;
- 9) проверить визуально выполнение распечатки тестовой страницы и её качества, что подтверждает правильную настройку, и работу настраиваемого принтера;
- 10) →[x], расположенную в верхнем правом углу окна web-браузера Mozilla FireFox для закрытия системы печати CUPS.

Примечание. При создании нескольких локальных принтеров, один принтер следует назначить в качестве основного, т.е. используемого по умолчанию. Для этого следует нажать на кнопку [Администрирование] и выбрать из списка *<Установить как принтер по умолчанию>* определенного принтера на вкладке *Принтеры* в разделе *<Название принтера>* (рис. 4.95).

#### 4.4.3. Установка и настройка принт-сервера

Перед выполнением данного этапа необходимо подключить устанавливаемый принтер к порту (USB/LPT) терминальной станции и включить его. Принтер становится доступным из терминальных сессий и любых компьютеров, подключённых к сети терминальных станций.

Для выполнения установки локального принтера для принт-сервера следует:

- 1) активировать разрешение использования терминальной станции и подключенного к ней принтера в качестве принт-сервера (см. п. 4.2.6.1);
- 2) выполнить все действия пункта 4.4.1., т.е. создать новый принтер, например, HP\_LaserJet\_1200;
- 3) выбрать вкладку *Принтеры*, выбрать *<Название принтера>*;
- 4) →[Администрирование] →[Изменить принтер] только что созданного принтера, на экран выводится окно *Изменить принтер* (рис. 4.97);

- 5) выбрать необходимый принтер или порт;
- 6) →[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.98);



[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Изменить принтер

### Изменение HP\_LaserJet\_1200

Сейчас подключен: ☒ http://hostname:631/ipp/

Установленные принтеры: ☐ CAPT Printer  
☐ HP Printer (HPLIP)

Найденные сетевые принтеры:

Другие сетевые принтеры: ☐ AppSocket/HP JetDirect  
☐ Internet Printing Protocol (ipp)  
☐ LPD/LPR Host or Printer  
☐ Internet Printing Protocol (http)  
☐ Internet Printing Protocol (https)  
☐ Internet Printing Protocol (ipps)

CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.97

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Изменить принтер

### Изменение принтера HP\_LaserJet\_1200

Описание:   
(расширенное описание принтера, например, "HP LaserJet с дуплексной печатью")

Расположение:   
(местоположение принтера, например, "Кабинет 55")

Подключение: http://hostname:631/ipp/

Совместный доступ: ☐ Разрешить совместный доступ к этому принтеру

CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.



Рис. 4.98

7) выполнить изменения параметров при необходимости, поставить галочку в поле *Разрешить совместный доступ к этому принтеру*;

8) →[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.99);

9) выбрать значение «RAW» в списке параметра *Создать*::;

10)→[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.100);

11)выбрать значение «Raw Queue (en)» в списке параметра *Модель*;

12)→[Сохранить], на вкладке *Администрирование* выводятся новые параметры (рис.4.101);

CUPS.org Начало Администрирование Группы Справка Задания Принтеры

## Изменить принтер

### Изменение HP\_LaserJet\_1200

Описание: HP\_LJ1200  
Расположение:  
Подключение: http://hostname:631/ipp/  
Совместный доступ: Нет совместного доступа к этому принтеру  
Создать: HP   
Модель: Текущий драйвер - HP LaserJet 1200 pcl3, hpcups 3.14.10  
HP LaserJet 1200 pcl3, hpcups 3.14.10 (en)  
HP 910, hpcups 3.14.10 (en)  
HP 915, hpcups 3.14.10 (en)  
HP 2000C Foomatic/pcl3 (en)  
HP 2000c, hpcups 3.14.10 (en)  
HP 2500C Foomatic/pcl3 (en)  
HP 2500c, hpcups 3.14.10 (en)  
HP 2500CM Foomatic/Postscript (en)  
HP 2563 Foomatic/lp2563 (en)  
или использовать файл PPD:  Файл не выбран.

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.99

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Изменить принтер

### Изменение HP\_LaserJet\_1200

Описание: HP\_LJ1200

Расположение:

Подключение: http://hostname:631/ipp/

Совместный доступ: Нет совместного доступа к этому принтеру

Создать: HP

Модель: 

Текущий драйвер - HP LaserJet 1200 pcl3, hpcups 3.14.10

HP LaserJet 1200 pcl3, hpcups 3.14.10 (en)

Raw Queue (en)

или использовать файл PPD:  Файл не выбран.

Рис. 4.100

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Изменить принтер

### Изменение принтера HP\_LaserJet\_1200

Параметры принтера [HP\\_LaserJet\\_1200](#) успешно изменены.

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.101

13) на экран выводится окно *<Название принтера>* (рис. 4.102);

14) → [Обслуживание] → [Печатать пробную страницу] для распечатки тестовой страницы;

15) проверить визуально выполнение распечатки тестовой страницы и её качества, что подтверждает правильную установку, и работу добавленного принтера;

16) → [x], расположенную в верхнем правом углу окна web-браузера Mozilla FireFox для закрытия системы печати CUPS.

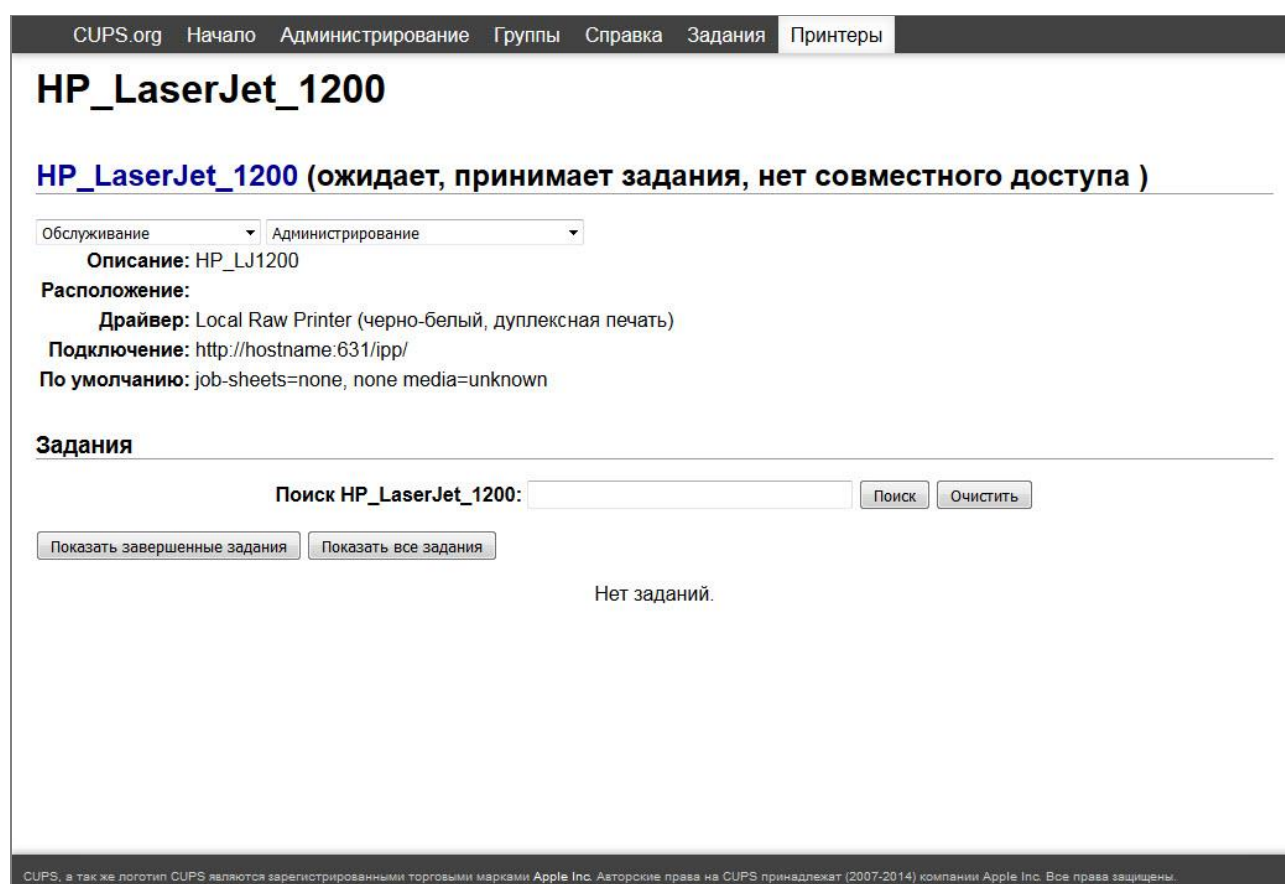


Рис. 4.102

Для выполнения настройки установленного локального принтера для принт-сервера в системе CUPS следует выполнить действия, описанные в пункте 4.4.2.

Для выполнения настройки локального принтера для принт-сервера в среде Windows следует:

1) включить компьютер, подключённый к сети терминальных станций и на котором предполагается использование данного принтера, или открыть терминальную сессию ОС Windows на терминальной станции;

2) запустить программу *Мастер установки принтеров* (→Пуск →Настройка →Принтеры и факсы →пункт меню *Установка принтера*), на экран выводится окно *Мастер установки принтеров* (рис.4.103);

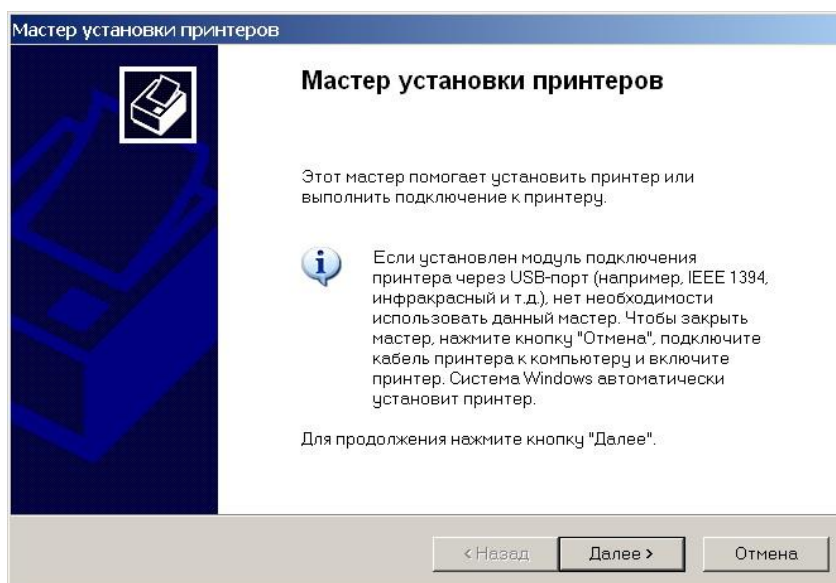


Рис. 4.103

3) →[Далее], в окне мастера установки принтеров предлагается выбрать тип устанавливаемого принтера (рис. 4.104);

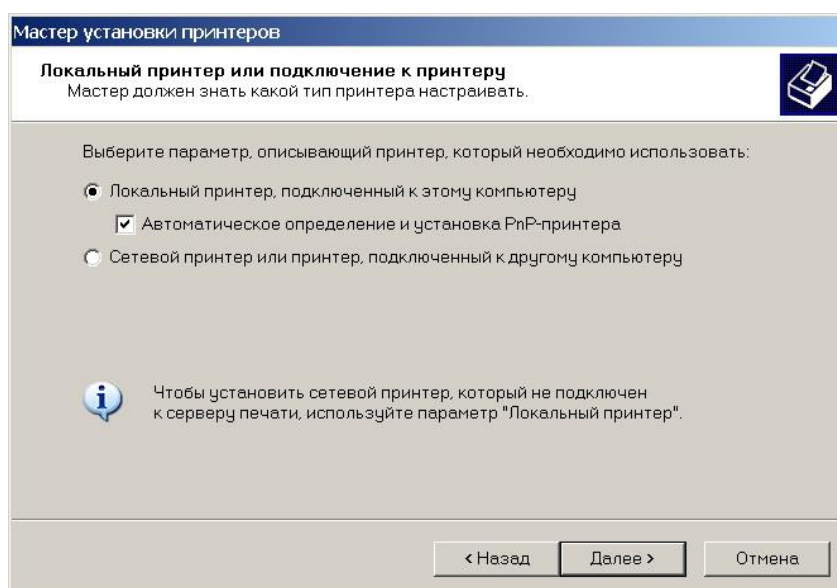


Рис. 4.104

- 4) выбрать параметр *Локальный принтер, подключённый к этому компьютеру* (установлен по умолчанию);
- 5) снять «галочку» у параметра *Автоматическое определение и установка PnP-принтера* для отмены автоматического поиска и установки PnP-принтера;
- 6) →[Далее], в окне мастера установки принтеров предлагается выбрать тип порта принтера или создать новый (рис. 4.105);
- 7) выбрать параметр *Создать новый порт*;
- 8) выбрать значение «Standard TCP/IP port» в выпадающем списке параметра *Тип порта*: (рис. 4.106);

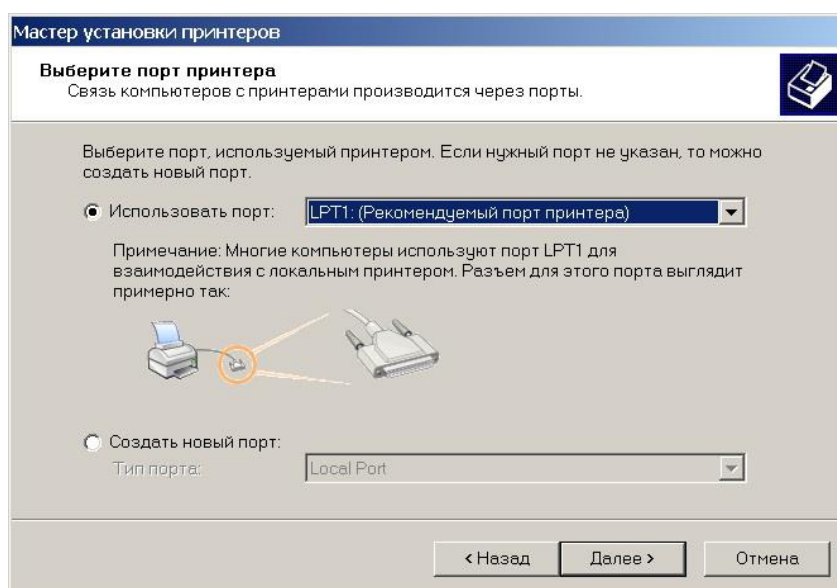


Рис. 4.105

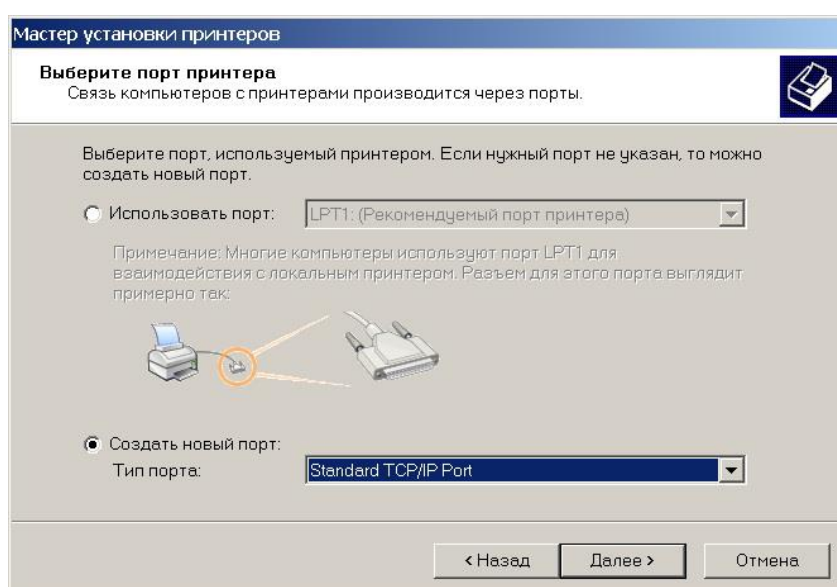


Рис. 4.106

9) →[Далее], на экран выводится окно *Мастер добавления стандартного порта TCP/IP принтера* (рис. 4.107);

10) →[Далее], в окне мастера добавления стандартного порта TCP/IP принтера предлагается ввести имя принтера (IP-адрес) и имя его порта (см. рис. 4.108);

11) ввести IP-адрес терминальной станции и имя порта в соответствующие поля;

12) →[Далее], в окне мастера добавления стандартного порта TCP/IP принтера предлагается выбрать тип устройства (рис.4.109);

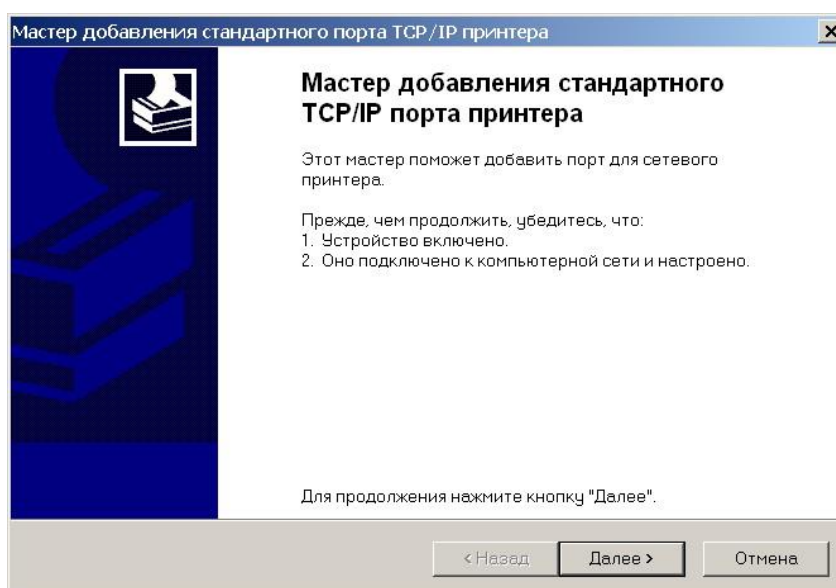


Рис. 4.107

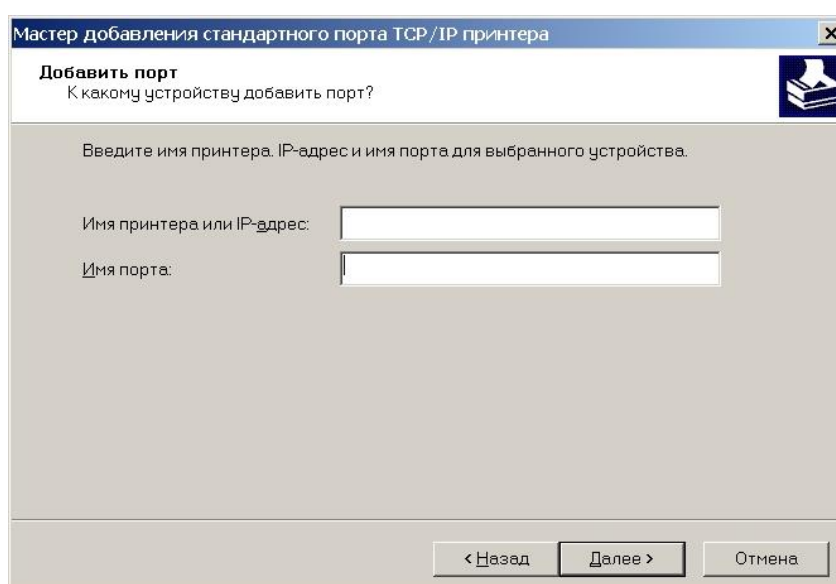


Рис. 4.108

13) ввести IP-адрес терминальной станции и имя порта в соответствующие поля;

14) → [Далее], в окне мастера добавления стандартного порта TCP/IP принтера предлагается выбрать тип устройства (рис.4.109);

15) выбрать параметр *Особое*, параметры типа устройства следует оставить без изменения;

16) → [Далее], в окне мастера добавления стандартного порта TCP/IP принтера выводится информация о созданном порте (рис.4.110);



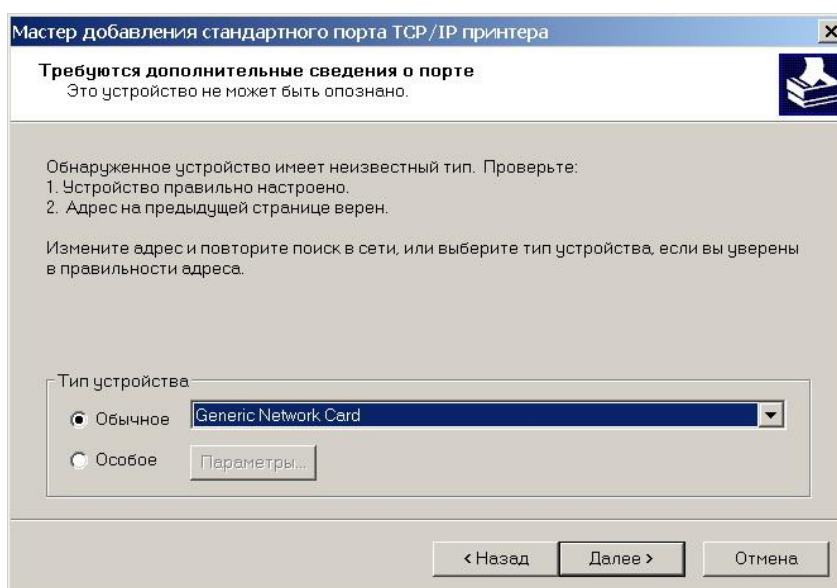


Рис. 4.109

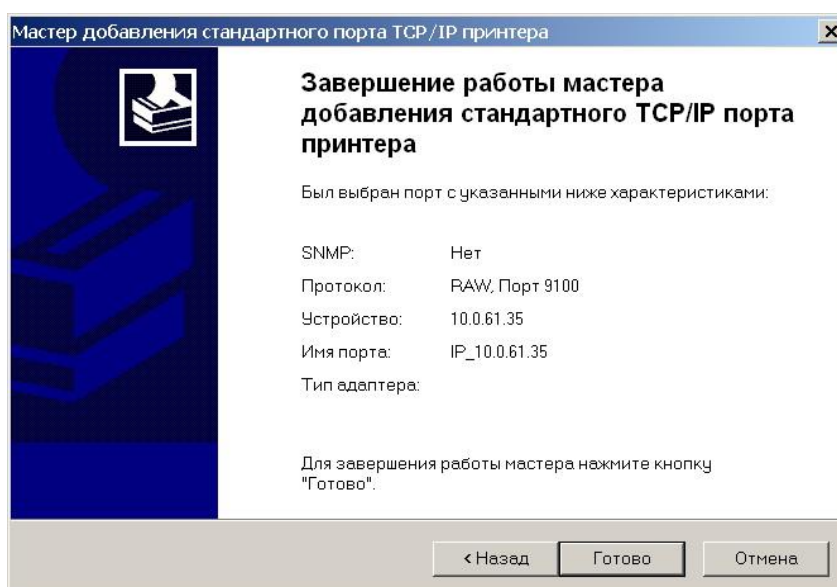


Рис. 4.110

17) → [Готово], в окне мастера установки принтеров предлагается установить драйвер (рис. 4.111);



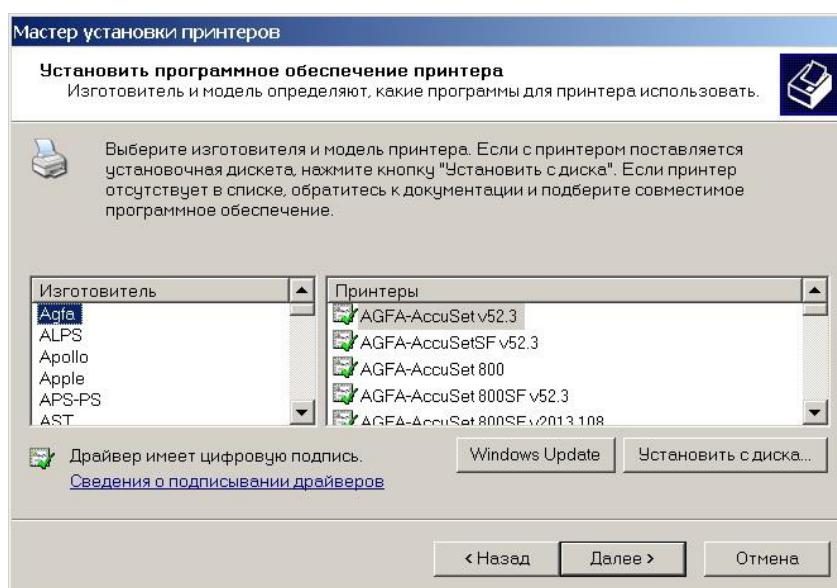


Рис. 4.111

18) выбрать изготовителя и модель принтера (при отсутствии в списке соответствующей модели принтера, следует установить необходимый драйвер с прилагаемого к принтеру диска (→[Установить с диска ...]) или подобрать совместимый драйвер по модели из представленного списка);

19) →[Далее], в окне мастера установки принтеров предлагается назначить имя для устанавливаемого принтера и сделать его принтером, используемым по умолчанию, т.е. основным (рис. .4.112);

20) ввести имя принтера, либо оставить приведённое без изменения

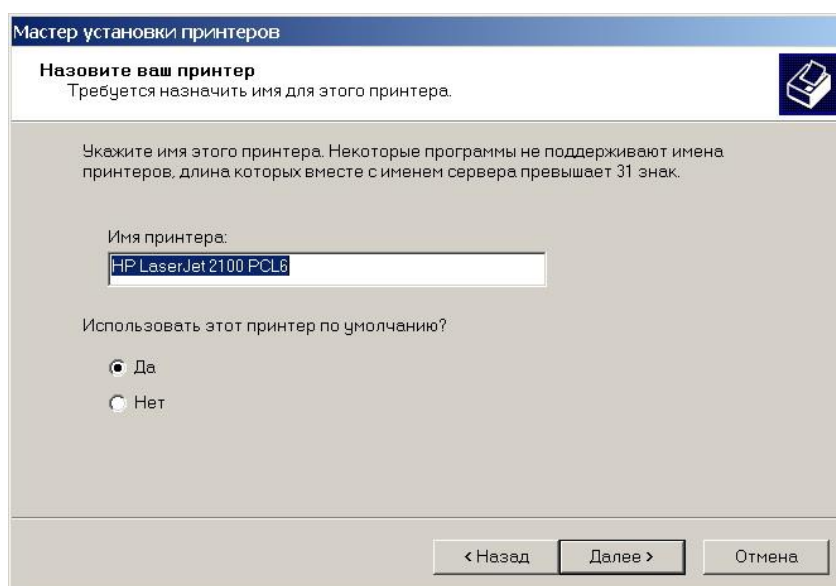


Рис.4.112 ;

21) выбрать параметр *Да* для установки принтера в качестве основного (установлен по умолчанию);

22) → [Далее], в окне мастера установки принтеров предлагается определить доступ к данному принтеру (рис. 4.113);

23) выбрать параметр *Нет общего доступа к этому принтеру* (установлен по умолчанию);

24) → [Далее], в окне мастера установки принтеров предлагается выбрать тестирование печати принтера после его установки (рис. 4.114);

25) выбрать параметр «Да» (установлен по умолчанию);

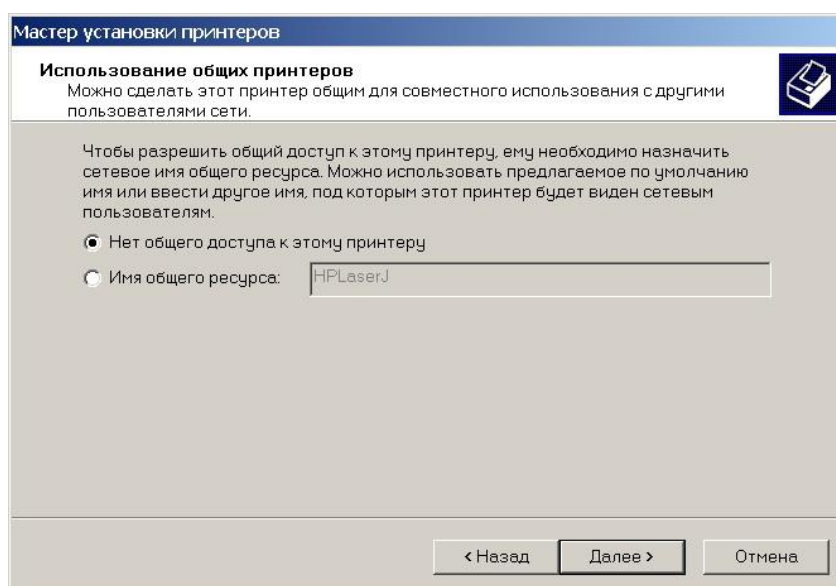


Рис. 4.113

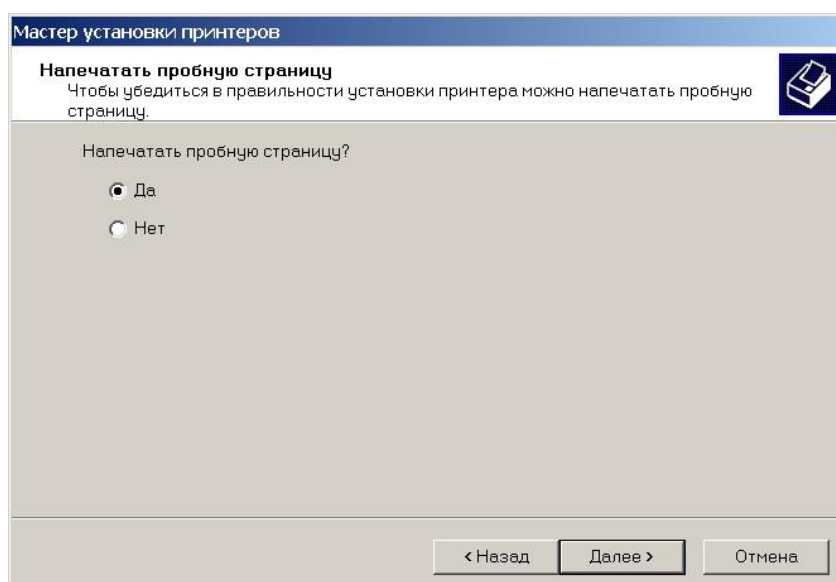


Рис. 4.114

26) → [Далее], в окне мастера установки принтеров выводится итоговая информация об установке принтера для проверки выполненных операций (рис. 4.115);

27) → [Готово];

28) проверить визуально выполнение распечатки тестовой страницы и её качества, что подтверждает правильную установку, настройку и работу терминальной станции в качестве принт-сервера.

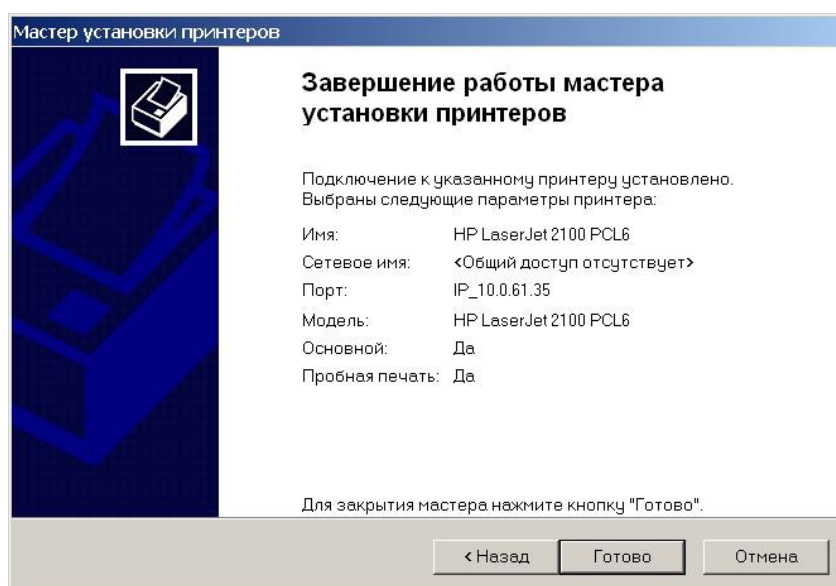


Рис. 4.115

#### 4.4.4. Установка и настройка сетевого принтера

Перед выполнением данного этапа необходимо подключить устанавливаемый принтер к локальной сети и включить его.

Для выполнения установки нового сетевого принтера следует:

- 1) выполнить действия 1 - 5, описанные в пункте 4.4.1.;
- 2) выбрать значение порта «AppSocket/HP JetDirect» в списке параметра *Устройство*;
- 3) →[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.116);

The screenshot shows the CUPS web interface. At the top is a navigation bar with links: CUPS.org, Начало, Администрирование (highlighted), Группы, Справка, Задания, and Принтеры. Below the navigation bar is a large heading "Добавить принтер". Underneath it is a sub-heading "Добавление принтера". A form labeled "Подключение:" has a text input field containing "socket". Below the input field is a section titled "Примеры:" followed by a list of URI examples: `http://hostname:631/ipp/`, `http://hostname:631/ipp/port1`, `ipp://hostname/ipp/`, `ipp://hostname/ipp/port1`, `lpd://hostname/queue`, `socket://hostname`, and `socket://hostname:9100`. Below the examples is a text instruction: "Смотрите раздел "Сетевые принтеры" для выяснения правильного адреса вашего принтера." At the bottom of the form is a button labeled "Продолжить". At the very bottom of the page, there is a small copyright notice: "CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены."

Рис. 4.116

- 4) ввести универсальный идентификатор устройства в строке *URI устройства* - IP-адрес и порт принтера, например, `socket://10.0.147.77:9100`;
- 5) →[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.117);
- 6) выбрать название принтера;
- 7) →[Продолжить], на вкладке *Администрирование* выводятся новые параметры (рис.4.118);

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Добавить принтер

### Добавление принтера

**Название:**   
(может содержать любые символы, кроме "/", "# и пробела)

**Описание:**   
(расширенное описание, например, "HP LaserJet с дуплексной печатью")

**Расположение:**   
(месторасположение принтера, например, "Кабинет 55")

**Подключение:**

**Совместный доступ:** ☐ Разрешить совместный доступ к этому принтеру

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.117

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Добавить принтер

### Добавление принтера

**Название:** HP\_1200\_network

**Описание:**

**Расположение:**

**Подключение:** socket://10.0.147.77:9100

**Совместный доступ:** Нет совместного доступа к этому принтеру

**Создать:** Generic

**Модель:**

- Generic PCL 6/PCL XL Printer Foomatic/ljet4d (en)
- Generic PCL 6/PCL XL Printer Foomatic/pxlcolor (en)
- Generic PCL 6/PCL XL Printer Foomatic/pxlmono (en)
- Generic PCL Laser Printer (en)
- Generic PDF Printer (en)
- Generic PostScript Level 1 Printer Foomatic/Postscript1 (en)
- Generic PostScript Printer (en)**
- Generic PostScript Printer Foomatic/Postscript (en)
- Generic text-only printer (en)
- Generic ZjStream Printer Foomatic/foo2zjs (en)

**или использовать файл PPD:**  Файл не выбран.

CUPS, а также логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.118

- 8) выбрать модель «Generic» в списке параметра *Создать*;
- 9) →[Продолжить], выбрать значение драйвера «Generic PostScript Printer (en)» в списке параметра *Модель*;
- 10) →[Добавить принтер], на экран выводится окно *Требуется аутентификация*;
- 11) ввести имя и пароль администратора в соответствующие поля (имя администратора CUPS - admin, пароль - admin, значения, используемые по умолчанию);
- 12) на экран выводится окно установки параметров по умолчанию для нового принтера, при необходимости можно изменить настройки;
- 13) →[Сохранить параметры по умолчанию], на вкладке *Администрирование* выводятся новые параметры (рис.4.119);
- 14) нажать левой клавишей мыши на название нового принтера, на экран выводится окно *<Название принтера>* (рис. 4.120);
- 15) →[Обслуживание] →[Печатать пробную страницу], для распечатки тестовой страницы;
- 16) проверить визуально выполнение распечатки тестовой страницы и её качества, что подтверждает правильную установку, и работу добавленного принтера;
- 17) →[x], расположенную в верхнем правом углу окна web-браузера Mozilla FireFox для закрытия системы печати CUPS.

Для выполнения настройки установленного сетевого принтера в системе CUPS следует выполнить действия, описанные в пункте 4.4.2.

Примечание. При создании нескольких сетевых принтеров один принтер следует назначить в качестве основного, т.е. используемого по умолчанию, это относится и к случаю, когда создано несколько локальных и сетевых принтеров. Для этого следует нажать на кнопку [Сделать принтером по умолчанию] определённого принтера на вкладке *Принтеры* окна *<Название принтера>* (см.рис.4.94, рис.4.102, рис. 4.120).

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## Настроить параметры принтера

### Настройки по умолчанию для HP\_1200\_network

Принтер [HP\\_1200\\_network](#) теперь использует параметры по умолчанию.

CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.119

[CUPS.org](#) [Начало](#) [Администрирование](#) [Группы](#) [Справка](#) [Задания](#) [Принтеры](#)

## HP\_1200\_network

### HP\_1200\_network (ожидает, принимает задания, нет совместного доступа )

Обслуживание

Администрирование

**Описание:**  
**Расположение:**  
**Драйвер:** Generic PostScript Printer (цветной)  
**Подключение:** socket://10.0.147.77:9100  
**По умолчанию:** job-sheets=none, none media=iso\_a4\_210x297mm sides=one-sided

### Задания

Поиск HP\_1200\_network:

Нет заданий.

CUPS, а так же логотип CUPS являются зарегистрированными торговыми марками Apple Inc. Авторские права на CUPS принадлежат (2007-2014) компании Apple Inc. Все права защищены.

Рис. 4.120



#### 4.5. Удаление печатающих устройств

Для выполнения удаления печатающего устройства следует:

- 1) выполнить действия 1, 2, описанные в пункте 4.4.1.;
- 2) выбрать вкладку *Принтеры*;
- 3) выбрать удаляемый принтер из приведённых на вкладке *Принтеры*, например, HP\_1200\_network;
- 4) →[Администрирование] →[Удалить принтер], на экран выводится окно *Удаление принтера* (рис. 4.121), в котором запрашивается подтверждение на выполнение данной операции;
- 5) →[Удалить принтер], на экран выводится окно *Требуется аутентификация* (см. рис. 4.91);
- 6) ввести имя и пароль администратора в соответствующие поля (имя администратора CUPS - admin, пароль - admin, значения, используемые по умолчанию), на вкладке *Администрирование* выводится результат операции (рис. 4.122);
- 7) →[x], расположенную в верхнем правом углу окна web-браузера Mozilla FireFox для закрытия системы печати CUPS.

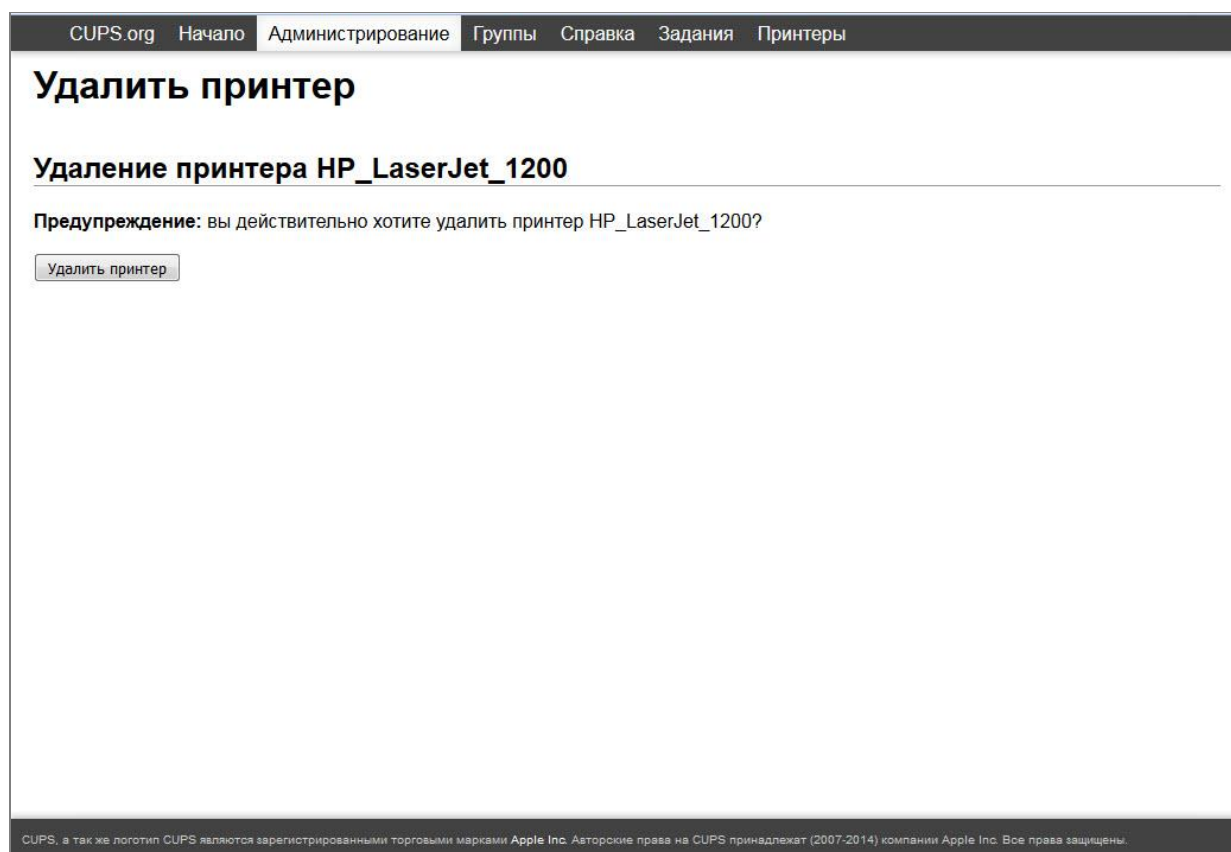


Рис. 4.121

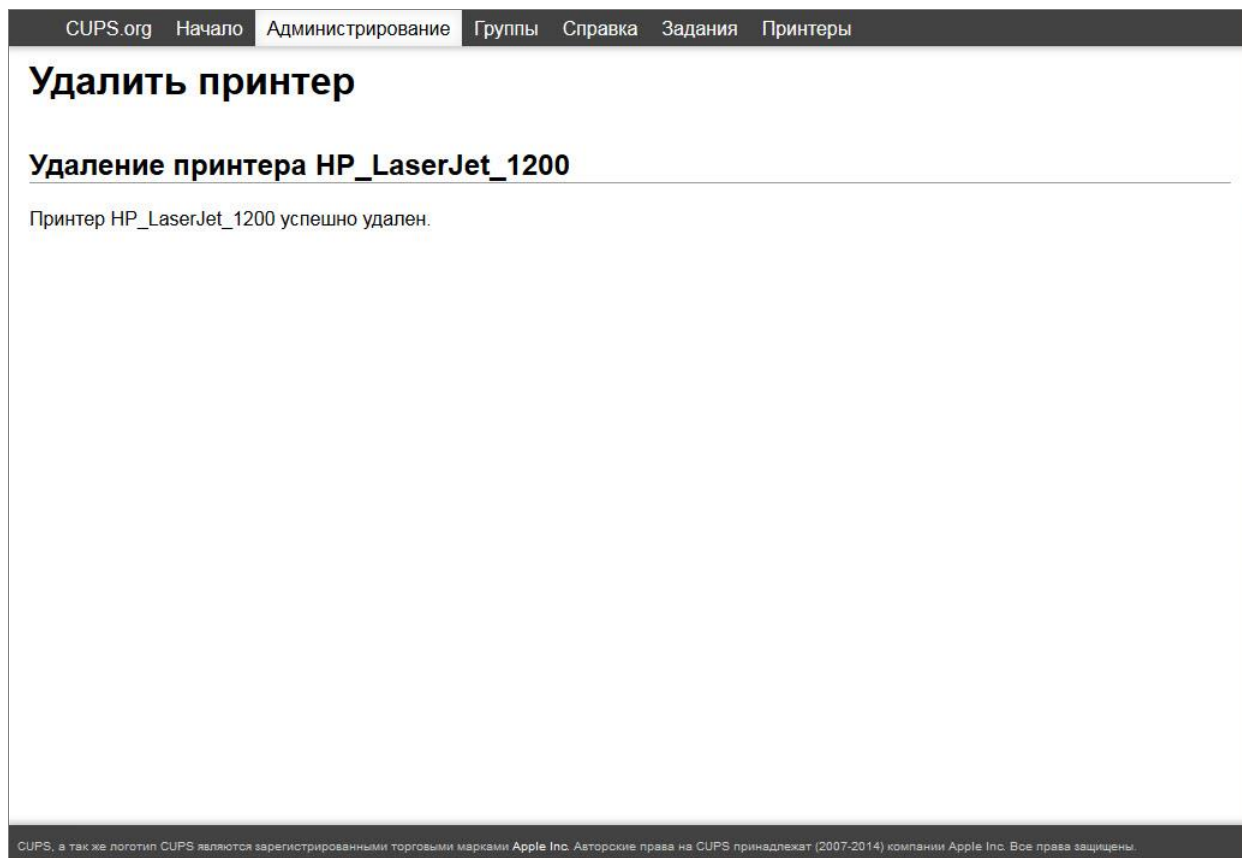


Рис. 4.122

## 4.6. Установка и настройка сканирующих устройств

Пользователю предоставляется возможность использования терминальной станции и подключённого к ней сканера в качестве скан-сервера. Сканер становится доступным из терминальных сессий ОС UNIX\Linux\Windows и любых компьютеров, подключённых к сети терминальных станций.

Пользователю также предоставляется возможность работы со сканерами штрих-кодов, которые подключаются к COM-порту или разъёму PS/2 терминальной станции.

### 4.6.1. Установка и настройка скан-сервера

Перед выполнением данного этапа необходимо подключить устанавливаемый сканер к порту (USB/LPT) терминальной станции и включить его.

Для использования терминальной станции в качестве скан-сервера следует:

1) разрешить использование терминальной станции и подключенного к ней сканера в качестве скан-сервера (см. п. 4.2.6.1);

2) выполнить настройку установленного сканера по IP-адресу терминальной станции с помощью специальной программы, например, SaneTwain (см. <http://sanetwain.ozuzo.net/>), в терминальной сессии или на любом компьютере, подключённом к сети терминальных станций и на котором предполагается его использование.

### 4.6.2. Установка и настройка сканера штрих-кодов

Перед выполнением данного этапа необходимо подключить устанавливаемый сканер штрих-кодов к COM-порту или разъёму PS/2 клавиатуры терминальной станции.

При необходимости одновременного подключения клавиатуры и сканера штрих-кодов к одному разъёму PS/2 следует использовать PS/2 разветвитель.

При подключении сканера штрих-кодов к COM-порту терминальной станции следует разрешить перенаправление COM/LPT-портов в сессию на терминальном сервере (см. п. 4.2.6.1).

## 4.7. Обновление ПО терминальной станции

### 4.7.1. Обновление ПО терминальной станции из системного меню

Для обновления ПО терминальной станции из системного меню рабочего стола следует:

1) обратиться в Единый центр поддержки пользователей компании Kraftway (см. приложение 1) для получения загрузочного образа *bootflash\_linux\_x.x\_hdd.img* / *bootflash\_linux\_x.x\_zip.img* с новой версией ПО «Kraftway Terminal Linux», где *x.x* - номер версии ПО, *hdd*, *zip* - типы устройств, для которых созданы образы;

2) скопировать полученный образ на USB-диск, например: *bootflash\_linux\_4.8\_hdd.img* или создать загрузочный USB-диск из полученного образа (см. п. 4.7.2);

3) →[Пуск] →*Обновить прошивку*, на экран выводится окно *upgrade* (рис.4.123) с приглашением на подключение USB-диска с обновлённой версией ПО «Kraftway Terminal Linux»;

4) подключить USB-диск к свободному USB-порту терминальной станции. Если терминальная станция загружена в UEFI (версии ПО KTL 4.7 и выше) на экране появится сообщение о проверке подлинности подписи KTL (рис. 4.124);

5) далее начинается процесс обновления ПО с выводом подробного описания его этапов на экран монитора (проверка файлов, подготовка раздела к прошивке, создание файловой системы на разделе, монтирование раздела к файловой системе, установка загрузчика, копирование файлов на раздел, рис. 4.125);

6) извлечь USB-диск из USB-порта терминальной станции при появлении системного сообщения об успешном выполнении установки ПО;

7) нажать клавишу *Enter* на клавиатуре или дождаться автоматической перезагрузки терминальной станции по истечении 10 секунд;

8) дождаться загрузки терминальной станции.

Примечания:

1. Последовательность действий 3 и 4 можно менять местами

2. Если проверка подлинности подписи KTL (действие 4), не пройдена на экран выводится сообщение об ошибке, установка ПО прерывается, терминал выключается.

3. Если вовремя не извлечь USB-диск из USB-порта терминальной станции после успешной прошивки ПО, то после перезагрузки терминала на экран монитора будет выведено следующее сообщение вида:

Remove disks or other media.

Press any key to restart

Для продолжения загрузки терминала следует извлечь USB-диск из USB-порта и нажать любую клавишу на клавиатуре.

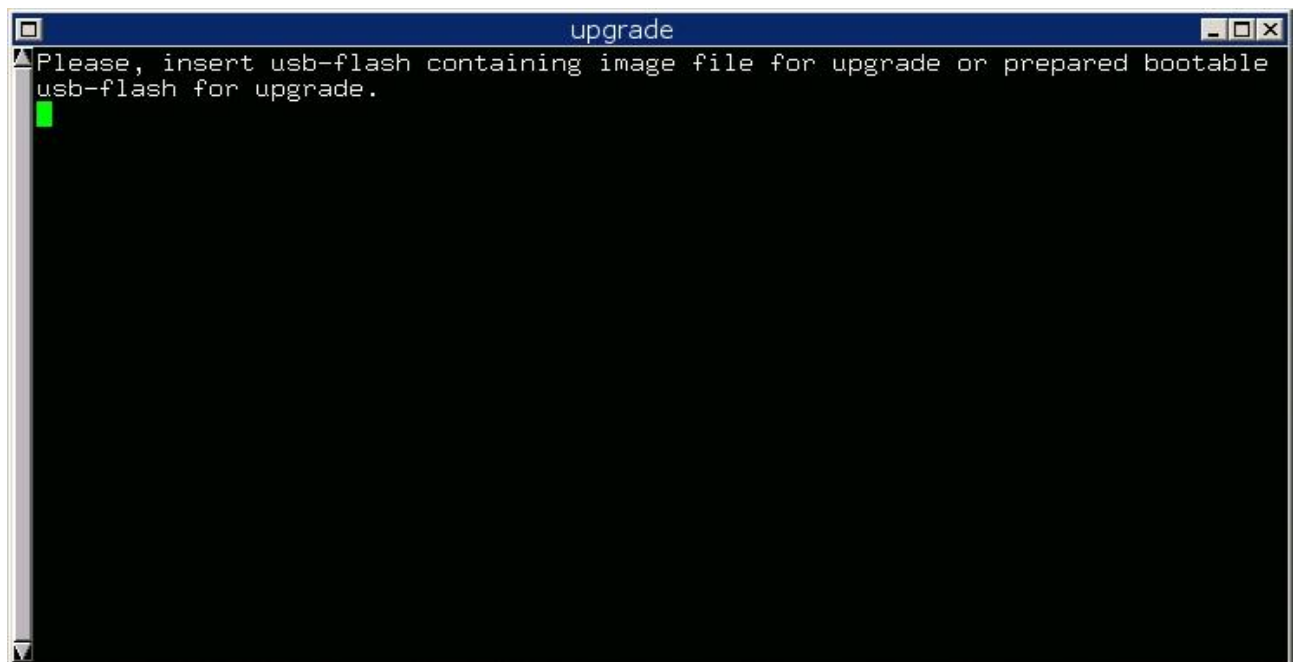


Рис. 4.123

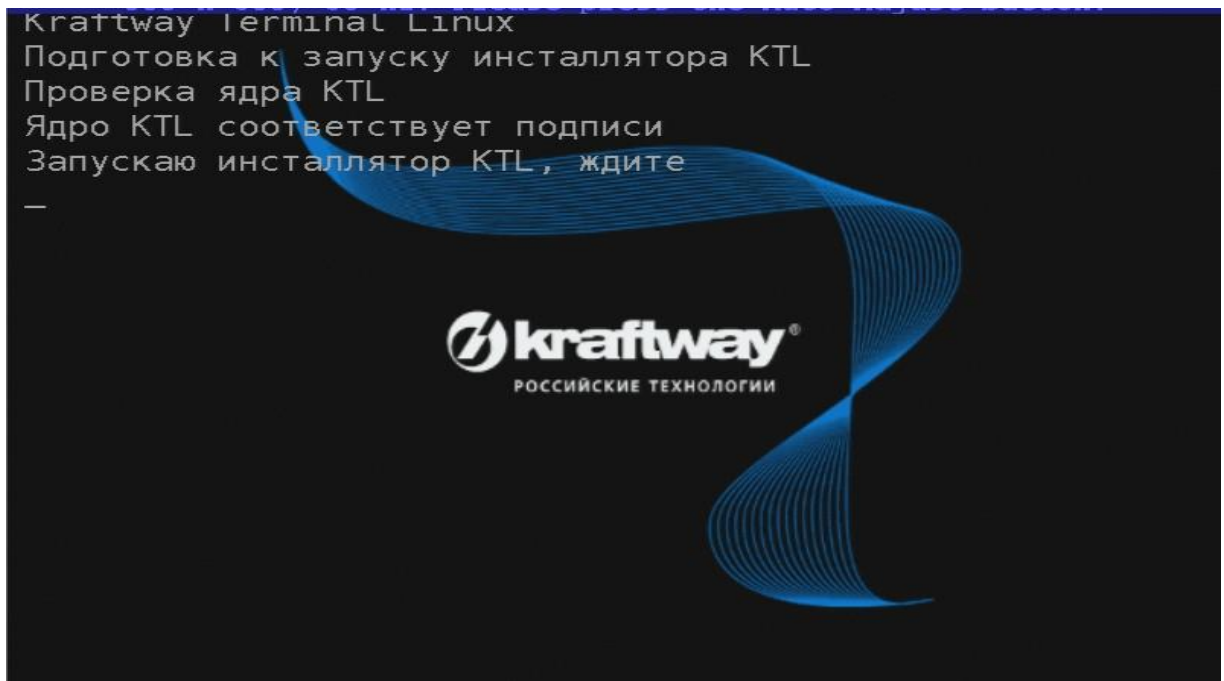


Рис. 4.124

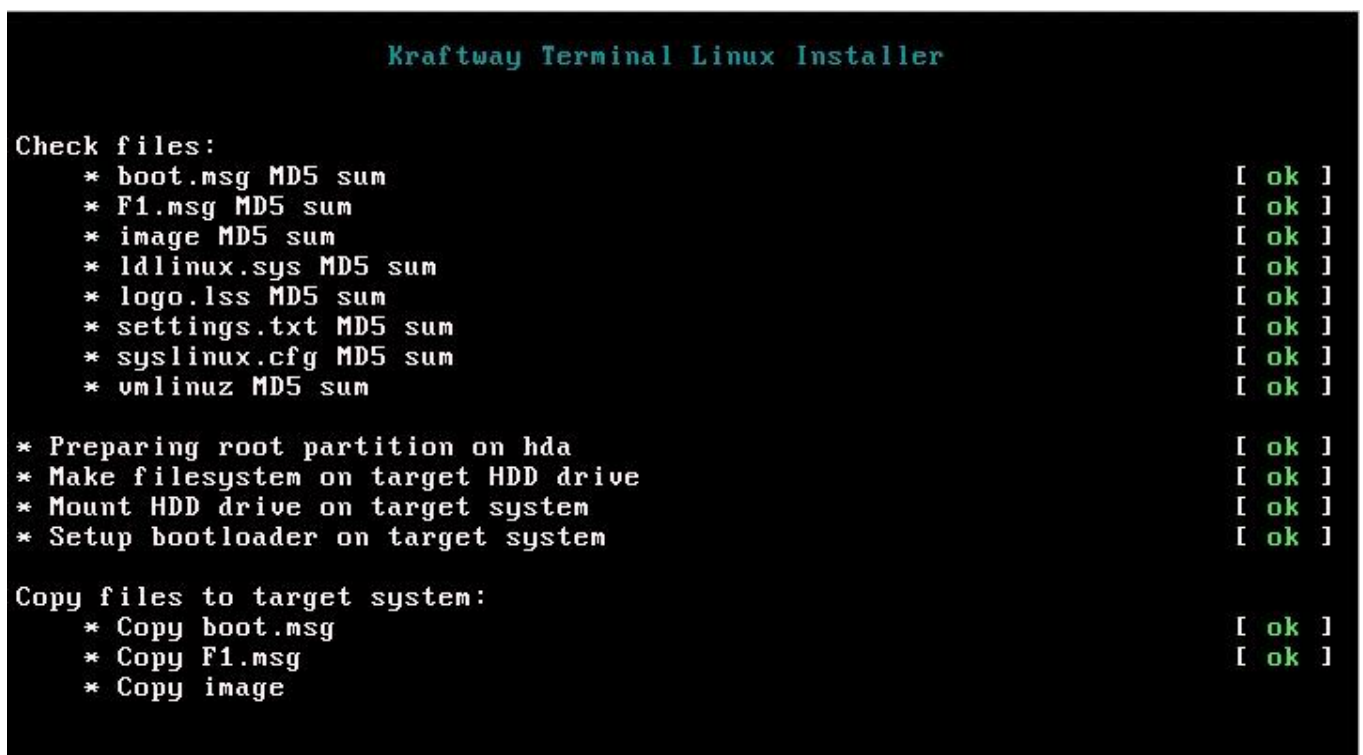


Рис. 4.125

#### 4.7.2. Создание загрузочного USB-flash диска для установки ПО

Для создания загрузочного USB-диска на ПК, работающем под управлением ОС Windows следует:

- 1) подключить USB-flash к компьютеру;
- 2) запустить программу Image Writer for Windows, у пользователя должны быть права администратора (рис. 4.126);



Рис. 4.126

3) в поле *Image File* нажать на кнопку с изображением папки и в появившемся окне выбрать нужный файл образа;

4) в поле *Device* выбрать USB-диск, на который будет производится запись;

5) → [write].

**ВНИМАНИЕ: ВСЕ ДАННЫЕ С USB-FLASH ДИСКА БУДУТ УДАЛЕНЫ.**

**ВНИМАНИЕ: ПРИ НЕВЕРНОМ ЗАДАНИИ ПУТИ К УСТРОЙСТВУ, НА КОТОРОЕ ПРОИЗВОДИТСЯ ЗАПИСЬ, МОГУТ БЫТЬ УНИЧТОЖЕНЫ ВСЕ ДАННЫЕ НА ДРУГОМ НОСИТЕЛЕ.**

6) дождаться, пока программа закончит копирование. После этого загрузочный USB-flash диск готов.

Примечание. Исполняемый файл *win32diskimager-binary.zip* программы Image Writer for Windows можно скачать с сайта <http://sourceforge.net/projects/win32diskimager>.

Для создания загрузочного USB-flash диска на ПК, работающем под управлением ОС GNU/Linux следует:

- 1) подключить USB-flash к компьютеру;
- 2) если в системе настроено автоматическое монтирование подключаемых устройств, то необходимо размонтировать USB-flash;
- 3) перенести файл образа Kraftway Terminal Linux на USB-flash с помощью встроенной программы dd (команда: `dd if=bootflash_linux_x.x_zip.img of=/dev/<device>`, где <device> - имя, подключенного устройства, например: sdb);

**ВНИМАНИЕ: ВСЕ ДАННЫЕ С USB-FLASH ДИСКА БУДУТ УДАЛЕНЫ.**

- 4) дождаться, пока программа закончит копирование. После этого загрузочный USB-flash диск готов.

После установки ПО на терминал Вам может потребоваться вернуть USB-flash диск в исходное состояние. Если вы используете ОС Windows 7 или XP:

- 1) чтобы удалить созданную разметку на диске, повторите процедуру очистки содержимого диска с помощью программы diskpart;
- 2) нажмите кнопку Start (Пуск), в поле “Найти программы и файлы” введите diskpart. Откроется окно терминала с программой DiskPart. У пользователя должны быть права администратора;
- 3) введите команду `list disk` и найдите свой подключенный USB-диск (определить можно по размеру);
- 4) введите команду `select disk <номер>` (нужно подставить номер диска, которой вы определили);
- 5) введите команду `clean` (эта команда очистит данные на диске);
- 6) введите команду `exit` (чтобы выйти из программы).

После этого выньте USB-flash и вставьте заново. Windows предложит отформатировать диск.

Если вы используете ОС GNU/Linux, вы можете удалить созданный на USB-flash диске раздел с помощью программы fdisk и создать новый. Затем отформатировать созданный раздел в необходимую файловую систему.

.

#### 4.8. Подключение к терминальному серверу



Пункт системного меню *Подключиться к серверу* используется для подключения терминальной станции к серверу по выбранному типу соединения. Доступно несколько типов соединения:

- запуск пользовательских сессий ОС Windows по протоколам ICA, RDP, Spice и ALP;
- запуск пользовательских сессий ОС UNIX (Linux) по протоколам X11, NX, OpenSSH, Spice, ALP, X2GO ;
- запуск платформонезависимой VNC-сессии;
- запуск сессий VMWare View по протоколам RDP, PCoIP.

Для открытия требуемой сессии следует:

- 1) →[Пуск] на панели задач;
- 2) выбрать пункт *Подключиться к серверу*;
- 3) в окне *Настройка подключения терминала* в поле выбора *Тип соединения* (рис. 4.127) указать нужный тип соединения;

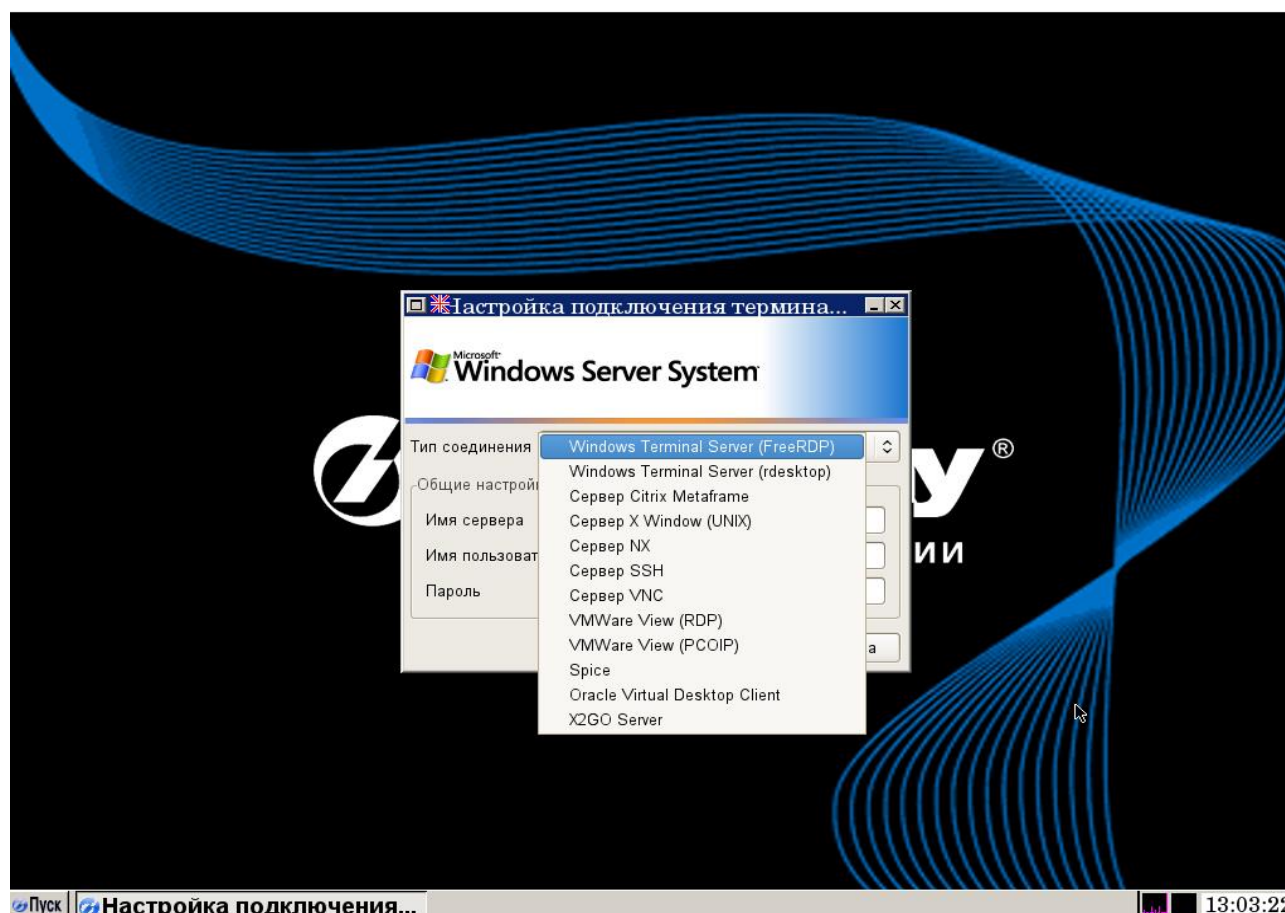


Рис. 4.127

- 4) заполнить поля общих настроек (при необходимости);
- 5) →[OK].

#### 4.9. Дополнительные возможности системного меню

##### 4.9.1. Работа в командной строке

Для запуска и работы в командной строке следует:

- 1) →[Пуск] на панели задач;

2) выбрать пункт *Командная строка* в появившемся системном меню, на экран выводится окно *urxvt* терминала (рис. 4.128) с приглашением для ввода команд;

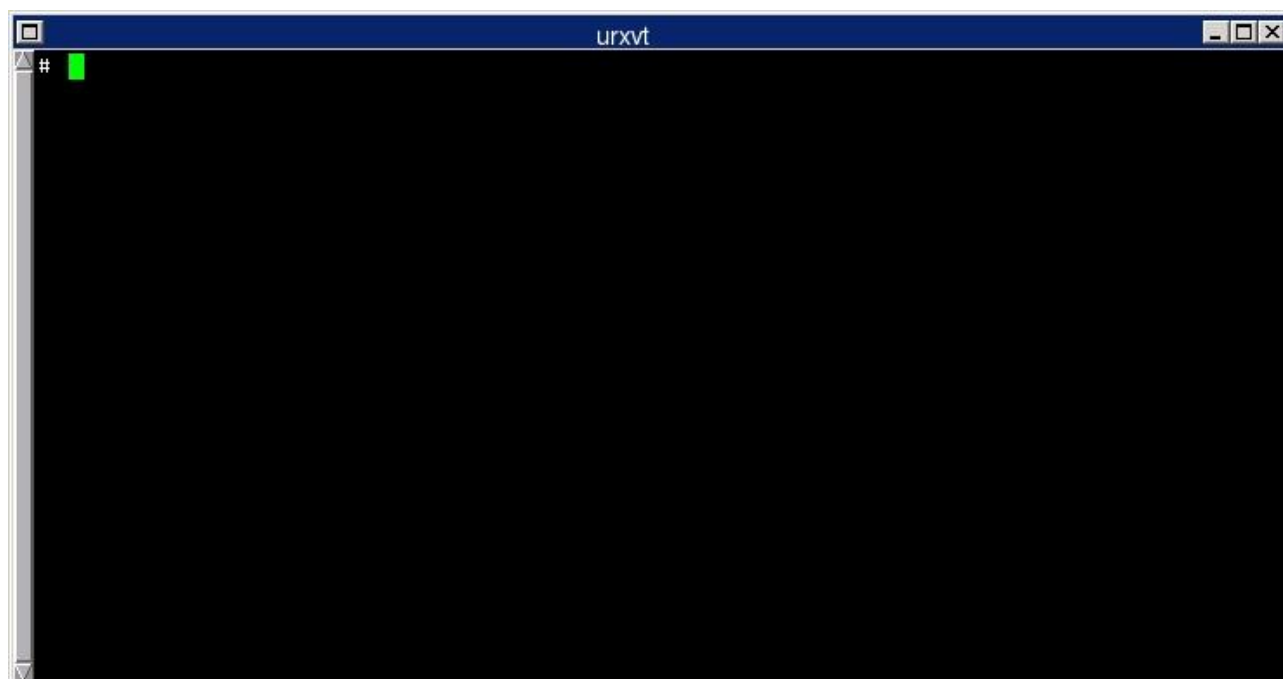
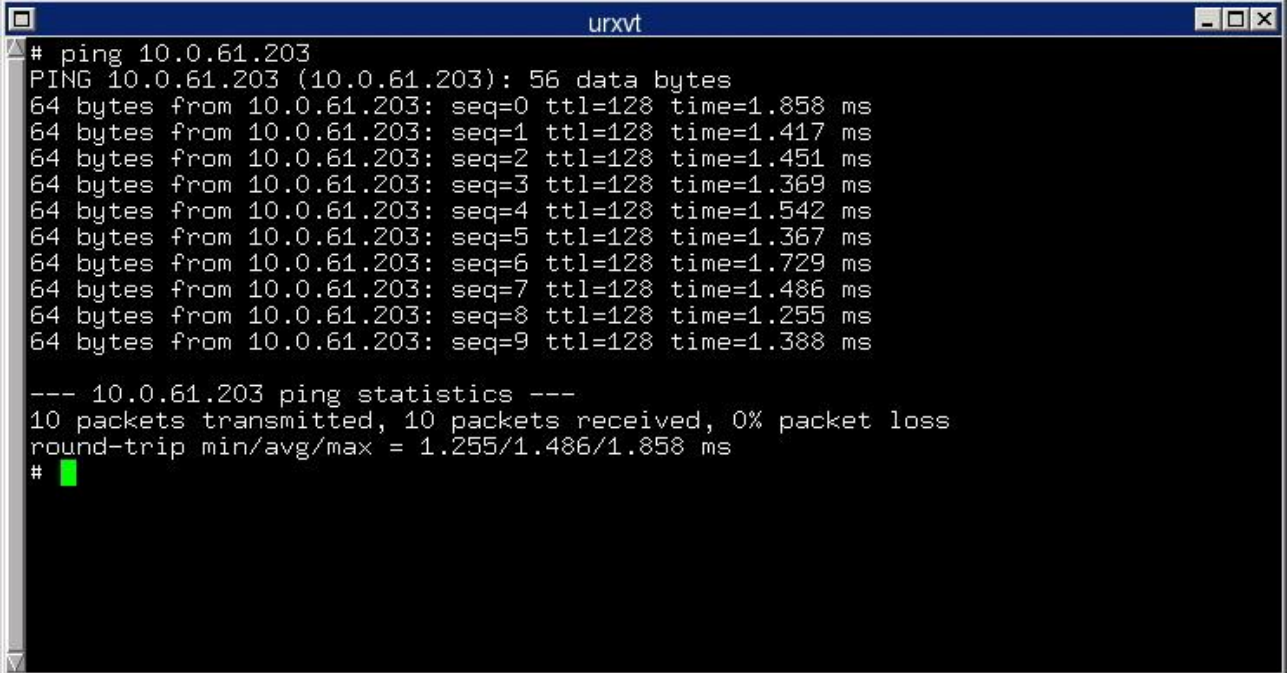


Рис. 4.128

3) ввести необходимую команду (например `ping 10.0.61.203`), в окне *urxvt* терминала выводится соответствующая информация (рис. 4.129);

4) →[x], расположенную в верхнем правом углу окна, для выхода из режима командной строки.



```
# ping 10.0.61.203
PING 10.0.61.203 (10.0.61.203): 56 data bytes
64 bytes from 10.0.61.203: seq=0 ttl=128 time=1.858 ms
64 bytes from 10.0.61.203: seq=1 ttl=128 time=1.417 ms
64 bytes from 10.0.61.203: seq=2 ttl=128 time=1.451 ms
64 bytes from 10.0.61.203: seq=3 ttl=128 time=1.369 ms
64 bytes from 10.0.61.203: seq=4 ttl=128 time=1.542 ms
64 bytes from 10.0.61.203: seq=5 ttl=128 time=1.367 ms
64 bytes from 10.0.61.203: seq=6 ttl=128 time=1.729 ms
64 bytes from 10.0.61.203: seq=7 ttl=128 time=1.486 ms
64 bytes from 10.0.61.203: seq=8 ttl=128 time=1.255 ms
64 bytes from 10.0.61.203: seq=9 ttl=128 time=1.388 ms

--- 10.0.61.203 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 1.255/1.486/1.858 ms
#
```

Рис. 4.129

#### 4.9.2. Работа с утилитой сканирования

Пользователю предоставляется возможность использования универсальной утилиты для сканирования документов при работе со сканирующими устройствами (см. пункт 4.6).

Для запуска и работы утилиты сканирования следует:

- 1) →[Пуск] на панели задач;
- 2) выбрать пункт *Утилита для сканирования* в появившемся системном меню, на экран выводится окно *Сканирование терминала* (рис.4.130);

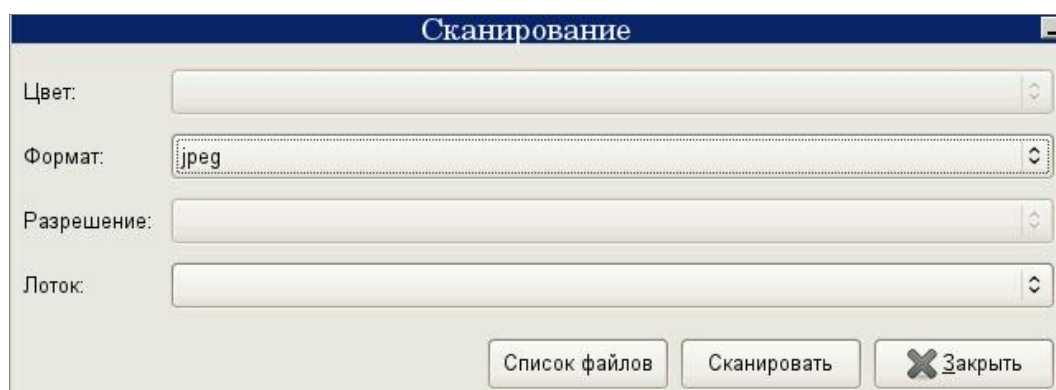


Рис. 4.130

- 3) внести необходимые изменения в параметры настроек;
- 4) →[Сканировать];
- 5) →[Список файлов], на экран выводится окно *Список файлов* (рис. 4.131);

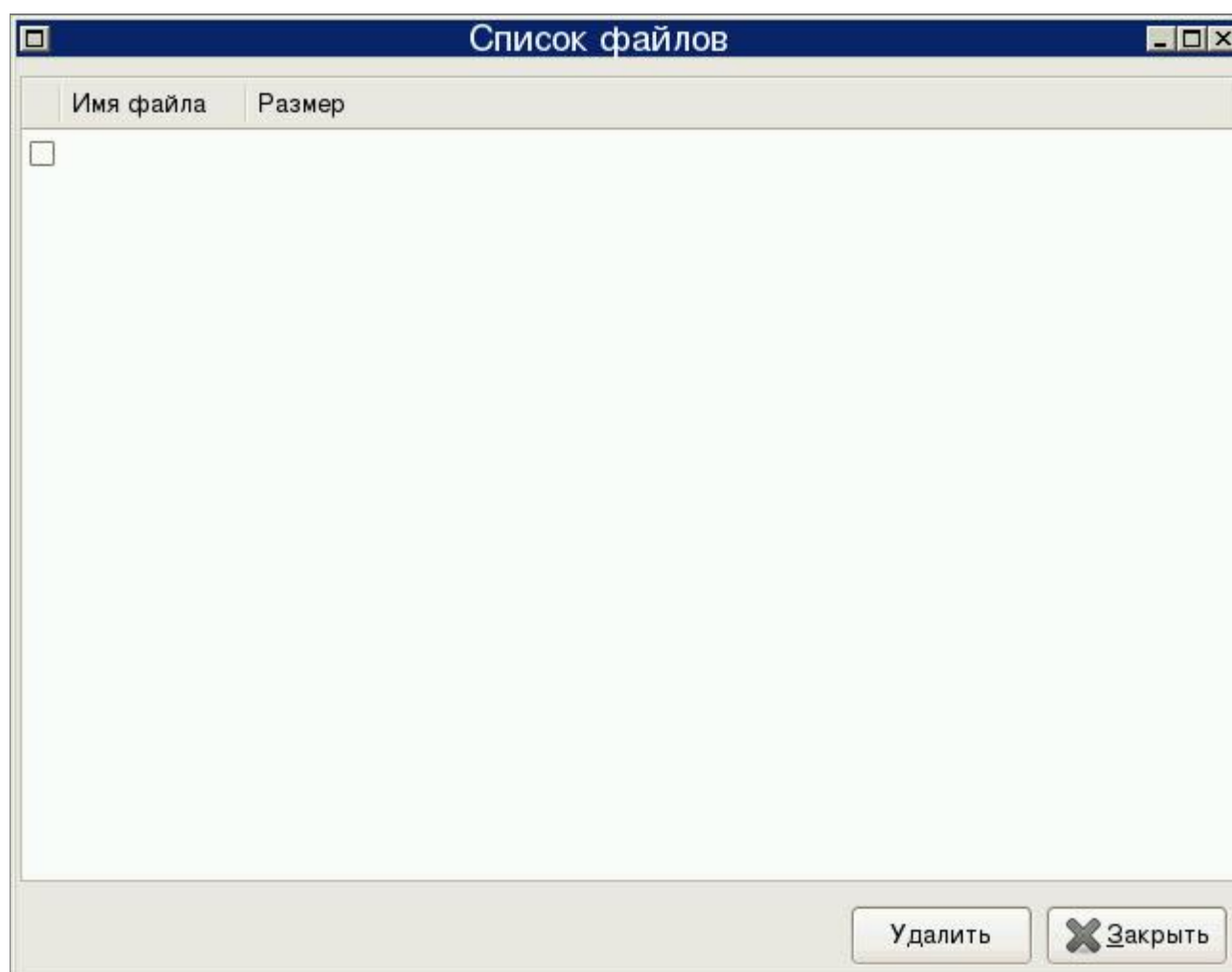


Рис. 4.131

6) →[Заккрыть], для выхода из режима сканирования.

#### 4.9.3. Вывод информации о системе

Для получения информации о версии ПО, которое установлено на данной терминальной станции, следует:

- 1) →[Пуск] на панели задач;
- 2) выбрать в появившемся системном меню пункт *О системе*, на экран выводится окно *О системе* (рис. 4.132);
- 3) →[x], расположенную в верхнем правом углу окна, или →[OK] для закрытия информационного окна.

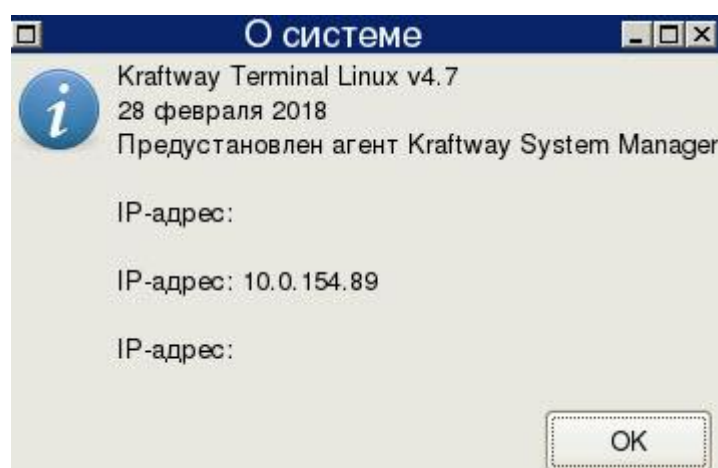


Рис. 4.132

#### 4.9.4. Контрольная сумма системы

Контрольная сумма предназначена для проверки целостности системы.

Для снятия контрольной суммы следует:

- 1) →[Пуск] на панели задач;
- 2) выбрать пункт *Контрольная сумма* в появившемся системном меню, на экран выводится окно *Контрольная сумма* (рис. 4.133) с указанием контрольной суммы системы.

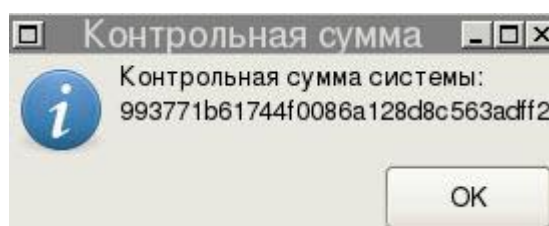


Рис. 4.133

#### 4.9.5. Настройка звука

Предназначена для настройки звуковой карты.

Для запуска и работы с настройками звуковой карты следует:

- 1) → [Пуск] на панели задач;
- 2) выбрать пункт *Настройка звука* в появившемся системном меню, на экран выводится окно с параметрами настройки звука (рис. 4.134);
- 3) выбрать из списка *Sound card* требуемую звуковую карту;
- 4) →[Выбрать каналы] в окне настройки звука, на экран выводится окно *Управляемые каналы* для выбора управляемых каналов (рис. 4.135);
- 5) выбрать требуемые каналы →[Заккрыть], в зависимости от выбора настраиваемого канала в окне появляются вкладки: *Playback*, *Capture*, *Switches*, *Options*;
- 6) с помощью ползунков установить уровень громкости, включить или отключить требуемые звуковые каналы, выполнить настройку дополнительных параметров (если необходимо);
- 7) →[Выход], для выхода из настроек звука.

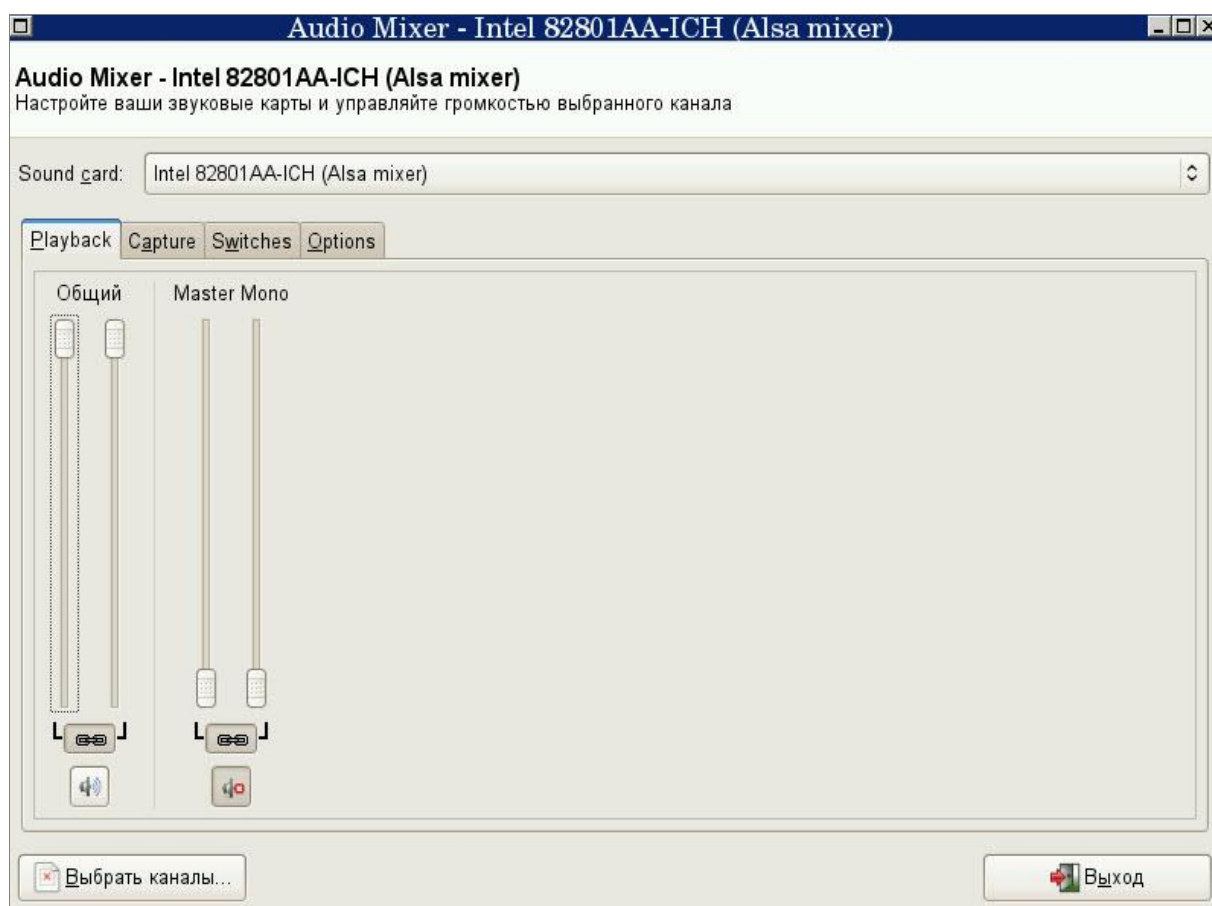


Рис. 4.134

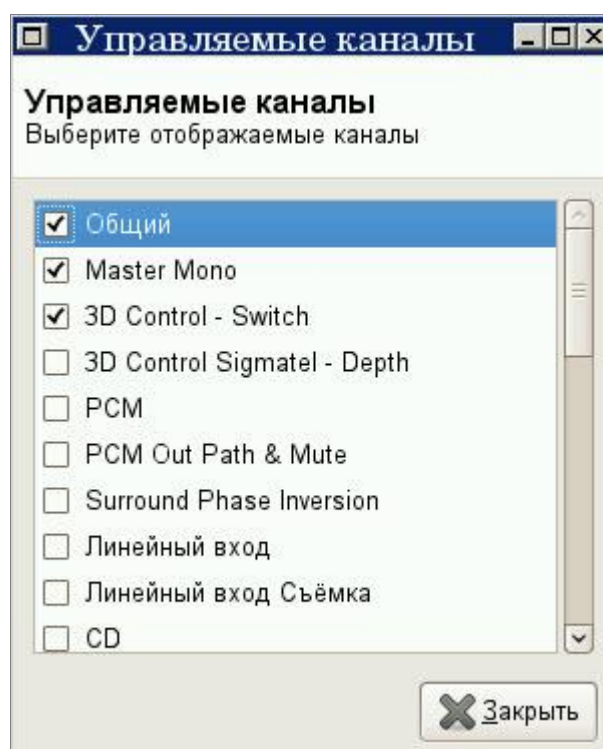


Рис.4.135

#### 4.9.6. Спящий режим

Пользователю предоставляется возможность вводить терминальную станцию в спящий режим. Этот режим применяется при временных перерывах в работе и позволяет вводить терминальную станцию в режим пониженного энергопотребления с сохранением всех работающих приложений. Для ввода системы в спящий режим:

- 1) →[Пуск] на панели задач;
- 2) выбрать в появившемся системном меню пункт *Спящий режим*, на экран выводится диалоговое окно *Спящий режим* (рис. 4.136);
- 3) →[ОК], система входит в спящий режим.

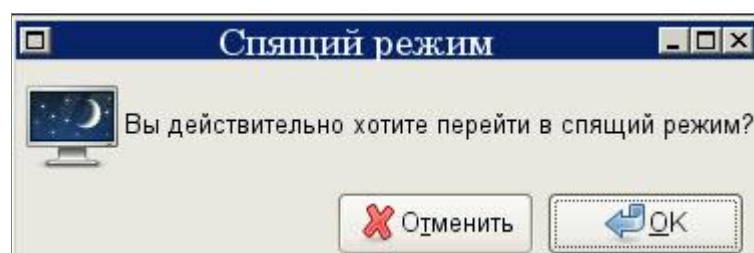


Рис. 4.136



Для выхода из спящего режима нужно нажать кнопку включения/выключения питания (Power).

Примечание. Вводить терминальную станцию в спящий режим возможно путем нажатия кнопки Power на корпусе станции. Для этого предварительно настраиваются действия при нажатии кнопки Power в пункте меню консоли администратора → *Устройства* → *Устройства* (см.п. 4.2.6.1).

#### 4.10. Аутентификации пользователя с помощью USB-ключа (смарт-карты)

Для обеспечения аутентификации пользователя с помощью USB-ключа (смарт-карты) серии eToken при входе в сессии ОС Windows администратору следует выполнить на Windows-сервере установку и настройку специального ПО компании ЗАО «Аладдин Р.Д.» (<http://www.aladdin.ru>), руководствуясь соответствующими инструкциями данного производителя.

Для обеспечения аутентификации пользователя с помощью идентификатора серии Rutoken при входе в сессии ОС Windows администратору следует выполнить на Windows-сервере установку и настройку специального ПО компании ЗАО «Актив-софт» (<http://www.rutoken.ru/>), руководствуясь соответствующими инструкциями данного производителя.

Дополнительная настройка ПО «KTL» для обеспечения аутентификации пользователя с помощью USB-ключа (смарт-карты) не требуется.

## 5. СООБЩЕНИЯ АДМИНИСТРАТОРУ

Системные сообщения - это текстовые или графические сообщения, выводимые на экран монитора в процессе загрузки и работы ОС «Kraftway Terminal Linux», а также в процессе работы ПК «Kraftway Linux Terminal Suite» терминальной станции.

При невозможности открытия требуемой терминальной сессии на экран монитора выводится системное окно об ошибке (рис. 5.1).

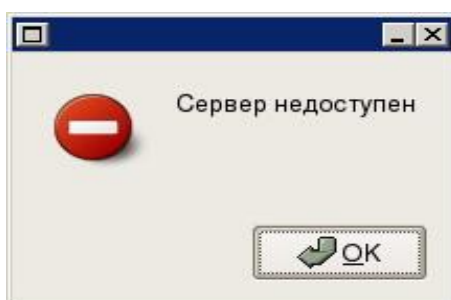


Рис. 5.1

Во время удалённого обновления ПО (см. п. 4.2.5.5) на экран монитора терминальной станции выводится сообщение следующего вида:

Wait upgrade file, from web-interface.

При отсутствии журнала логов выводится системное окно (рис. 5.2).

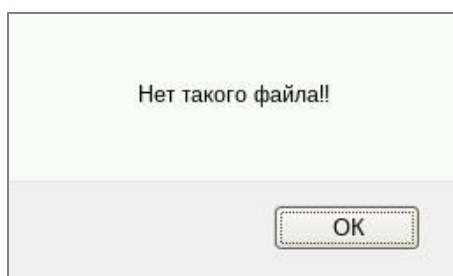


Рис. 5.2

## ПРИЛОЖЕНИЕ 1

## ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

При возникновении различных проблем, связанных с работой ПО «Kraftway Terminal Linux», терминальной станции, а также для получения консультации, пользователю необходимо вначале обратиться в службу технической поддержки или к системному администратору локальной сети своей организации.

Пользователь также может обратиться в Контакт-Центр поддержки пользователей компании Kraftway. Перед обращением в Контакт-Центр поддержки пользователей предлагается:

1) подготовить следующую информацию:

- модель терминальной станции;
- серийный номер терминальной станции;
- версия ПО терминальной станции;
- подробное описание неисправности;
- сообщения об ошибках;
- коды ошибок (при наличии).

2) ознакомиться с дополнительными материалами на веб-странице «Центр поддержки пользователей» (<http://www.kraftway.ru/support/support.php>): часто задаваемые вопросы, документация и т.д.

Примечание. Модель и серийный номер терминальной станции содержатся в гарантийном талоне и специальной наклейке на задней панели терминальной станции.

Консультацию Контакт-Центра поддержки пользователей компании Kraftway можно получить круглосуточно:

1) по телефонам:

- тел. №1: (495) 969-24-04 - для Москвы;
- тел. №2: 8 (800) 200-03-55 - для регионов;

2) через Интернет-форму:

→[интернет-форму] на веб-странице: <http://www.kraftway.ru/support/support.php>

## ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращение/Термин	Наименование и определение
ЛВС	Локальная вычислительная сеть
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
ПСКЗИ	Персональное средство криптографической защиты информации
ALP	Appliance Link Protocol, протокол удаленного доступа, разработанный компанией Oracle, используется в OVDC
BIOS	Basic Input/Output System, базовая система ввода-вывода
ICA	Independent Computer Architecture, протокол удаленного доступа, разработанный компанией Citrix System
KTL	Kraftway Terminal Linux
OVDC	Oracle Virtual Desktop Client, приложение для виртуализации рабочих мест, разработанное компанией Oracle
PCoIP	Personal Computer over Internet Protocol, протокол удаленного доступа, разработанный компанией Teradici
RDP	Remote Desktop Protocol, протокол удаленного доступа, принятый в программных продуктах фирмы Microsoft
Spice	Simple Protocol for Independent Computing Environments, протокол удаленного доступа, разработанный компанией Qumranet
X11	Протокол, определяющий взаимодействие между приложением и системой отображения графики в UNIX системах