ViPNet Terminal 4

Руководство пользователя

infotecs

ФРКЕ.00154-01 34 01

Версия продукта 4.1.8

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, дом 1/23, строение 1

Тел: (495) 737-61-96 (горячая линия), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение 6
О документе 7
Для кого предназначен документ 7
Соглашения документа 7
О программе 9
Назначение ViPNet Terminal 9
Основные возможности ViPNet Terminal 10
Комплект поставки 11
Обратная связь 12

Глава 1. Общие сведения 13
Варианты исполнения ViPNet Terminal 14
Системные требования для варианта исполнения Live USB 15
Аппаратная платформа Kraftway Credo VV18 16
Аппаратная платформа TONK TN1902 17

Глава 2. Начало работы с ViPNet Terminal 19
Подготовка к запуску ViPNet Terminal 20
Запуск ViPNet Terminal в варианте исполнения Live USB 21
Запуск ViPNet Terminal в вариантах исполнения K и T 22
Графический интерфейс ViPNet Terminal 24
Многооконный режим работы 25
Полноэкранный режим работы 27

Глава 3. Настройка ViPNet Terminal с помощью веб-интерфейса 28
Начало работы с веб-интерфейсом ViPNet Terminal 29
Режимы пользователя и администратора 30
Режим ограниченной функциональности 30
Настройка системных параметров 32
Настройка системного времени 32
Настройка параметров экрана 33
Настройка перенаправления звуковых устройств на терминальный сервер 34
Настройка параметров прокси-сервера 35
Настройка подключения к сети 38
Настройка подключения к сети Ethernet 38

Настройка подключения к сети Wi-Fi 39
Настройка подключения к сети 3G 41
Подключение к сети LTE 42
Изменение таблицы маршрутизации 43
Изменение списка DNS-серверов 44
Изменение списка NTP-серверов 45
Изменение списка доступных терминальных серверов 47
Добавление терминального сервера 48
Настройка дополнительных параметров подключения к терминальному серверу 50
Дополнительные параметры подключения к терминальному серверу Windows Server 50
Дополнительные параметры подключения к терминальному серверу Citrix в обычном режиме 52
Дополнительные параметры подключения к терминальному серверу Citrix в «режиме киоска» 54
Дополнительные параметры подключения к терминальному серверу по протоколу HTTP или HTTPS 55
Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами VMware 57
Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами IBS 60
Настройка перенаправления USB-устройств 62
Работа со списком узлов защищенной сети 64
Работа с интегрированным сетевым экраном 66
Общие сведения 66
Основные принципы фильтрации трафика 66
Общие сведения о сетевых фильтрах 67
Использование групп объектов 69
Просмотр сетевых фильтров 70
Просмотр групп объектов 71
Работа с конфигурациями сетевого экрана 72
Описание конфигураций сетевого экрана 72
Смена конфигурации 72

Глава 4. Сценарии работы в терминальной сессии 74
Использование звуковых устройств в терминальной сессии 75
Использование съемных носителей в терминальной сессии 76
Использование электронной подписи в терминальной сессии 77
Печать на локальном принтере в терминальной сессии 78

Установка принтера 79
Участие в видеоконференциях 84
Участие в видеоконференции TrueConf 84
Участие в видеоконференции Vinteo 85

Приложение A. Глоссарий 87

Приложение B. Указатель 92

Введение

О документе 7

О программе 9

Комплект поставки 11

Обратная связь 12

О документе

Для кого предназначен документ

Документ предназначен для пользователей программного обеспечения ViPNet Terminal. Предполагается, что пользователи имеют навыки работы с веб-браузером Firefox и общее представление о настройке его подключения через прокси-сервер.

В документе содержится информация, необходимая для запуска ViPNet Terminal, описывается работа с веб-интерфейсом. В документе также приведены типовые сценарии работы в терминальной сессии: работа со звуковыми и съемными носителями, использование электронной подписи, печать на локальном принтере.

Сценарии работы с веб-интерфейсом, требующие прав администратора, а также сценарии настройки ViPNet Terminal с помощью командного интерпретатора описаны в руководстве «ViPNet Terminal. Руководство администратора».

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе

Назначение ViPNet Terminal

Программное обеспечение ViPNet Terminal предназначено для организации защищенного рабочего места пользователя сети ViPNet и выполняет функцию тонкого клиента (см. Глоссарий, стр. 91).

ПО ViPNet Terminal может поставляться в базовом и минимальном вариантах.

В минимальном варианте ViPNet Terminal позволяет организовать следующие виды защищенного удаленного доступа:

- Доступ к удаленному рабочему столу на терминальном сервере (см. глоссарий, стр. 90) Windows Server 2003/2008/2008 R2/2012/2012 R2 (по протоколу RDP).
- Доступ к удаленному рабочему столу и опубликованным приложениям на сервере Citrix (по протоколам ICA, HTTP/HTTPS).
- Доступ к службам, реализованным по технологии Web Access (по протоколам HTTP и HTTPS).
- Доступ к виртуальным рабочим столам, реализованным по технологии VMware Horizon View (по протоколам PCoIP, Blast и RDP).

В базовом варианте также доступны следующие функции:

- Доступ к виртуальным рабочим столам, реализованным по технологии IBS Parallels VDI.
- Доступ к виртуальным рабочим столам, реализованным по технологии Fusion Access (по протоколу HDP — Huawei Desktop Protocol).
- Доступ к видеоконференциям TrueConf и Vinteo.

Преимущество работы в режиме терминального клиента заключается в снижении расходов на программное и аппаратное обеспечение, уменьшении затрат времени на администрирование, повышении уровня защиты от внутренних злоумышленников.

С точки зрения технологии ViPNet, узел с ПО ViPNet Terminal является клиентом сети ViPNet. ПО ViPNet Terminal осуществляет шифрование IP-трафика и выполняет функции персонального сетевого экрана. Терминальный сервер может быть расположен на защищенном узле ViPNet или на узле, который туннелируется координатором ViPNet. Тем самым обеспечивается защита ViPNet Terminal от сетевых атак и вмешательства в терминальную сессию пользователя.

Основные возможности ViPNet Terminal

При работе на компьютере с программным обеспечением ViPNet Terminal пользователю предоставляются следующие возможности:

- Подключение к заданным терминальным серверам (см. «Изменение списка доступных терминальных серверов» на стр. 47).
- Использование в терминальной сессии электронной подписи (см. «Использование электронной подписи в терминальной сессии» на стр. 77).
- Использование в терминальной сессии следующих устройств, подключенных к компьютеру с ПО ViPNet Terminal:
  - звуковых устройств (см. «Использование звуковых устройств в терминальной сессии» на стр. 75);
  - съемных носителей (см. «Использование съемных носителей в терминальной сессии» на стр. 76);
  - принтера (см. «Печать на локальном принтере в терминальной сессии» на стр. 78);
  - USB-устройств (веб-камер, сканеров и других) (см. «Настройка перенаправления USB-устройств» на стр. 62).
- Обмен данными между разными терминальными сессиями с использованием буфера обмена.

Комплект поставки

ViPNet Terminal поставляется либо в виде образа ПО, либо в одном из вариантов с предустановленным ПО:

- Образ загрузочного диска базовой версии ПО `terminal_vipnet_base_i386_x.x.x-xxxx.usb.img` или образ загрузочного диска минимальной версии ПО `terminal_vipnet_minimal_i386_x.x.x-xxxx.usb.img`.
- Образ установочного диска базовой версии ПО `terminal_vipnet_base_i386_x.x.x-xxxx.img` или образ установочного диска минимальной версии ПО `terminal_vipnet_minimal_i386_x.x.x-xxxx.img`.
- USB Flash.
- Компактный компьютер Kraftway Credo VV18.
- Компактный компьютер TONK TN1902.

В комплект поставки также входит документация в формате PDF:

- «ViPNet Terminal. Быстрый старт».
- «ViPNet Terminal. Общее описание».
- «ViPNet Terminal. Установка и обновление».
- «ViPNet Terminal. Руководство пользователя».
- «ViPNet Terminal. Руководство администратора».
- «Справочное руководство по командному интерпретатору. Приложение к руководству администратора ViPNet Terminal».
- «Справочное руководство по конфигурационным файлам. Приложение к руководству администратора ViPNet Terminal».
- «ViPNet Terminal. API ЭП в браузере Firefox. Руководство разработчика».

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения http://infotecs.ru/products/disclosure.php. Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru.

1

Общие сведения

Варианты исполнения ViPNet Terminal 14

Системные требования для варианта исполнения Live USB 15

Аппаратная платформа Kraftway Credo VV18 16

Аппаратная платформа TONK TN1902 17

Варианты исполнения ViPNet Terminal

ViPNet Terminal имеет три варианта исполнения. Эти варианты отличаются носителем, который используется в качестве загрузочного:

- Исполнение Live USB — в качестве загрузочного используется USB-носитель.
- Исполнение K — исполнение на базе компактного компьютера Kraftway Credo VV18 (см. «Аппаратная платформа Kraftway Credo VV18» на стр. 16). В этом варианте в качестве загрузочного носителя используется встроенная карта CompactFlash.
- Исполнение T — исполнение на базе компактного компьютера TONK TN1902 (см. «Аппаратная платформа TONK TN1902» на стр. 17). В этом варианте в качестве загрузочного носителя используется встроенный SSD-диск.

Программное обеспечение ViPNet Terminal функционирует под управлением операционной системы Linux. В качестве консоли используются монитор и клавиатура.

Системные требования для варианта исполнения Live USB

В варианте исполнения Live USB в качестве загрузочного должен использоваться USB-носитель объемом не менее 4 Гбайт. Для операции удаленного обновления ПО необходим USB-носитель объемом не менее 8 Гбайт.

ViPNet Terminal в варианте исполнения Live USB рекомендуется использовать на IBM-совместимых компьютерах (стационарных или портативных) следующей конфигурации:

- Процессор — не менее Intel Pentium III.
- Оперативная память — не менее 2 Гбайт.
- Сетевые интерфейсы — один интерфейс Ethernet 10/100/1000 (Ethernet 10/100).
- Разъемы USB 2.0 — не менее трех.
- Графический адаптер — карта VGA.

Аппаратная платформа Kraftway Credo VV18

В варианте исполнения K в качестве аппаратной платформы для программного обеспечения ViPNet Terminal используется компактный компьютер Kraftway Credo VV18. Компьютер представляет собой вычислительную платформу на базе процессора Intel Atom с частотой 1,66 ГГц. Компьютер выполнен в прочном корпусе, устойчив к пыли и вибрациям, обладает низким уровнем энергопотребления и тепловыделения, имеет миниатюрные размеры и малый вес. Он может устанавливаться на столе или крепиться по стандарту VESA 100 на любую поверхность, в том числе на заднюю стенку монитора.

На передней панели компьютера Kraftway Credo VV18 расположены два разъема USB, два аудиоразъема и кнопка питания. Остальные коммуникационные разъемы находятся на задней панели компьютера.

Рисунок 1. Задняя панель компьютера Kraftway Credo VV18

Компьютер Kraftway Credo VV18 имеет следующие технические характеристики:

Таблица 3. Характеристики компактного компьютера Kraftway Credo VV18

Описание	Характеристика
Процессор	Intel Atom N450, FSB 667; 1,66 ГГц
Оперативная память	2 Гбайт
Сетевые интерфейсы	1 интерфейс Ethernet 10/100/1000 Мбит/с Адаптер Wi-Fi 802.11b/g
Графический адаптер	VGA, максимальное разрешение 2048x1536
Накопитель	CompactFlash от 4 Гбайт
Разъемы ввода-вывода	6 разъемов USB 2.0 1 разъем VGA (D-Sub) 1 разъем RJ-45
Мощность источника питания	36 Вт (внешний адаптер AC-DC)

Аппаратная платформа TONK TN1902

В варианте исполнения T в качестве аппаратной платформы для программного обеспечения ViPNet Terminal используется компактный компьютер TONK TN1902. Компьютер представляет собой вычислительную платформу на базе 4-ядерного процессора INTEL Baytrail-D J1900 с частотой 2,41 ГГц. Компьютер выполнен в компактном корпусе, обладает высоким уровнем производительности, имеет миниатюрные размеры и малый вес. Он может устанавливаться на столе или крепиться по стандарту VESA 100 на любую поверхность, в том числе на заднюю стенку монитора.

На передней панели компьютера TONK TN1902 расположен разъем USB 3.0, два аудиоразъема и кнопка питания. Остальные коммуникационные разъемы находятся на задней панели компьютера.

Рисунок 2. Передняя и задняя панели компьютера TONK TN1902

Компьютер TONK TN1902 имеет следующие технические характеристики:

Таблица 4. Характеристики компактного компьютера TONK TN1902

Описание	Характеристика
Процессор	INTEL Baytrail-D J1900 Quad-Core; 2.42GHz
Оперативная память	4 Гбайт
Сетевые интерфейсы	1 интерфейс Ethernet 10/100/1000 Мбит/с Адаптер Wi-Fi 802.11b/g
Графический адаптер	Intel® Graphics Media Accelerator 3600, максимальное разрешение 1920x1200 (DVI), 2560x1600 (Display Port)
Накопитель	SSD 16 Гбайт
Разъемы ввода-вывода	5 разъемов USB 2.0 1 разъем USB 3.0 1 разъем Display Port 1 разъем DVI 1 разъем RJ-45
Мощность источника питания	10 Вт (внешний адаптер AC-DC)

2

Начало работы с ViPNet Terminal

Подготовка к запуску ViPNet Terminal 20

Запуск ViPNet Terminal в варианте исполнения Live USB 21

Запуск ViPNet Terminal в вариантах исполнения K и T 22

Графический интерфейс ViPNet Terminal 24

Многооконный режим работы 25

Полноэкранный режим работы 27

Подготовка к запуску ViPNet Terminal

Для возможности запуска ViPNet Terminal необходимо предварительно установить справочники и ключи сетевого узла ViPNet. Процедура установки подробно описана в документе «ViPNet Terminal. Установка и обновление».

Во время установки справочников и ключей требуется указать способ аутентификации пользователя, который зависит от того, где сохранены ключи пользователя:

- Аутентификация по паролю, если ключи пользователя сохранены в файле дистрибутива.
- Аутентификация с использованием внешнего устройства, если ключи пользователя сохранены на устройстве аутентификации.

О выбранном способе аутентификации вы можете узнать у администратора вашей сети ViPNet. Администратор также должен сообщить вам пароль пользователя сетевого узла или предоставить внешнее устройство аутентификации вместе с ПИН-кодом.

Запуск ViPNet Terminal в варианте исполнения Live USB

Если вы используете ViPNet Terminal в варианте исполнения Live USB (см. «Варианты исполнения ViPNet Terminal» на стр. 14), выполните следующие действия:

1. Выключите компьютер и подключите к нему загрузочный USB-носитель с программным обеспечением ViPNet Terminal.
2. Включите компьютер.
3. Если ранее в качестве загрузочного диска не был установлен USB-носитель:
   - Во время автоматического теста оборудования нажмите клавишу **Delete**, чтобы войти в режим настройки BIOS.
   - Настройте загрузку с USB-носителя и выйдите из BIOS с сохранением настроек.
4. Если для аутентификации пользователя используется внешнее устройство, подключите его к USB-разъему компьютера.

Внимание! Не подключайте к ViPNet Terminal более одного устройства аутентификации.

---

5. При загрузке операционной системы в соответствующем окне введите пароль пользователя ViPNet либо ПИН-код внешнего устройства аутентификации (в зависимости от способа аутентификации, который был указан при установке справочников и ключей). Затем нажмите клавишу **Enter**.

Примечание. Если вы несколько раз подряд ввели неверный пароль, ввели неверный ПИН-код или подключили неверное внешнее устройство аутентификации, чтобы сделать очередную попытку аутентификации, подождите несколько секунд.

Задержка реализована для предотвращения возможности подбора пароля, ПИН-кода или подходящего устройства методом перебора. Если вы ввели неверный пароль или ПИН-код либо подключичили неверное устройство аутентификации 10 раз подряд, ViPNet Terminal выключается.

После загрузки операционной системы появится рабочий стол ViPNet Terminal (см. «Графический интерфейс ViPNet Terminal» на стр. 24).

6. При необходимости настройте системное время (см. «Настройка системного времени» на стр. 32) и параметры подключения к сети (см. «Настройка подключения к сети» на стр. 38).
7. Для начала работы подключитесь к терминальному серверу или веб-ресурсам.

Запуск ViPNet Terminal в вариантах исполнения K и T

Если вы используете ViPNet Terminal в вариантах исполнения K или T (см. «Варианты исполнения ViPNet Terminal» на стр. 14), выполните следующие действия:

1 Включите компактный компьютер.

2 Если для аутентификации пользователя используется внешнее устройство, подключите его к USB-разъему компьютера.

Внимание! Не подключайте к ViPNet Terminal более одного устройства аутентификации.

3 При загрузке операционной системы в соответствующем окне введите пароль пользователя ViPNet либо ПИН-код внешнего устройства аутентификации (в зависимости от способа аутентификации, который был указан при установке справочников и ключей). Затем нажмите клавишу **Enter**.

Примечание. Если вы несколько раз подряд ввели неверный пароль, ввели неверный ПИН-код или подключили неверное внешнее устройство аутентификации, чтобы сделать очередную попытку аутентификации, подождите несколько секунд.

Задержка реализована для предотвращения возможности подбора пароля, ПИН-кода или подходящего устройства методом перебора. Если вы ввели неверный пароль или ПИН-код либо подключичили неверное устройство аутентификации 10 раз подряд, ViPNet Terminal выключается.

4 Если аппаратная платформа компьютера является сертифицированной, но параметры BIOS были изменены, то появится предложение восстановить параметры BIOS, заверенные сертифицирующим органом.

```
BIOS settings are NOT default!
Please, reset BIOS settings!
Enter <y> to reset bios settings and reboot or <n> to continue booting [y/n] _
```

Рисунок 3. Предложение восстановить параметры BIOS, заверенные сертифицирующим органом

Для восстановления параметров BIOS введите символ «y», после чего компьютер автоматически перезагрузится. Чтобы продолжить загрузку операционной системы без изменения параметров BIOS, введите символ «n». Однако в этом случае после запуска ViPNet Terminal не будет иметь доступа к сети.

Для несертифицированной аппаратной платформы проверка параметров BIOS не производится.

После загрузки операционной системы появится рабочий стол ViPNet Terminal (см. «Графический интерфейс ViPNet Terminal» на стр. 24).

5 При необходимости настройте системное время (см. «Настройка системного времени» на стр. 32) и параметры подключения к сети (см. «Настройка подключения к сети» на стр. 38).

6 Для начала работы подключитесь к терминальному серверу или веб-ресурсам.

Графический интерфейс ViPNet Terminal

После запуска компьютера с программным обеспечением ViPNet Terminal автоматически загружается графический интерфейс пользователя. В зависимости от заданных параметров графического интерфейса рабочий стол ViPNet Terminal может работать в одном из двух режимов:

- Многооконный режим работы (на стр. 25). В этом режиме на рабочем столе может быть одновременно открыто несколько окон терминальных сессий и веб-браузера Firefox.
- Полноэкранный режим работы (на стр. 27). В этом режиме автоматически выполняется подключение к терминальному серверу по умолчанию, окно терминальной сессии или веб-браузера Firefox разворачивается на весь экран.

Примечание. Чтобы перейти из многооконного режима рабочего стола в полноэкранный, при настройке параметров экрана в веб-интерфейсе (см. «Настройка параметров экрана» на стр. 33) снимите соответствующий флажок и в появившемся окне нажмите кнопку **OK**.

Чтобы перейти из полноэкранного режима рабочего стола в многооконный, обратитесь к администратору ViPNet Terminal.

Многооконный режим работы

В многооконном режиме работы после загрузки операционной системы на экране появляется рабочий стол. В нижней части экрана находятся панель задач и кнопка меню .

Чтобы начать работу, нажмите кнопку и в появившемся меню выберите один из пунктов:

- Один из заданных терминальных серверов, чтобы запустить терминальную сессию (см. Глоссарий, стр. 90) или подключиться к веб-ресурсам. Список доступных терминальных серверов расположен в верхней части меню.
- Пункт **Видеоконференция**, чтобы открыть клиент видеоконференций TrueConf.
- Пункт **Настройка**, чтобы настроить параметры ViPNet Terminal (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29).
- Пункт **Принтеры**, чтобы установить локальный принтер (см. «Установка принтера» на стр. 79).

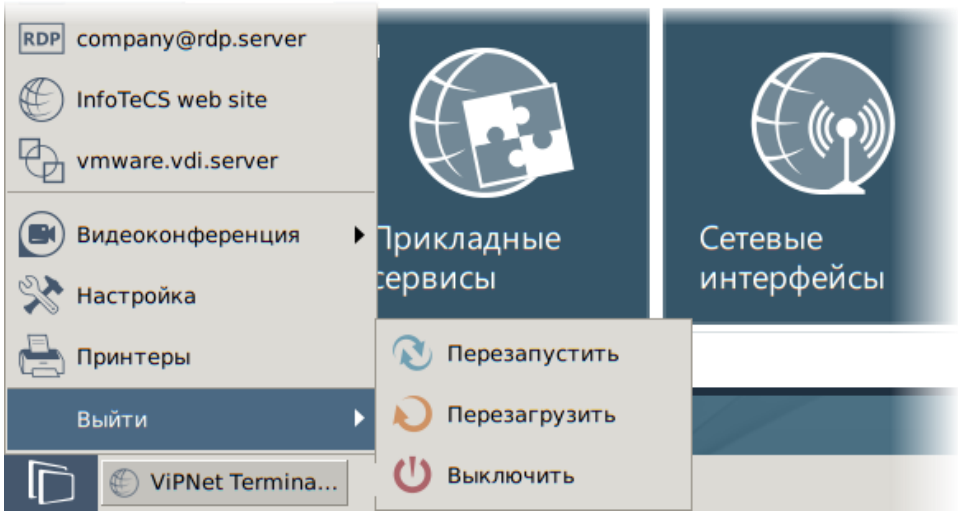

Рисунок 4. Многооконный режим работы

Каждая запущенная терминальная сессия открывается в отдельном окне. Доступ к веб-ресурсам, настройка ViPNet Terminal через веб-интерфейс и установка принтера выполняются в окне веб-браузера Firefox.

Вы можете запустить веб-браузер Firefox и несколько терминальных сессий одновременно. Все открытые окна отображаются на панели задач.

В правой части панели задач находятся следующие элементы:

- Кнопка регулировки громкости . Чтобы изменить громкость подключенных к компьютеру устройств воспроизведения звука, щелкните значок и установите уровень громкости с помощью ползунка.
- Индикатор раскладки клавиатуры. Чтобы изменить раскладку, щелкните значок RU или EN либо нажмите клавиши **Alt+Shift**.

- Индикатор подключения к защищенной сети (см. Глоссарий, стр. 88). Чтобы просмотреть информацию о статусе подключения к защищенной сети ViPNet и активном сетевом интерфейсе, наведите указатель мыши на индикатор подключения. Чтобы обновить информацию о статусе подключения, щелкните индикатор.
- Текущая дата и время. Щелкнув поле, в котором отображаются дата и время, вы можете открыть календарь.

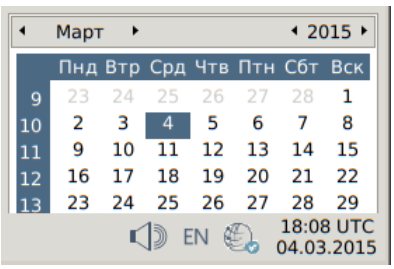

Рисунок 5. Значки уведомлений на панели задач

Для завершения работы или перезагрузки компьютера нажмите кнопку , в появившемся меню выберите **Выйти** и затем щелкните один из пунктов:

- **Перезапустить** — чтобы перезапустить графический интерфейс ViPNet Terminal.
- **Перезагрузить** — чтобы перезагрузить компьютер.
- **Выключить** — чтобы выключить компьютер.

Полноэкранный режим работы

Полноэкранный режим работы предназначен для случаев, когда требуется ограничить доступ к настройке ViPNet Terminal, например на информационных табло и подобных устройствах.

В полноэкранном режиме после загрузки операционной системы выполняется автоматическое подключение к терминальному серверу, который задан в качестве сервера по умолчанию. Подключение к другим терминальным серверам, открытие других окон и изменение языка с помощью графического интерфейса невозможно, не отображаются панель задач и кнопка меню .

3

Настройка ViPNet Terminal с помощью веб-интерфейса

Начало работы с веб-интерфейсом ViPNet Terminal 29

Настройка системных параметров 32

Настройка подключения к сети 38

Изменение списка доступных терминальных серверов 47

Работа со списком узлов защищенной сети 64

Работа с интегрированным сетевым экраном 66

Начало работы с веб-интерфейсом ViPNet Terminal

Если вы работаете в многооконном режиме, вы можете настроить параметры ViPNet Terminal с помощью веб-интерфейса. Для этого выполните следующие действия:

1 Нажмите кнопку и в меню выберите пункт **Настройка**, откроется начальная страница настройки ViPNet Terminal.

Рисунок 6. Начальная страница настройки ViPNet Terminal

2 Для настройки и просмотра параметров ViPNet Terminal щелкните одну из плиток:

- **ViPNet VPN** (см. «Работа со списком узлов защищенной сети» на стр. 64).
- **Межсетевой экран** (см. «Работа с интегрированным сетевым экраном» на стр. 66).
- **Терминальные серверы** (см. «Изменение списка доступных терминальных серверов» на стр. 47).

- **Прикладные сервисы**.
- **Сетевые интерфейсы** (см. «Настройка подключения к сети» на стр. 38).
- **Системные настройки** (см. «Настройка системных параметров» на стр. 32).

3 Чтобы изменить язык интерфейса, щелкните ссылку с названием языка в нижней части окна.

4 Чтобы узнать версию программного обеспечения ViPNet Terminal вашего сетевого узла, щелкните значок в правом верхнем углу окна.

Режимы пользователя и администратора

Взаимодействие с веб-интерфейсом ViPNet Terminal может осуществляться в двух режимах:

- В режиме пользователя вы можете выполнять следующие действия:
  - Настраивать системные параметры ViPNet Terminal, в том числе разрешать или запрещать перенаправление на терминальный сервер звуковых устройств.
  - Изменять настройки сетевых интерфейсов.
  - Изменять настройки прикладных сервисов.
  - Настраивать подключение к терминальным серверам.
  - Просматривать список узлов сети ViPNet.
  - Просматривать списки сетевых фильтров, заданных для своего сетевого узла.
  - Просматривать списки групп объектов различных типов.
- В режиме администратора вам доступны все возможности пользователя. Кроме того вы можете выполнять следующие действия:
  - Создавать и изменять уже имеющиеся сетевые фильтры и группы объектов (см. документ «ViPNet Terminal. Руководство администратора»).
  - Разрешать или запрещать перенаправление на терминальный сервер локальных устройств всех доступных типов (см. документ «ViPNet Terminal. Руководство администратора»).

Режим ограниченной функциональности

В случае выключения одного или нескольких основных процессов ViPNet Terminal (iplircfg, failoverd) веб-интерфейс переходит в режим ограниченной функциональности. При этом появляется сообщение со списком остановленных процессов и функций, управление которыми будет недоступно в этом режиме.

В режиме ограниченной функциональности в случае остановки демона iplircfg целиком блокируются разделы **ViPNet VPN** и **Межсетевой экран**.

Вы можете просмотреть информацию об остановленных процессах, недоступных разделах веб-интерфейса или ограниченных функциях, щелкнув специальный значок в верхнем правом углу страницы .

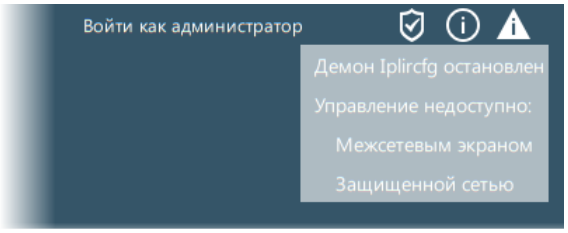

Рисунок 7. Просмотр информации об ограничениях функциональности

Настройка системных параметров

Перед началом использования ViPNet Terminal рекомендуется настроить такие параметры, как системное время, режим энергосбережения монитора и перенаправление локальных устройств на терминальный сервер.

Настройка системного времени

Чтобы компьютер с программным обеспечением ViPNet Terminal корректно взаимодействовал с другими защищенными узлами ViPNet, необходимо правильно настроить системную дату и время.

Внимание! Если системные дата и время заданы неверно, защищенные соединения с другими узлами ViPNet могут быть заблокированы.

Чтобы настроить системное время, выполните следующие действия:

1. На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Системные настройки**.
2. На странице **Системные настройки** откройте вкладку **Дата и время**.
3. Задайте часовой пояс, дату и время:
   - В соответствующем списке выберите часовой пояс, в котором вы находитесь.
   - В поле **Дата** щелкните значок и выберите текущую дату.
   - В соответствующее поле введите текущее время.
   - С помощью переключателя укажите, какое время установлено в BIOS компьютера:
     - **UTC** — в BIOS установлено время UTC. В этом случае системное время рассчитывается на основании времени, заданного в BIOS, с поправкой на выбранный часовой пояс.
     - **Локальное** — в BIOS установлено локальное время. В этом случае время, заданное в BIOS, считается корректным системным временем для выбранного часового пояса.

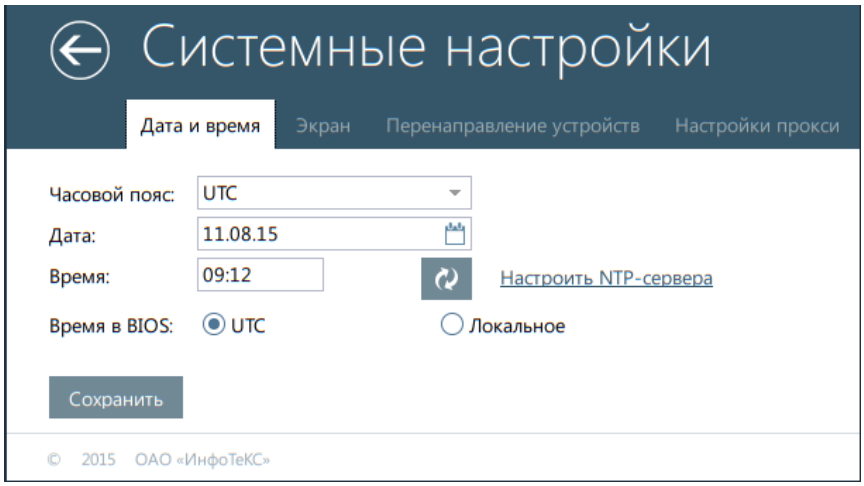

Рисунок 8. Настройка системного времени

4 Чтобы применить изменения, нажмите кнопку **Сохранить**. При этом системное время будет установлено с учетом настройки времени в BIOS.

5 Чтобы синхронизировать время с серверами точного времени, щелкните значок **Синхронизировать с NTP-сервером** .

По умолчанию в качестве серверов точного времени используются публичные NTP-серверы из кластера `pool.ntp.org`. В случае необходимости вы можете дополнить список NTP-серверов, например добавить корпоративный NTP-сервер (см. «Изменение списка NTP-серверов» на стр. 45).

Внимание! На узлах ViPNet Terminal в варианте исполнения Live USB синхронизированное время не записывается в BIOS. Поэтому после синхронизации не нажимайте кнопку **Сохранить**, иначе системное время может оказаться неправильным.

Настройка параметров экрана

В случае необходимости вы можете изменить разрешение экрана и настроить режим энергосбережения. Если режим энергосбережения включен, при отсутствии действий пользователя через 5 минут гаснет изображение на экране, через 30 минут отключается питание монитора.

Чтобы изменить параметры экрана, выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Системные настройки**.

2 На странице **Системные настройки** откройте вкладку **Экран**.

3 Чтобы изменить разрешение экрана, в списке **Размер экрана графической сессии** выберите нужное значение. По умолчанию установлено значение **auto** — оптимальное разрешение определяется автоматически.

Примечание. Если к ViPNet Terminal подключены два монитора, то настройка применяется к обоим мониторам одновременно.

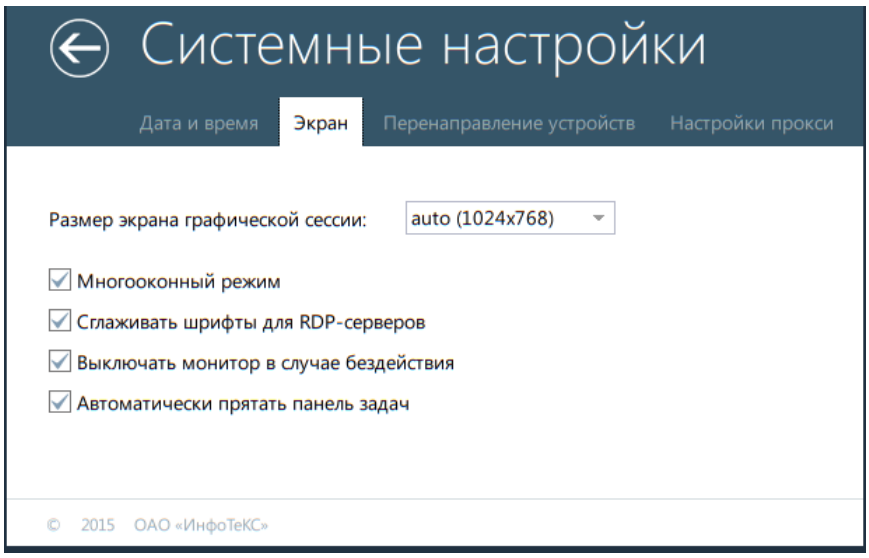

Рисунок 9. Настройка параметров экрана

4 Чтобы переключить в полноэкранный режим работы рабочего стола, снимите флажок **Многооконный режим** и в появившемся окне нажмите кнопку **OK**.

Примечание. Чтобы перейти из полноэкранного режима рабочего стола в многооконный, обратитесь к администратору ViPNet Terminal.

5 Во время терминальных сессий, установленных по протоколу RDP, для отображения шрифтов по умолчанию используется метод сглаживания ClearType. Чтобы не использовать сглаживание, снимите флажок **Сглаживать шрифты для RDP-серверов**.

6 Чтобы включить или отключить режим энергосбережения, установите или снимите флажок **Выключать монитор в случае бездействия**. По умолчанию режим энергосбережения включен.

7 При работе в многооконном режиме для увеличения рабочего пространства на экране вы можете скрыть панель задач. При этом она будет появляться только при подведении указателя мыши к нижней границе экрана. Чтобы скрыть панель задач, установите флажок **Автоматически прятать панель задач**.

Настройка перенаправления звуковых устройств на терминальный сервер

При подключении к терминальным серверам Windows Server или Citrix, а также при подключении к виртуальным рабочим столам вы можете использовать различные локальные устройства,

подключенные к компьютеру с программным обеспечением ViPNet Terminal (см. «Основные возможности ViPNet Terminal» на стр. 10). С помощью веб-интерфейса вы можете настроить перенаправление звуковых устройств, а также проверить настройку перенаправления других устройств. Для этого выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Системные настройки**.

2 На странице **Системные настройки** откройте вкладку **Перенаправление устройств**.

На вкладке **Перенаправление устройств** находится список локальных устройств с текущими настройками перенаправления.

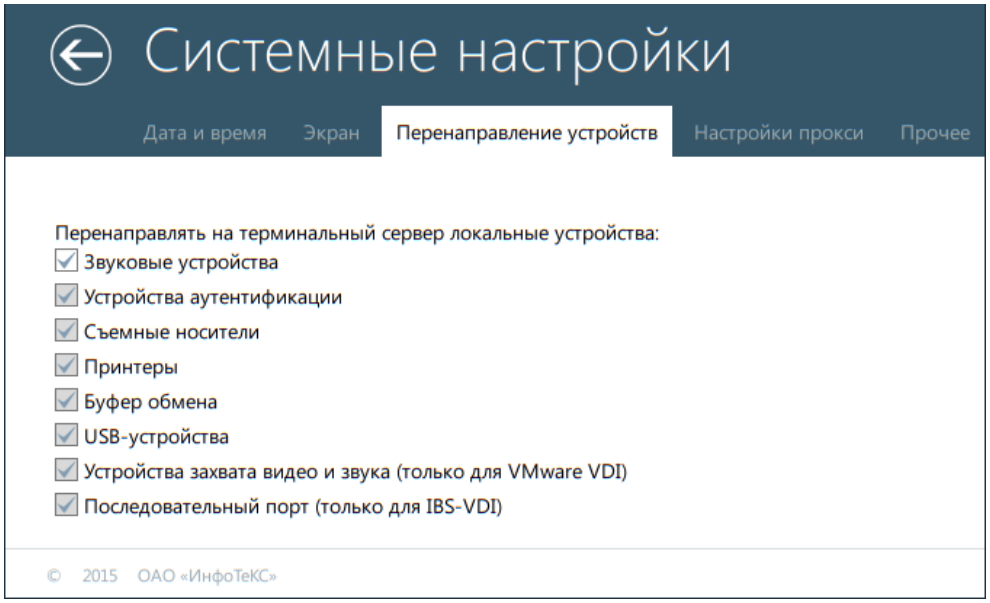

Рисунок 10. Настройка перенаправления устройств на терминальный сервер

3 Чтобы разрешить или запретить перенаправление звуковых устройств на терминальный сервер, установите или снимите флажок **Звуковые устройства**.

Примечание. Для регулировки громкости устройств воспроизведения звука воспользуйтесь кнопкой на панели задач (см. «Многооконный режим работы» на стр. 25).

4 Чтобы разрешить или запретить перенаправление других устройств, обратитесь к администратору ViPNet Terminal.

Настройка параметров прокси-сервера

Если в вашей сети для доступа к сети Интернет используется прокси-сервер (см. Глоссарий, стр. 90), вам необходимо задать его параметры. Параметры прокси-сервера вы можете узнать у вашего сетевого администратора.

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Системные настройки**.

2 На странице **Системные настройки** откройте вкладку **Настройки прокси**.

3 Выберите режим использования прокси-сервера:

- **Без прокси** — чтобы отключить использование прокси-сервера.
- **Ручная настройка службы прокси** — чтобы включить использование прокси-сервера и задать его параметры.

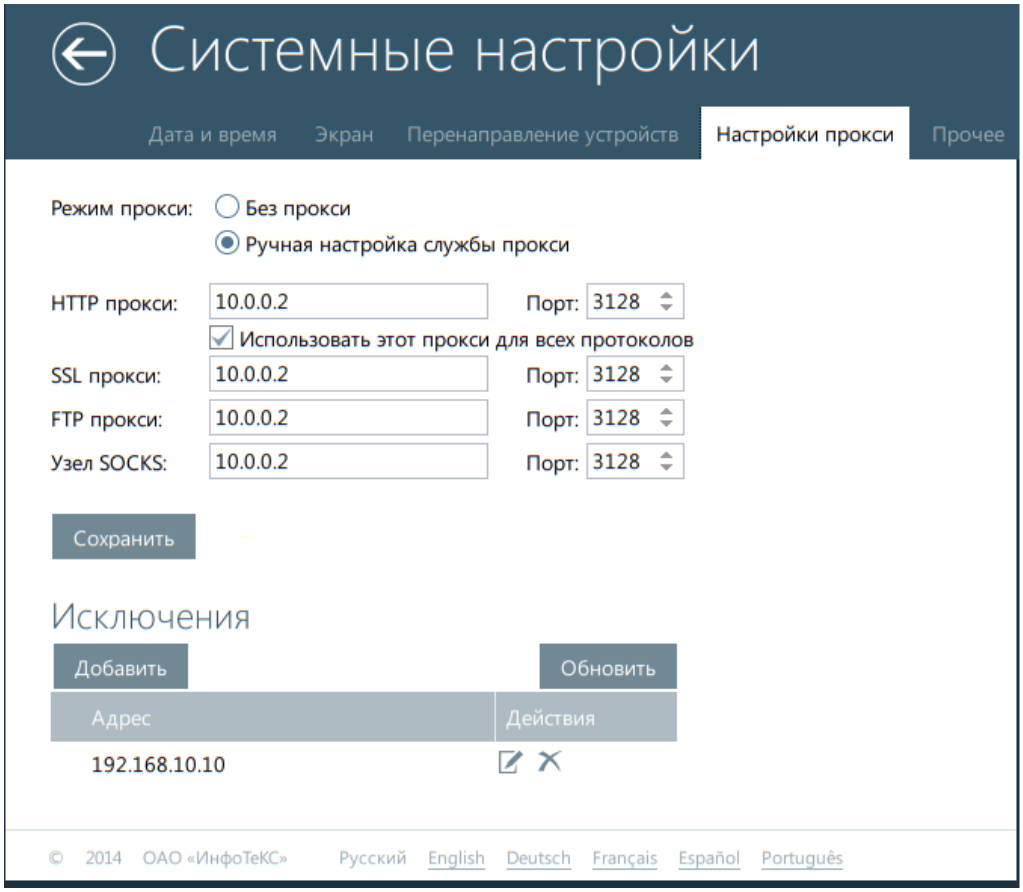

Рисунок 11. Настройка параметров прокси-сервера

4 Если вы включили использование прокси-сервера, укажите следующие параметры:

- В поле **HTTP прокси** задайте IP-адрес или DNS-имя прокси-сервера.
- В поле **Порт** укажите номер порта.
- Установите флажок **Использовать этот прокси для всех протоколов**, если для всех протоколов используется один и тот же прокси-сервер.

  Если для разных протоколов — HTTP, SSL, FTP или SOCKS — требуются отдельные прокси-серверы, снимите флажок **Использовать этот прокси для всех протоколов** и укажите адрес и порт прокси-сервера для каждого протокола.

Если для подключения к отдельным адресам не нужно использовать прокси-сервер, нажмите кнопку **Добавить** и задайте исключение. В качестве исключения можно указать IP-адрес или DNS-имя, подсеть в формате CIDR или домен. Таким образом вы можете задать список исключений.

Для изменения отдельного исключения щелкните значок в строке этого исключения, для удаления — значок .

При необходимости вы можете обновить список исключений с помощью соответствующей кнопки.

5 Чтобы сохранить настройки прокси-сервера, нажмите кнопку **Сохранить**.

Настройка подключения к сети

Для подключения к терминальным серверам и работы с защищенными веб-ресурсами необходимо физическое подключение к сети. Программное обеспечение ViPNet Terminal поддерживает следующие типы подключения: Ethernet (на стр. 87), Wi-Fi (см. Глоссарий, стр. 88), 3G (см. Глоссарий, стр. 87), LTE (см. Глоссарий, стр. 88). Возможность выбора типов подключения зависит от конфигурации вашего компьютера.

Настройка подключения к сети Ethernet

Чтобы настроить подключение ViPNet Terminal к сети Ethernet, выполните следующие действия:

1. На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Сетевые интерфейсы**.
2. На странице **Сетевые интерфейсы** откройте вкладку **Ethernet**.
3. На вкладке **Ethernet** убедитесь, что сетевой интерфейс включен (переключатель находится в положении). Чтобы включить сетевой интерфейс, щелкните переключатель.

Примечание. Если в момент включения сетевого интерфейса Ethernet включены какие-либо другие сетевые интерфейсы, появится предупреждение об их автоматическом отключении. В окне предупреждения нажмите кнопку **OK**.

---

4. Выберите режим настройки подключения к сети Ethernet:
   - **Автоматически** — чтобы автоматически получить параметры сетевого подключения от DHCP-сервера (если в сети существует DHCP-сервер).
   - **Вручную** — чтобы задать параметры сетевого подключения самостоятельно.

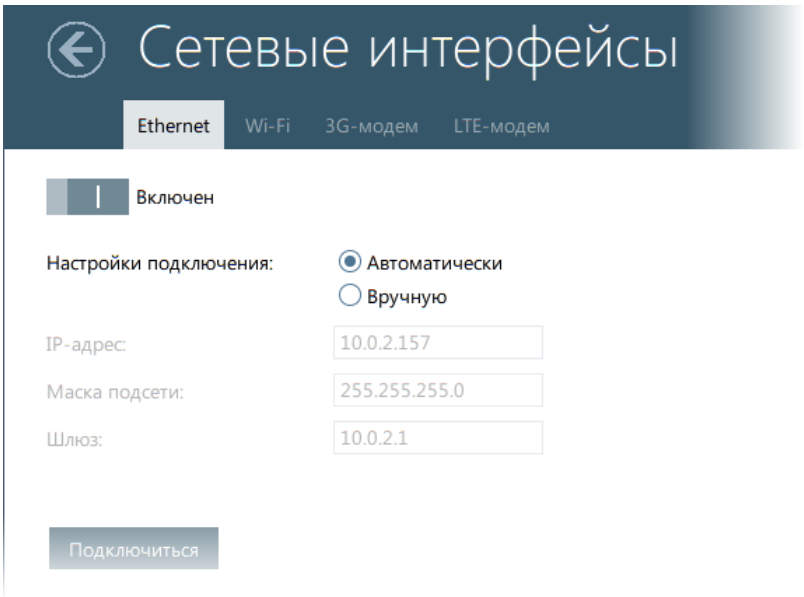

Рисунок 12. Настройка подключения к сети Ethernet

5 Если вы выбрали настройку вручную, укажите следующие параметры:

- В поле **IP-адрес** задайте IP-адрес вашего компьютера.
- В поле **Маска подсети** укажите маску.
- В поле **Шлюз** укажите IP-адрес шлюза по умолчанию.

6 Чтобы сохранить параметры подключения, заданные вручную, или получить параметры автоматически, нажмите кнопку **Подключиться**.

7 Если вы настроили подключение вручную, рекомендуется указать адреса используемых в сети DNS-серверов (см. «Изменение списка DNS-серверов» на стр. 44) и NTP-серверов (см. «Изменение списка NTP-серверов» на стр. 45).

Если вы выбрали автоматическую настройку сетевого подключения, информация о доступных DNS-серверах и NTP-серверах может быть получена от DHCP-сервера.

Настройка подключения к сети Wi-Fi

Если компьютер с ПО ViPNet Terminal укомплектован адаптером Wi-Fi, вы можете настроить подключение к беспроводной сети Wi-Fi (см. Глоссарий, стр. 88). Для этого выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Сетевые интерфейсы**.

2 На странице **Сетевые интерфейсы** откройте вкладку **Wi-Fi**.

3 На вкладке **Wi-Fi** убедитесь, что сетевой интерфейс Wi-Fi включен (переключатель находится в положении). Чтобы включить сетевой интерфейс, щелкните переключатель.

Примечание. Если в момент включения интерфейса Wi-Fi включены какие-либо другие сетевые интерфейсы, появится предупреждение об их автоматическом отключении. В окне предупреждения нажмите кнопку **OK**.

На странице будет отображен список доступных беспроводных сетей:

- Если ранее были сохранены параметры подключения для какой-либо доступной сети, будет выполнено автоматическое подключение к этой сети. Сеть, к которой подключен ваш компьютер, будет обозначена значком ✓.
- Защищенные сети обозначены значком 🔒.
- Сети, в которых используется неподдерживаемый тип аутентификации, обозначены значком ⚠. Вы можете подключиться к сетям, которые открыты или используют типы аутентификации WPA-PSK и WPA2-PSK.

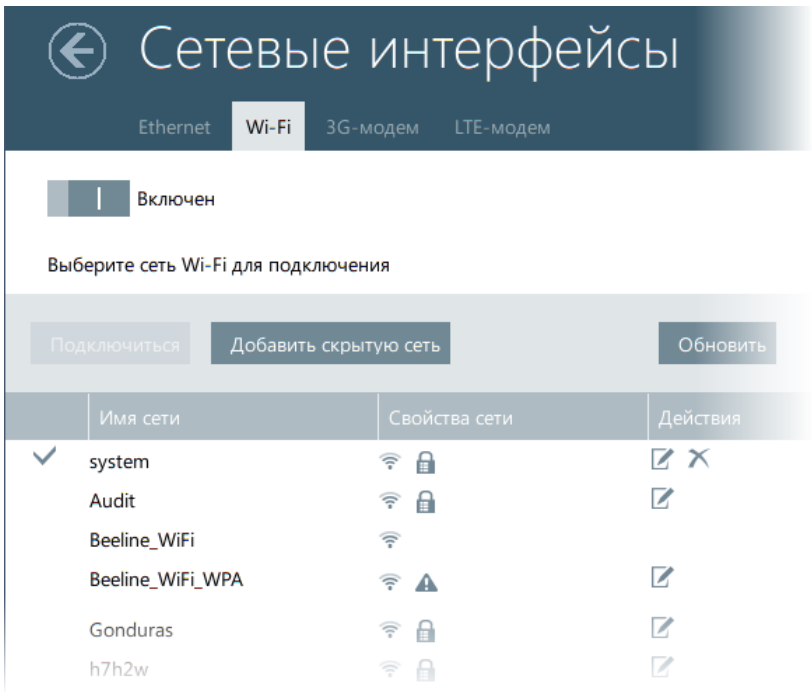

Рисунок 13. Настройка подключения к сети Wi-Fi

4 Чтобы подключиться к какой-либо сети:

- Выберите сеть в списке и нажмите кнопку **Подключиться**.
- В окне **Подключение к <имя сети>** при необходимости выберите тип шифрования и введите пароль.
- Нажмите кнопку **Подключиться**.

Если заданные параметры верны, ваш компьютер будет подключен к выбранной сети, параметры подключения будут сохранены.

5 Чтобы изменить параметры подключения к сети:

- В строке с именем сети, параметры которой требуется изменить, щелкните значок ✎.
- В окне **Изменение настроек <имя сети>** выполните необходимые изменения.

- Нажмите кнопку **Сохранить**.

6 Чтобы удалить сохраненные параметры подключения к сети, в строке с именем сети щелкните значок ✕.

Параметры подключения к выбранной сети будут удалены. Если вы были подключены к этой сети, соединение будет прервано.

Если требуется подключиться к скрытой сети Wi-Fi, и вам известны имя и пароль доступа к сети, выполните следующие действия:

1 На вкладке **Wi-Fi сеть** нажмите кнопку **Добавить скрытую сеть**.

2 В окне **Подключение к скрытой сети** укажите имя сети, тип шифрования и при необходимости пароль.

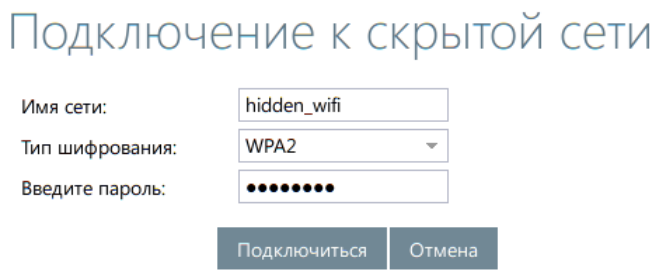

Рисунок 14. Подключение к скрытой сети

3 Нажмите кнопку **Подключиться**.

Настройка подключения к сети 3G

Если у вас имеется 3G-модем, вы можете подключиться к Интернету через мобильную сеть 3G (см. Глоссарий, стр. 87). По умолчанию в список операторов сети 3G включены следующие операторы: Билайн, Мегафон, МТС, Скай Линк, Verizon, Vodafone, Deutsche Telekom. Если вы пользуетесь услугами других операторов, администратор сети ViPNet может дополнить список операторов в программе ViPNet Центр управления сетью. Подробнее о задании списка операторов сети 3G см. документ «ViPNet Terminal. Общее описание».

Чтобы настроить подключение к сети 3G, выполните следующие действия:

1 Подключите к компьютеру 3G-модем.

Примечание. Перед использованием 3G-модема может потребоваться его активация. Также убедитесь, что на вашем счете достаточно средств для подключения к Интернету. Подробную информацию об использовании 3G-модема можно получить у оператора мобильной связи.

2 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Сетевые интерфейсы**.

3 На странице **Сетевые интерфейсы** откройте вкладку **3G-модем**.

4 На вкладке **3G-модем** в списке **Оператор** выберите оператора мобильной связи, услугами которого вы пользуетесь.

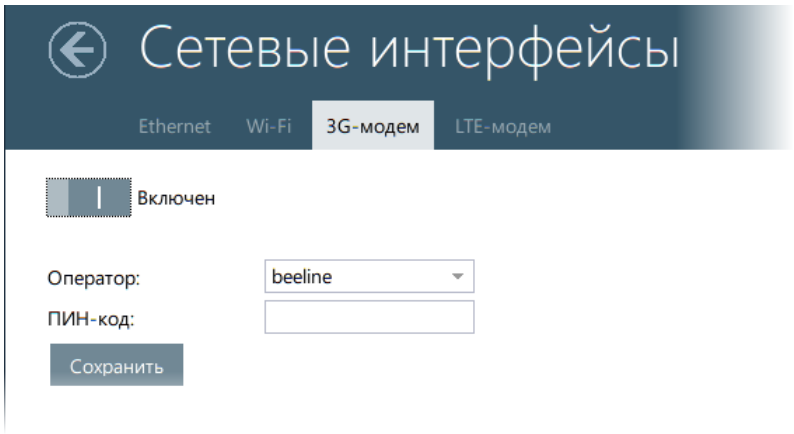

Рисунок 15. Настройка подключения к мобильной сети 3G

5 При необходимости в соответствующее поле введите ПИН-код SIM-карты.

6 Чтобы сохранить параметры подключения, нажмите кнопку **Сохранить**.

7 Чтобы включить 3G-модем, переведите переключатель в положение .

Примечание. Если в момент включения 3G-модема включены какие-либо другие сетевые интерфейсы, появится предупреждение об их автоматическом отключении. В окне предупреждения нажмите кнопку **OK**.

Подключение к сети LTE

Если у вас имеется LTE-модем, вы можете подключиться к Интернету через сеть LTE (см. Глоссарий, стр. 88). Для этого выполните следующие действия:

1 Подключите к компьютеру LTE-модем.

Примечание. Перед использованием LTE-модема может потребоваться его активация. Также убедитесь, что на вашем счете достаточно средств для подключения к Интернету. Подробную информацию об использовании LTE-модема можно получить у оператора мобильной связи.

2 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Сетевые интерфейсы**.

3 На странице **Сетевые интерфейсы** откройте вкладку **LTE-модем**.

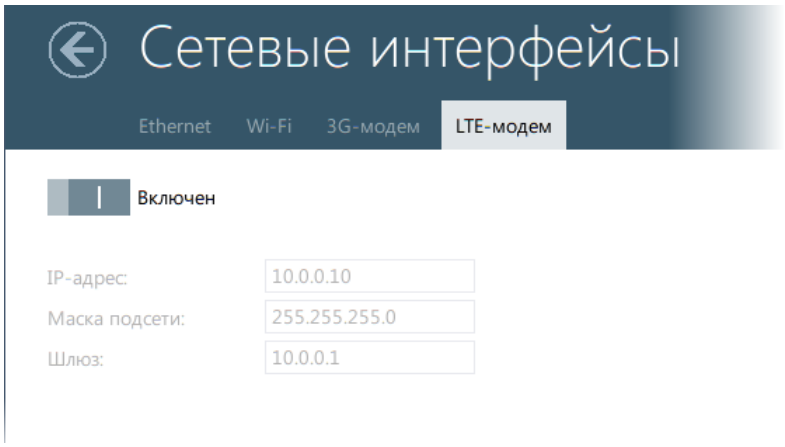

Рисунок 16. Подключение к сети LTE

4 Чтобы включить LTE-модем, переведите переключатель в положение . Параметры подключения к сети будут определены автоматически.

Примечание. Если в момент включения LTE-модема включены какие-либо другие сетевые интерфейсы, появится предупреждение об их автоматическом отключении. В окне предупреждения нажмите кнопку **OK**.

Изменение таблицы маршрутизации

Таблица маршрутизации (см. Глоссарий, стр. 90) задает соответствие между адресами назначения и шлюзами, через которые следует отправлять IP-пакеты на эти адреса. Если требуется добавить маршрут для соединения с узлами какой-либо локальной сети, вы можете изменить таблицу маршрутизации. Для этого выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Прикладные сервисы**.

2 На странице **Прикладные сервисы** откройте вкладку **Таблица маршрутизации**, будет отображен список заданных маршрутов.

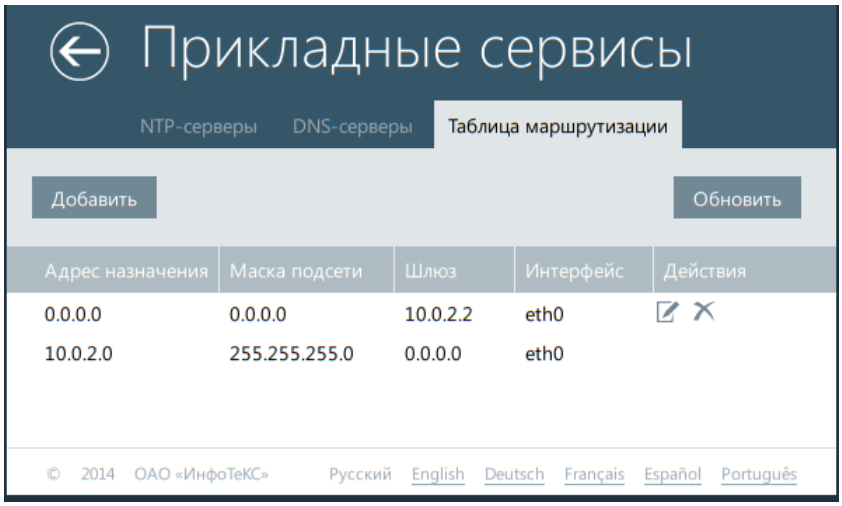

Рисунок 17. Настройка таблицы маршрутизации

3 Выполните одно из действий:

- Чтобы добавить новый маршрут, нажмите кнопку **Добавить** и задайте IP-адрес назначения маршрута, шлюз для доступа к IP-адресу назначения, а также маску подсети (сетевой интерфейс будет определен автоматически). Затем нажмите клавишу **Enter**.
- Чтобы отредактировать маршрут, дважды щелкните строку с ним и внесите необходимые изменения. Затем нажмите клавишу **Enter**.
- Чтобы удалить маршрут, в строке рядом с ним щелкните значок ✕. В окне сообщения нажмите клавишу **Enter**.

Примечание. Вы не можете удалить маршрут по умолчанию.

---

4 Чтобы обновить список маршрутов, нажмите кнопку **Обновить**. В результате обновления все неверно заданные маршруты автоматически будут удалены из списка.

Примечание. Маршруты для сети, к которой в данный момент нет активных подключений, будут неактивны. Неактивные маршруты обозначаются серым цветом и отображаются после всех активных маршрутов. Неактивные маршруты автоматически будут применены при подключении к сети, для которой они заданы.

Изменение списка DNS-серверов

DNS-серверы (см. Глоссарий, стр. 87) используются для разрешения символьных имен компьютеров в IP-адреса и наоборот. При автоматической настройке подключения к сети Ethernet адреса DNS-серверов могут быть получены от DHCP-сервера. При необходимости вы можете вручную указать адреса DNS-серверов, используемых в сети.

Чтобы изменить список используемых DNS-серверов, выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Прикладные сервисы**.

2 На странице **Прикладные сервисы** откройте вкладку **DNS-серверы**, будет отображен список заданных DNS-серверов.

   Адреса DNS-серверов, полученные от DHCP-сервера, имеют тип **Получен автоматически**. Такие адреса невозможно удалить или изменить. Адреса DNS-серверов, добавленные вручную, имеют тип **Добавлен вручную**.

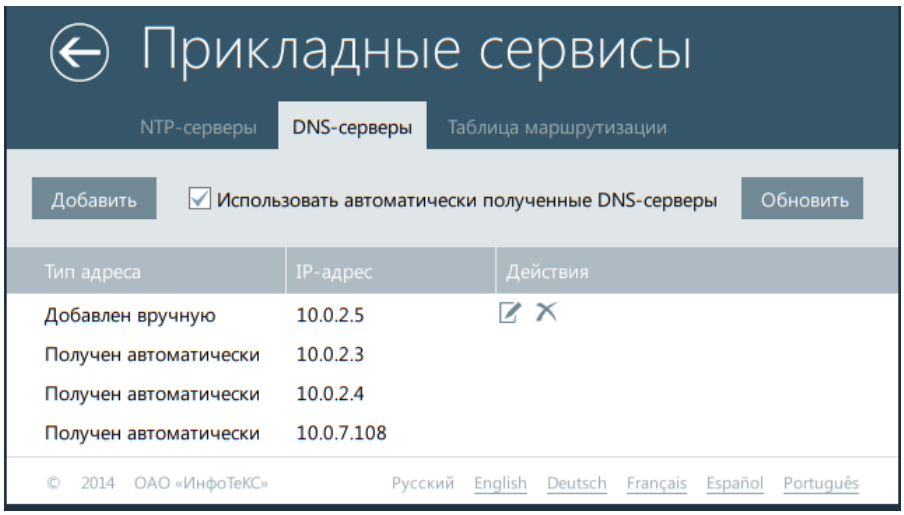

   Рисунок 18. Изменение списка DNS-серверов

3 Чтобы отказаться от использования DNS-серверов, полученных от DHCP-сервера, снимите флажок **Использовать автоматически полученные DNS-серверы** (по умолчанию установлен).

4 Выполните одно из действий:

   - Чтобы добавить IP-адрес DNS-сервера в список, нажмите кнопку **Добавить** и задайте IP-адрес DNS-сервера. Затем нажмите клавишу **Enter**.
   - Чтобы отредактировать IP-адрес DNS-сервера, дважды щелкните строку с ним и внесите необходимые изменения. Затем нажмите клавишу **Enter**.
   - Чтобы удалить IP-адрес DNS-сервера из списка, в строке рядом с ним щелкните значок ✕. В окне сообщения нажмите кнопку **OK**.

5 Чтобы обновить список DNS-серверов, нажмите соответствующую кнопку.

Изменение списка NTP-серверов

NTP-серверы (см. Глоссарий, стр. 88) используются для синхронизации системного времени с мировым. При автоматической настройке подключения к сети Ethernet адреса NTP-серверов могут быть получены от DHCP-сервера. Также вы можете задать собственный список NTP-серверов.

Чтобы изменить список используемых NTP-серверов, выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Прикладные сервисы**.

2 На странице **Прикладные сервисы** откройте вкладку **NTP-серверы**, будет отображен список заданных NTP-серверов.

В списке всегда присутствует сервер `pool.ntp.org`, используемый по умолчанию. Этот сервер невозможно удалить или изменить. Адреса NTP-серверов, полученные от DHCP-сервера, имеют тип **Получен автоматически**. Такие адреса невозможно удалить или изменить. Адреса NTP-серверов, добавленные вручную, имеют тип **Добавлен вручную**.

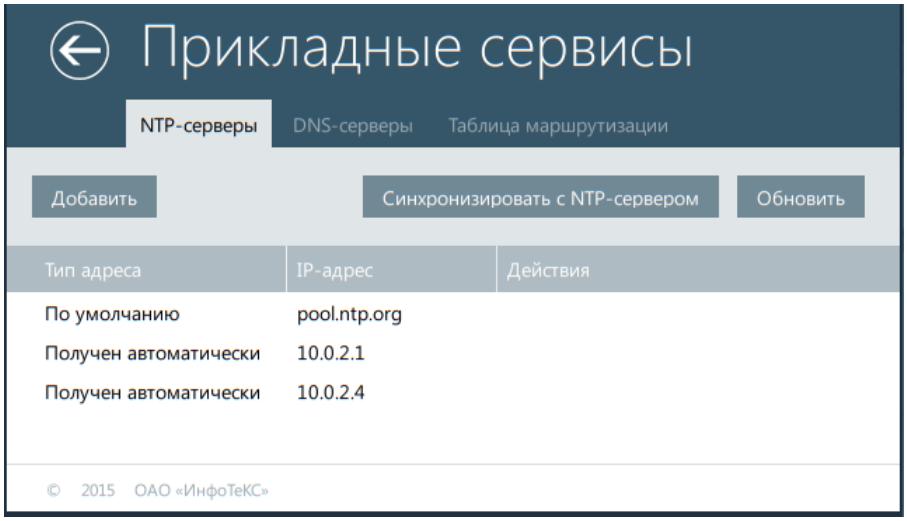

Рисунок 19. Изменение списка NTP-серверов

3 Выполните одно из действий:

- Чтобы добавить IP-адрес NTP-сервера в список, нажмите кнопку **Добавить** и задайте IP-адрес или DNS-имя NTP-сервера. Затем нажмите клавишу **Enter**.
- Чтобы отредактировать IP-адрес NTP-сервера, дважды щелкните строку с ним и внесите необходимые изменения. Затем нажмите клавишу **Enter**.
- Чтобы удалить IP-адрес NTP-сервера из списка, в строке рядом с ним щелкните значок ✕. В окне сообщения нажмите кнопку **OK**.

4 Чтобы обновить список NTP-серверов, нажмите соответствующую кнопку.

5 Чтобы синхронизировать системное время, нажмите кнопку **Синхронизировать с NTP-сервером**.

Изменение списка доступных терминальных серверов

С помощью ViPNet Terminal вы можете подключиться к удаленному рабочему столу или приложениям на терминальном сервере, к веб-ресурсам, а также к виртуальным рабочим столам, реализованным по технологии VMware Horizon/View или IBS Parallels VDI. Список терминальных серверов (см. Глоссарий, стр. 90), необходимых для работы, может быть задан с помощью веб-интерфейса ViPNet Terminal.

Примечание. Список терминальных серверов также может быть задан администратором сети ViPNet в программе ViPNet Центр управления сетью. Подробнее см. документ «ViPNet Terminal. Общее описание».

Чтобы изменить список терминальных серверов, выполните следующие действия:

1 В многооконном режиме работы нажмите кнопку и в меню выберите пункт **Настройка**, откроется начальная страница настройки ViPNet Terminal (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29).

2 На начальной странице щелкните плитку **Терминальные серверы**. На странице **Терминальные серверы** будет отображен текущий список серверов.

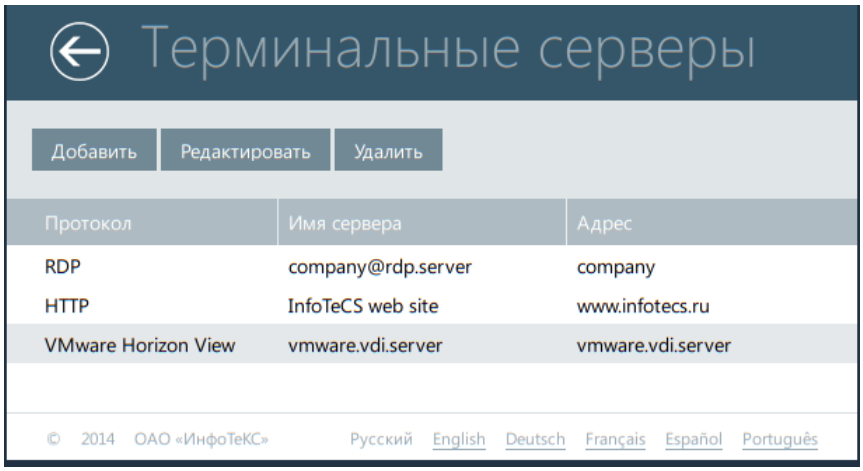

Рисунок 20. Список терминальных серверов

3 Чтобы добавить терминальный сервер, нажмите кнопку **Добавить** и следуйте указаниям раздела Добавление терминального сервера (на стр. 48).

4 Чтобы изменить параметры терминального сервера, выберите этот сервер в списке и нажмите кнопку **Редактировать**. Затем выполните необходимые изменения так же, как при добавлении нового сервера.

5 Чтобы удалить терминальный сервер из списка, выберите этот сервер в списке и нажмите соответствующую кнопку. В окне подтверждения нажмите кнопку **OK**, терминальный сервер будет удален.

Добавление терминального сервера

Чтобы добавить новый терминальный сервер, выполните следующие действия:

1 На странице **Терминальные серверы** нажмите кнопку **Добавить**. Откроется страница **Добавление терминального сервера**.

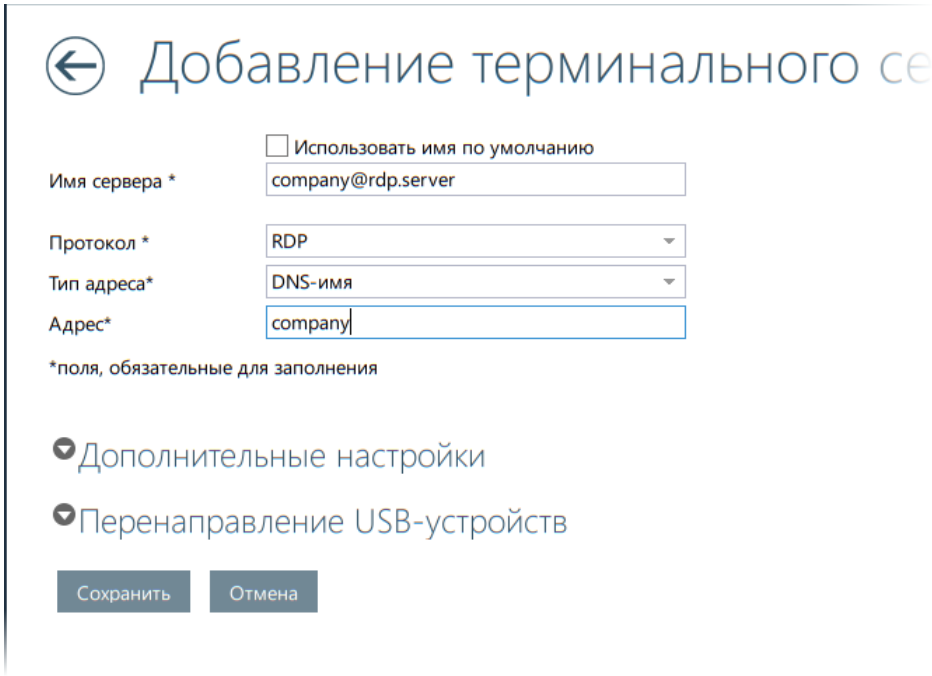

Рисунок 21. Добавление терминального сервера

2 Если вы хотите задать имя терминального сервера самостоятельно:

- Снимите флажок **Использовать имя по умолчанию**.
- Введите имя сервера в соответствующее поле.

Примечание. При вводе имени сервера вы можете использовать латиницу, кириллицу, цифры и специальные символы. Для переключения раскладки клавиатуры используйте сочетание клавиш **Alt+Shift** или значок раскладки на панели задач (см. «Многооконный режим работы» на стр. 25).

По умолчанию используется имя, которое совпадает с адресом сервера (IP-адрес, DNS-имя либо имя сетевого узла ViPNet в зависимости от того, как будет задан адрес доступа к серверу).

3 Укажите протокол для подключения к терминальному серверу:

- Для доступа к удаленному рабочему столу на сервере Windows Server в списке **Протокол** выберите пункт **RDP**.
- Для доступа к удаленному рабочему столу или приложениям на сервере Citrix в списке **Протокол** выберите пункт **ICA**. Если на терминальном сервере установлено ПО Citrix XenDesktop 7.0 или более поздней версии, используйте для подключения «режим киоска». Для этого установите соответствующий флажок напротив списка **Протокол**.

> **Примечание.** При подключении к серверу в «режиме киоска» терминальная сессия открывается в полноэкранном режиме. Чтобы завершить такую сессию, перезагрузите ViPNet Terminal либо перезапустите графическую сессию.

- Для доступа к веб-сайтам или веб-приложениям в списке **Протокол** выберите пункт **HTTP** или **HTTPS**.
- Для доступа к виртуальным рабочим столам VMware в списке **Протокол** выберите пункт **VMware Horizon View**.
- Для доступа к виртуальным рабочим столам IBS в списке **Протокол** выберите пункт **IBS Parallels VDI**.

> **Внимание!** Возможность организации доступа к виртуальным рабочим столам IBS недоступна в минимальном варианте ПО ViPNet Terminal.

4 Укажите адрес доступа к терминальному серверу. Для этого выполните одно из действий:

- Для доступа к терминальному серверу, который расположен на защищенном узле ViPNet, в списке **Тип адреса** выберите **ViPNet ID** и в списке **Адрес** выберите нужный сетевой узел ViPNet.
- Для доступа к серверу по IP-адресу в списке **Тип адреса** выберите **IP-адрес** и в поле **Адрес** введите IP-адрес терминального сервера.
- Для доступа к серверу по DNS-имени в списке **Тип адреса** выберите **DNS-имя** и в поле **Адрес** введите DNS-имя терминального сервера.

5 Если требуется указать дополнительные параметры подключения к терминальному серверу, раскройте группу **Дополнительные настройки** и следуйте указаниям раздела Настройка дополнительных параметров подключения к терминальному серверу (на стр. 62). К дополнительным параметрам относятся как параметры, не зависящие от протокола подключения к серверу (например размер окна), так и параметры, специфичные для выбранного протокола подключения (например имя приложения на сервере Citrix).

6 Если требуется перенаправлять на терминальный сервер USB-устройства, раскройте группу **Перенаправление USB-устройств** и следуйте указаниям раздела Настройка перенаправления USB-устройств (на стр. 62). Настройка перенаправления USB-устройств возможна, только если такое перенаправление разрешено администратором ViPNet Terminal.

7 Задав необходимые параметры, нажмите кнопку **Сохранить**. Новый сервер появится в списке в разделе **Терминальные серверы** (см. «Изменение списка доступных терминальных серверов» на стр. 47), а также будет добавлен в меню, которое вызывается кнопкой .

Настройка дополнительных параметров подключения к терминальному серверу

Дополнительные параметры настройки зависят от типа терминального сервера. Следуйте указаниям для типа терминального сервера, подключение к которому вы настраиваете:

- Дополнительные параметры подключения к терминальному серверу Windows Server (на стр. 50).
- Дополнительные параметры подключения к терминальному серверу Citrix в обычном режиме (на стр. 52).
- Дополнительные параметры подключения к терминальному серверу Citrix в «режиме киоска» (на стр. 54).
- Дополнительные параметры подключения к терминальному серверу по протоколу HTTP или HTTPS (на стр. 55).
- Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами VMware (на стр. 57).
- Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами IBS (на стр. 60).

Дополнительные параметры подключения к терминальному серверу Windows Server

Чтобы настроить дополнительные параметры терминального сервера Windows Server 2003/2008/2008 R2/2012/2012 R2, выполните следующие действия:

1 На странице **Добавление терминального сервера** (см. Рисунок 22 на стр. 48) раскройте группу **Дополнительные настройки**.

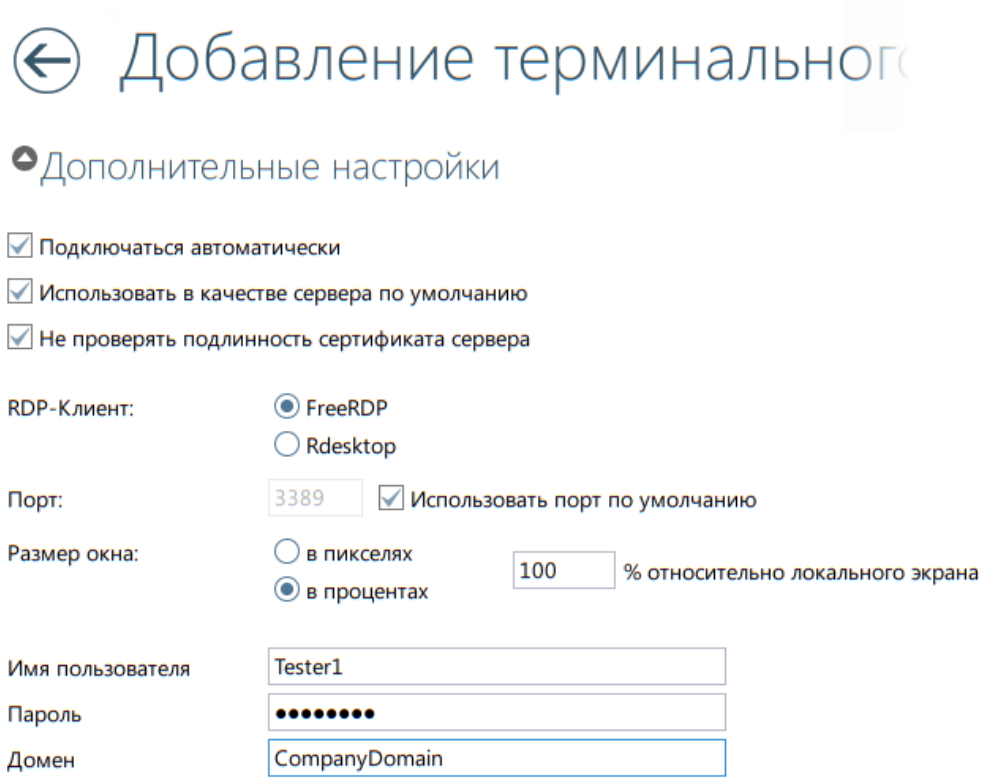

Рисунок 22. Дополнительные параметры при подключении по протоколу RDP

2 Если вы хотите, чтобы при запуске ViPNet Terminal происходило автоматическое подключение к серверу, установите флажок **Подключаться автоматически**.

3 Если вы хотите, чтобы редактируемый терминальный сервер использовался по умолчанию в полноэкранном режиме работы (см. «Полноэкранный режим работы» на стр. 27), установите флажок **Использовать в качестве сервера по умолчанию**.

Примечание. В качестве сервера по умолчанию может быть выбран только один терминальный сервер. Если сервер по умолчанию был задан ранее, вместо прежнего сервера по умолчанию будет использоваться новый.

---

4 Выберите программное обеспечение, которое будет использоваться для подключения к серверу. Для этого с помощью переключателя **RDP-клиент** выберите одно из значений:

- **Rdesktop** — RDP-клиент, отличающийся высокой стабильностью работы.
- **FreeRDP** — RDP-клиент с более богатыми функциональными возможностями по сравнению с Rdesktop.

5 При подключении к терминальному серверу проверяется подлинность SSL-сертификата. По умолчанию в случае, если проверить подлинность SSL-сертификата не удается, подключение к серверу не происходит. Если вы хотите разрешить подключение к серверу в любом случае, даже если не удалось проверить подлинность SSL-сертификата, установите флажок **Не проверять подлинность сертификата сервера**.

6 При необходимости измените порт доступа к терминальному серверу. Для этого снимите флажок **Использовать порт по умолчанию** и в поле **Порт** задайте нужный номер порта.

7 При необходимости укажите размер окна, в котором при подключении к серверу будет открываться терминальная сессия или веб-браузер. Для этого в группе **Размер окна** выполните одно из действий:

- Чтобы указать абсолютный размер окна, с помощью переключателя выберите пункт **в пикселях** и в соответствующих полях задайте ширину и высоту окна в пикселях.
- Чтобы указать размер окна в процентах относительно ширины и высоты экрана вашего компьютера, с помощью переключателя выберите пункт **в процентах** и в поле справа задайте число процентов.

Примечание. Чтобы изображение в окне не искажалось, мы рекомендуем задавать значения ширины и высоты окна, кратные четырем.

---

8 При необходимости для авторизации на терминальном сервере в соответствующих полях укажите:

- Имя пользователя.
- Пароль.
- Домен.

Дополнительные параметры подключения к терминальному серверу Citrix в обычном режиме

Чтобы настроить дополнительные параметры терминального сервера Citrix при подключении в обычном режиме, выполните следующие действия:

1 На странице **Добавление терминального сервера** (см. Рисунок 22 на стр. 48) раскройте группу **Дополнительные настройки**.

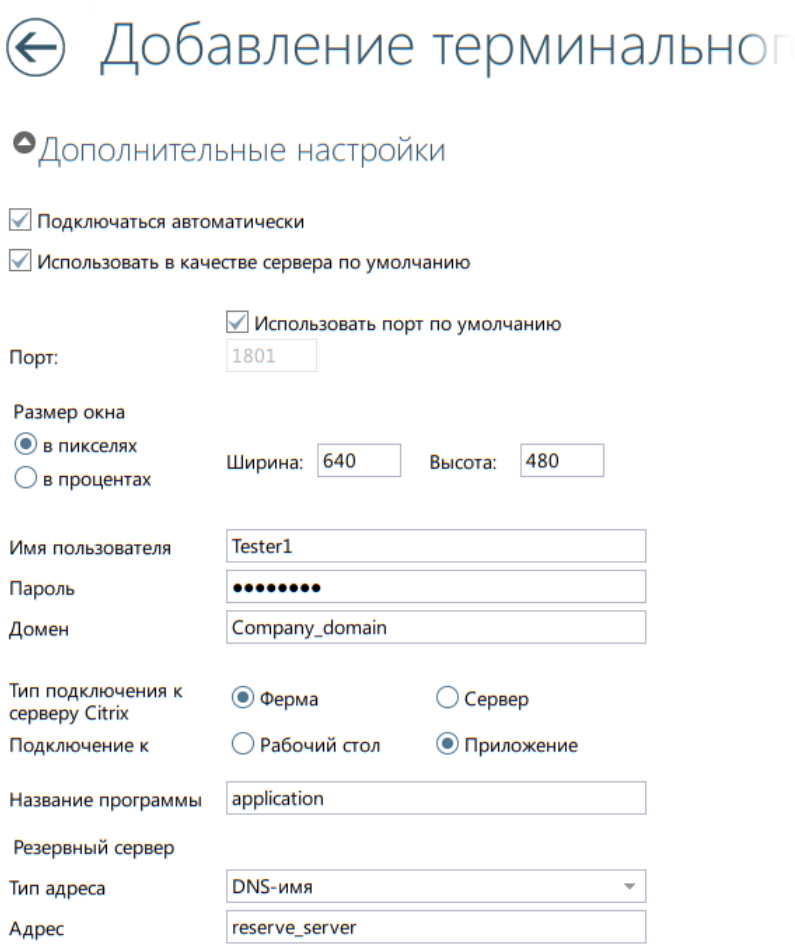

Рисунок 23. Дополнительные параметры при подключении по протоколу ICA в обычном режиме

2 Если вы хотите, чтобы при запуске ViPNet Terminal происходило автоматическое подключение к серверу, установите флажок **Подключаться автоматически**.

3 Если вы хотите, чтобы редактируемый терминальный сервер использовался по умолчанию в полноэкранном режиме работы (см. «Полноэкранный режим работы» на стр. 27), установите флажок **Использовать в качестве сервера по умолчанию**.

Примечание. В качестве сервера по умолчанию может быть выбран только один терминальный сервер. Если сервер по умолчанию был задан ранее, вместо прежнего сервера по умолчанию будет использоваться новый.

---

4 При необходимости измените порт доступа к терминальному серверу. Для этого снимите флажок **Использовать порт по умолчанию** и в поле **Порт** задайте нужный номер порта.

5 При необходимости укажите размер окна, в котором при подключении к серверу будет открываться терминальная сессия или веб-браузер. Для этого в группе **Размер окна** выполните одно из действий:

- Чтобы указать абсолютный размер окна, с помощью переключателя выберите пункт **в пикселях** и в соответствующих полях задайте ширину и высоту окна в пикселях.

- Чтобы указать размер окна в процентах относительно ширины и высоты экрана вашего компьютера, с помощью переключателя выберите пункт **в процентах** и в поле справа задайте число процентов.

Примечание. Чтобы изображение в окне не искажалось, мы рекомендуем задавать значения ширины и высоты окна, кратные четырем.

---

6 При необходимости для авторизации на терминальном сервере в соответствующих полях укажите:

- Имя пользователя.
- Пароль.
- Домен.

7 С помощью переключателя **Тип подключения к серверу Citrix** выберите одно из значений: **Ферма** — для подключения к ферме серверов Citrix или **Сервер** — для подключения к отдельному серверу.

8 С помощью переключателя **Подключение к** выберите одно из значений: **Рабочий стол** — для подключения к удаленному рабочему столу или **Приложение** — для запуска опубликованного на сервере приложения.

9 Если вы выбрали запуск приложения, в поле **Название программы** укажите имя опубликованного на сервере приложения.

10 Если вы выбрали подключение к ферме серверов и одновременно запуск приложения, при необходимости в группе **Резервный сервер** в соответствующих полях укажите тип адреса и адрес резервного сервера.

Дополнительные параметры подключения к терминальному серверу Citrix в «режиме киоска»

Чтобы настроить дополнительные параметры терминального сервера Citrix при подключении в «режиме киоска», выполните следующие действия:

1 На странице **Добавление терминального сервера** (см. Рисунок 22 на стр. 48) раскройте группу **Дополнительные настройки**.

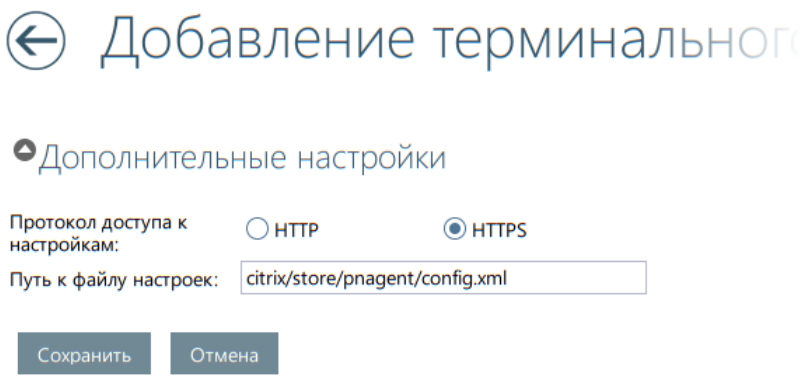

Рисунок 24. Дополнительные параметры при подключении по протоколу ICA в «режиме киоска»

2 При необходимости измените путь к конфигурационному файлу на терминальном сервере Citrix в соответствующем поле.

3 При необходимости измените протокол доступа к конфигурационному файлу. Для этого установите соответствующий переключатель.

Дополнительные параметры подключения к терминальному серверу по протоколу HTTP или HTTPS

Чтобы настроить дополнительные параметры терминального сервера с подключением по протоколу HTTP или HTTPS, выполните следующие действия:

1 На странице **Добавление терминального сервера** (см. Рисунок 22 на стр. 48) раскройте группу **Дополнительные настройки**.

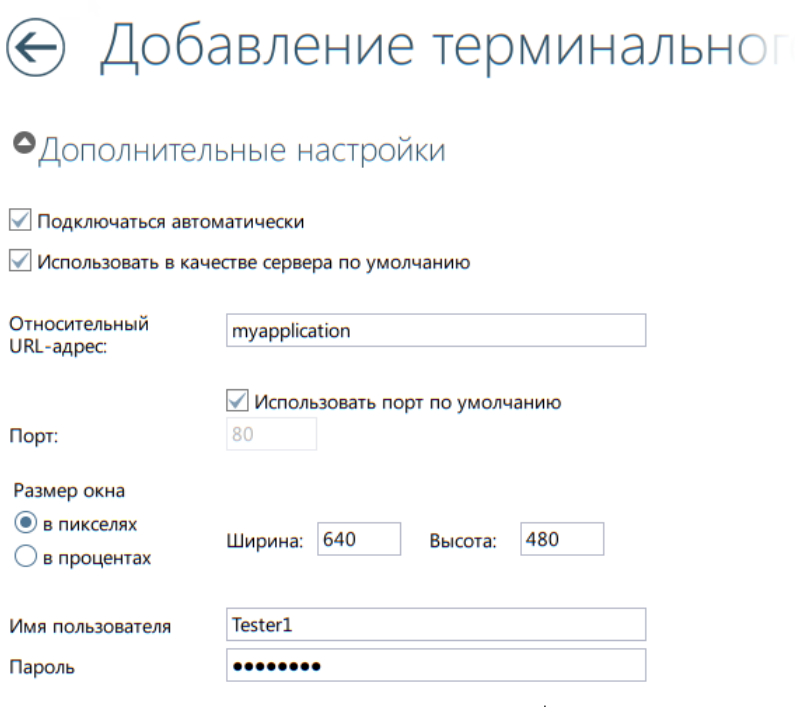

Рисунок 25. Дополнительные параметры при подключении по протоколам HTTP или HTTPS

2 Если вы хотите, чтобы при запуске ViPNet Terminal происходило автоматическое подключение к серверу, установите флажок **Подключаться автоматически**.

3 Если вы хотите, чтобы редактируемый терминальный сервер использовался по умолчанию в полноэкранном режиме работы (см. «Полноэкранный режим работы» на стр. 27), установите флажок **Использовать в качестве сервера по умолчанию**.

Примечание. В качестве сервера по умолчанию может быть выбран только один терминальный сервер. Если сервер по умолчанию был задан ранее, вместо прежнего сервера по умолчанию будет использоваться новый.

---

4 При необходимости в поле **Относительный URL** введите относительный URL-адрес страницы или веб-приложения на сервере.

Например, если для сервера с адресом `myserver.com` задан относительный URL-адрес `myapplication`, подключение к серверу будет выполняться по адресу `http://myserver.com/myapplication`.

5 При необходимости измените порт доступа к терминальному серверу. Для этого снимите флажок **Использовать порт по умолчанию** и в поле **Порт** задайте нужный номер порта.

6 При необходимости укажите размер окна, в котором при подключении к серверу будет открываться терминальная сессия или веб-браузер. Для этого в группе **Размер окна** выполните одно из действий:

- Чтобы указать абсолютный размер окна, с помощью переключателя выберите пункт **в пикселях** и в соответствующих полях задайте ширину и высоту окна в пикселях.

- Чтобы указать размер окна в процентах относительно ширины и высоты экрана вашего компьютера, с помощью переключателя выберите пункт **в процентах** и в поле справа задайте число процентов.

Примечание. Чтобы изображение в окне не искажалось, мы рекомендуем задавать значения ширины и высоты окна, кратные четырем.

---

7 При необходимости для авторизации на терминальном сервере в соответствующих полях укажите:

- Имя пользователя.
- Пароль.

Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами VMware

Чтобы настроить дополнительные параметры терминального сервера с рабочими столами VMware, выполните следующие действия:

1 На странице **Добавление терминального сервера** (см. Рисунок 22 на стр. 48) раскройте группу **Дополнительные настройки**.

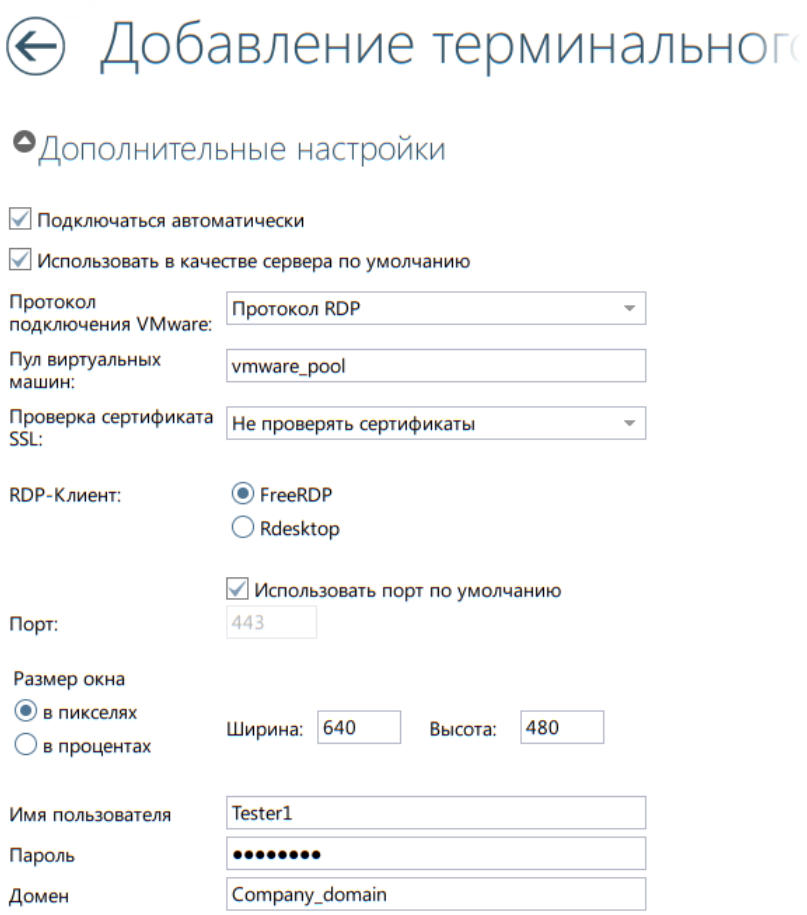

Рисунок 26. Дополнительные параметры при подключении по протоколу VMware Horizon View

2 Если вы хотите, чтобы при запуске ViPNet Terminal происходило автоматическое подключение к серверу, установите флажок **Подключаться автоматически**.

3 Если вы хотите, чтобы редактируемый терминальный сервер использовался по умолчанию в полноэкранном режиме работы (см. «Полноэкранный режим работы» на стр. 27), установите флажок **Использовать в качестве сервера по умолчанию**.

Примечание. В качестве сервера по умолчанию может быть выбран только один терминальный сервер. Если сервер по умолчанию был задан ранее, вместо прежнего сервера по умолчанию будет использоваться новый.

4 При необходимости выберите протокол для подключения к серверу VMware в соответствующем списке. Если не задавать этот параметр, используется протокол, установленный на сервере по умолчанию.

Примечание. Протокол, отличный от протокола по умолчанию, будет использоваться только в том случае, если в программе VMware View Connection Server, установленной на сервере, разрешен выбор протокола.

5 В поле **Пул виртуальных машин** укажите имя пула виртуальных рабочих столов, который будет использоваться по умолчанию при подключении к серверу.

6 В поле **Проверка сертификата SSL** установите режим проверки сертификата SSL при подключении к серверу:

- **Не подключаться, если сертификат ненадежный** — запрашивает подключение к серверу, если не удалось проверить подлинность SSL-сертификата.
- **Предупреждать о ненадежных сертификатах** — запрашивает разрешение на подключение без проверки подлинности, если не удалось проверить подлинность SSL-сертификата.
- **Не проверять сертификаты** — разрешает подключение к серверу в любом случае, даже если не удалось проверить подлинность SSL-сертификата.

По умолчанию используется режим **Предупреждать о ненадежных сертификатах**.

7 Если выбран протокол подключения **RDP**, с помощью переключателя **RDP-клиент** выберите программное обеспечение, которое будет использоваться для подключения к серверу:

- **Rdesktop** — RDP-клиент, отличающийся высокой стабильностью работы.
- **FreeRDP** — RDP-клиент с более богатыми функциональными возможностями по сравнению с Rdesktop.

8 При необходимости измените порт доступа к терминальному серверу. Для этого снимите флажок **Использовать порт по умолчанию** и в поле **Порт** задайте нужный номер порта.

9 При необходимости укажите размер окна, в котором при подключении к серверу будет открываться терминальная сессия или веб-браузер. Для этого в группе **Размер окна** выполните одно из действий:

- Чтобы указать абсолютный размер окна, с помощью переключателя выберите пункт **в пикселях** и в соответствующих полях задайте ширину и высоту окна в пикселях.
- Чтобы указать размер окна в процентах относительно ширины и высоты экрана вашего компьютера, с помощью переключателя выберите пункт **в процентах** и в поле справа задайте число процентов.

Примечание. Чтобы изображение в окне не искажалось, мы рекомендуем задавать значения ширины и высоты окна, кратные четырем.

---

10 При необходимости для авторизации на терминальном сервере в соответствующих полях укажите:

- Имя пользователя.
- Пароль.
- Домен.

Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами IBS

Чтобы настроить дополнительные параметры терминального сервера с рабочими столами IBS, выполните следующие действия:

1 На странице **Добавление терминального сервера** (см. Рисунок 22 на стр. 48) раскройте группу **Дополнительные настройки**.

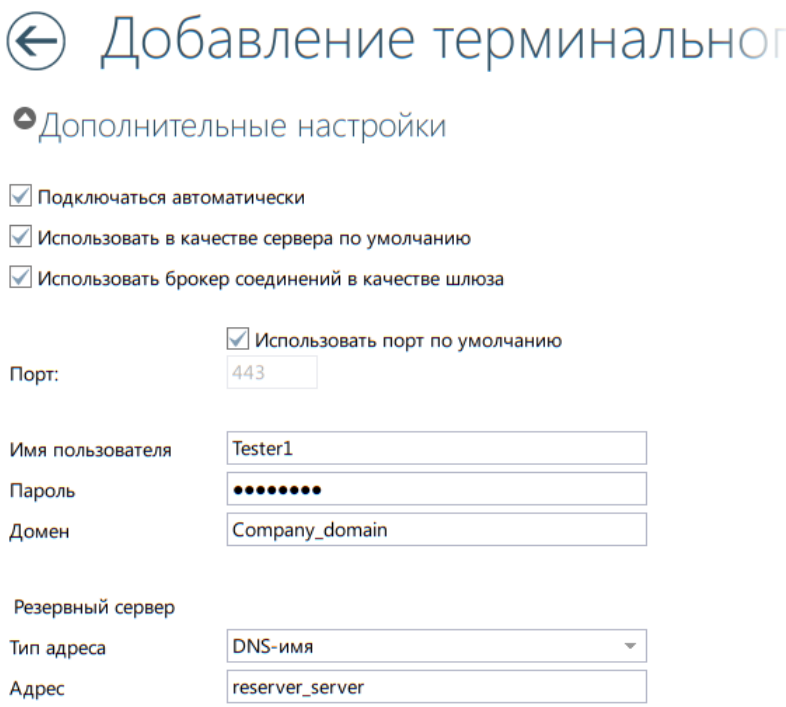

Рисунок 27. Дополнительные параметры при подключении по протоколу IBS VDI

2 Если вы хотите, чтобы при запуске ViPNet Terminal происходило автоматическое подключение к серверу, установите флажок **Подключаться автоматически**.

3 Если вы хотите, чтобы редактируемый терминальный сервер использовался по умолчанию в полноэкранном режиме работы (см. «Полноэкранный режим работы» на стр. 27), установите флажок **Использовать в качестве сервера по умолчанию**.

Примечание. В качестве сервера по умолчанию может быть выбран только один терминальный сервер. Если сервер по умолчанию был задан ранее, вместо прежнего сервера по умолчанию будет использоваться новый.

---

4 При необходимости измените порт доступа к терминальному серверу. Для этого снимите флажок **Использовать порт по умолчанию** и в поле **Порт** задайте нужный номер порта.

5 При необходимости для авторизации на терминальном сервере в соответствующих полях укажите:

- Имя пользователя.

- Пароль.
- Домен.

6 Чтобы получить доступ к виртуальным столам IBS, ViPNet Terminal подключается к специальному серверу — «брокеру соединений», который по умолчанию организует прямое соединение между ViPNet Terminal и терминальным сервером. Если требуется, во время терминальных сессий вы можете использовать брокер соединений в качестве шлюза. Для этого установите соответствующий флажок.

7 Для организации отказоустойчивого соединения вы можете задать резервный брокер соединений. При отказе основного брокера соединение будет выполняться через резервный. Чтобы задать резервный брокер соединений, в группе **Резервный сервер** в соответствующих полях укажите тип адреса и адрес резервного брокера.

Также вы можете задать следующие параметры подключения к терминальному серверу с рабочими столами IBS:

- Включение или выключение механизма перенаправления принтера Microsoft Easy Print вместо механизма, используемого по умолчанию при подключении к терминальному серверу.
- Тип подключения — для достижения максимального быстродействия при взаимодействии с терминальным сервером.

Чтобы задать указанные параметры, выполните следующие действия:

1 На начальной странице настройки (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29) щелкните плитку **Системные настройки**.

2 На странице **Системные настройки** откройте вкладку **Прочее**.

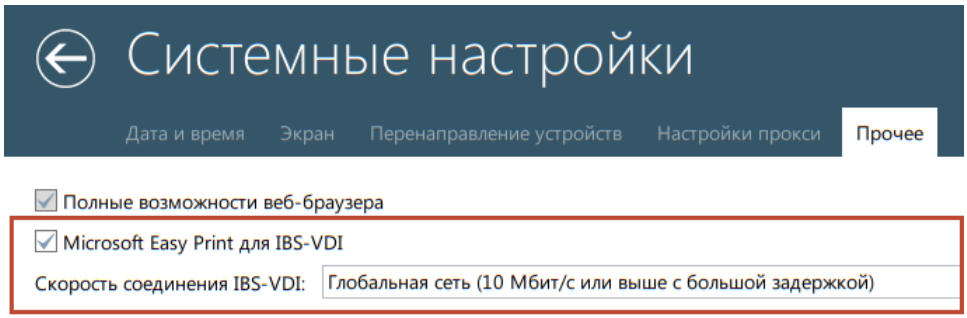

Рисунок 28. Задание параметров подключения по протоколу IBS VDI

3 Установите соответствующий значок и задайте тип вашего соединения с терминальным сервером.

Настройка перенаправления USB-устройств

Если администратор ViPNet Terminal разрешил перенаправление USB-устройств, вы можете задать способ перенаправления и список USB-устройств, разрешенных для перенаправления. Для этого выполните следующие действия:

1 На странице **Добавление терминального сервера** раскройте группу **Перенаправление USB-устройств**.

Примечание. Группа параметров **Перенаправление USB-устройств** присутствует, только если для доступа к терминальному серверу выбран протокол **RDP**, **ICA** или **VMware Horizon View**.

Если перенаправление USB-устройств запрещено, параметры будут недоступны (отображены серым цветом). За разрешением перенаправления обратитесь к администратору ViPNet Terminal.

---

2 В списке **Способ перенаправления** выберите одно из значений: **USB Redirector** или **VMware Horizon View PC-over-IP**.

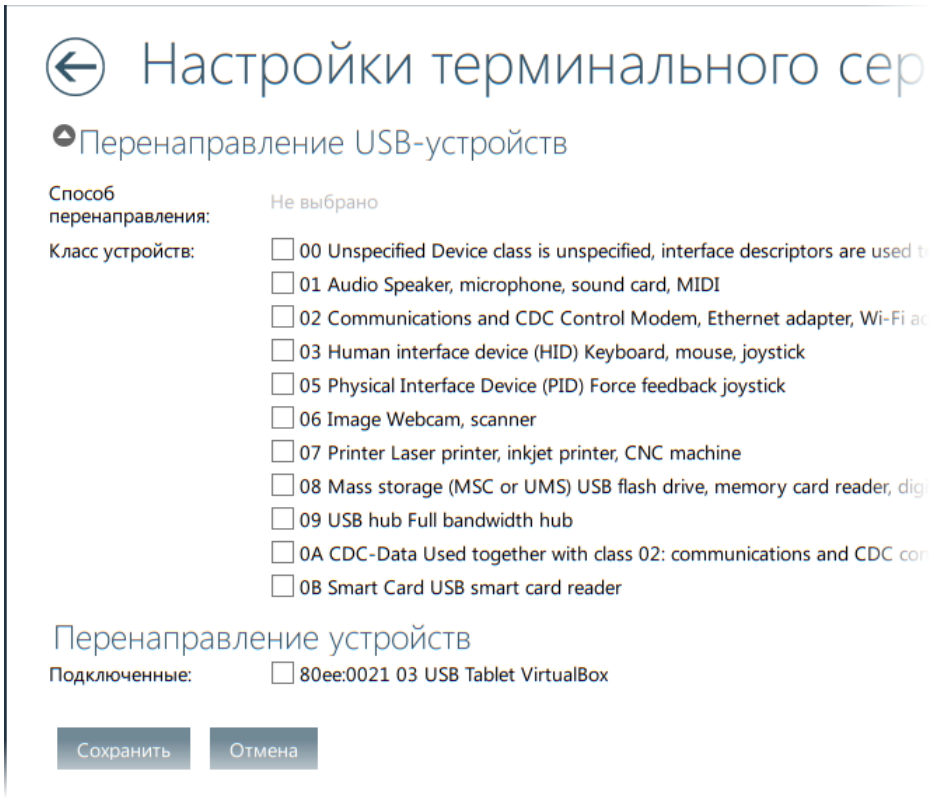

Рисунок 29. Настройка перенаправления USB-устройств на терминальный сервер

Примечание. Если для доступа к терминальному серверу используется протокол RDP или VMware Horizon View, то для перенаправления устройств способом **USB Redirector** на терминальном сервере должна быть установлена программа USB Redirector.

3 Установите флажки напротив тех классов USB-устройств, которые необходимо перенаправлять на данный терминальный сервер. Вы также можете выбрать устройства, подключенные к компьютеру. Список подключенных устройств отображается в группе **Перенаправление устройств**.

Примечание. Если разрешить перенаправление каких-либо устройств, подключенных к компьютеру, то во время работы в терминальной сессии такие устройства могут отсутствовать в списке обнаруженных USB-устройств, и настройка их перенаправления будет невозможна. Поэтому не рекомендуется изменять настройки перенаправления устройств при работе в терминальной сессии.

4 Чтобы сохранить изменения, нажмите кнопку **Сохранить**.

Внимание! Если вы используете ViPNet Terminal в варианте исполнения Live USB (см. «Варианты исполнения ViPNet Terminal» на стр. 14), не включайте перенаправление класса USB-устройств с номером 08. В противном случае при старте терминальной сессии работа ViPNet Terminal будет прекращена.

Работа со списком узлов защищенной сети

С помощью веб-интерфейса ViPNet Terminal вы можете просматривать список защищенных узлов, которые были связаны с данным сетевым узлом в программе ViPNet Центр управления сетью. Для этого выполните следующие действия:

1 На начальной странице веб-интерфейса выберите плитку **ViPNet VPN**.

2 На странице **Защищенная сеть** отобразится список связанных узлов сети ViPNet. Узлы, которые в данный момент отключены от сети либо для которых нет данных об их статусе, выделены серым цветом. Собственный узел ViPNet отображается в списке первым.

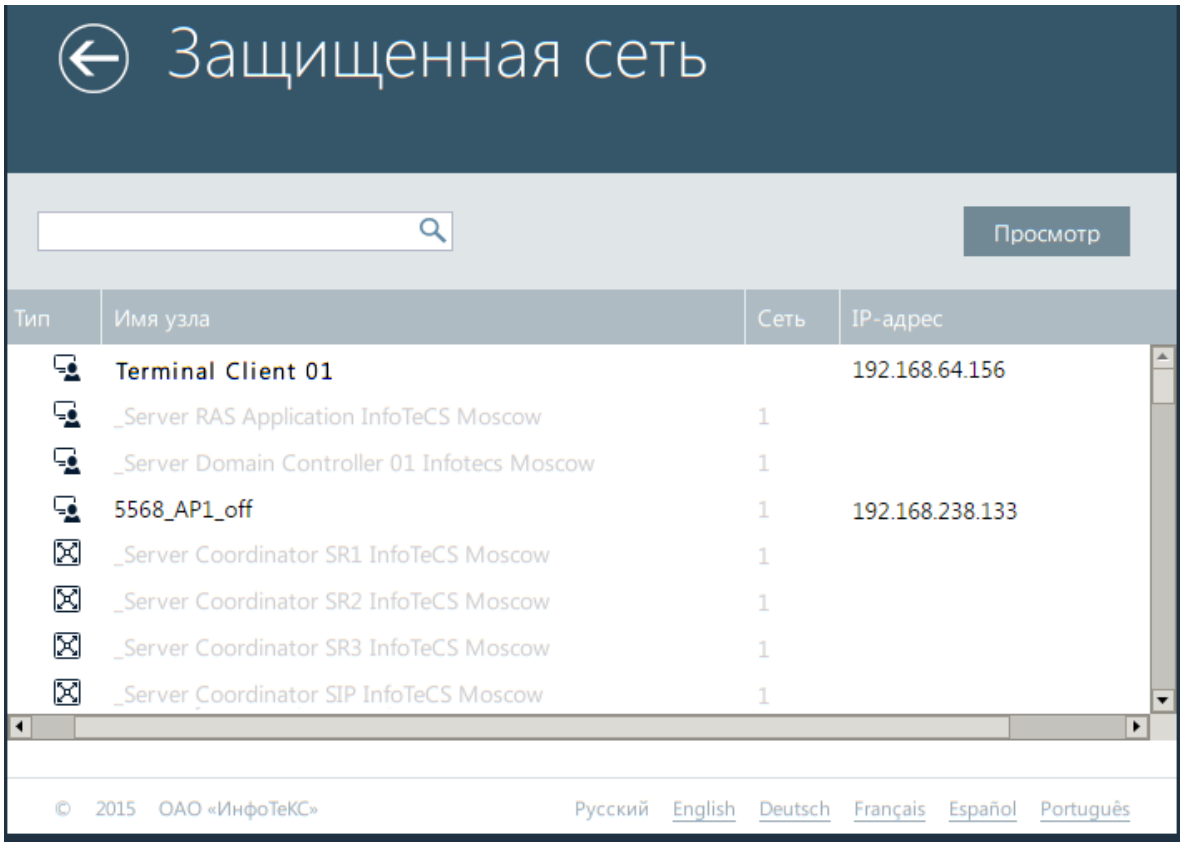

Рисунок 30. Просмотр списка защищенных узлов

3 Чтобы просмотреть информацию об узле, дважды щелкните его в списке. На открывшейся странице вы можете просмотреть следующую информацию:

- Общую информацию об узле (имя, версия ПО ViPNet, реальные и виртуальные IP-адреса узла).
- IP-адреса узла (список всех IP-адресов узла и способ доступа к узлу: по реальным или виртуальным адресам).
- Настройки межсетевого экрана при подключении узла к внешней сети.

- Настройки подключения к туннелируемым узлам.

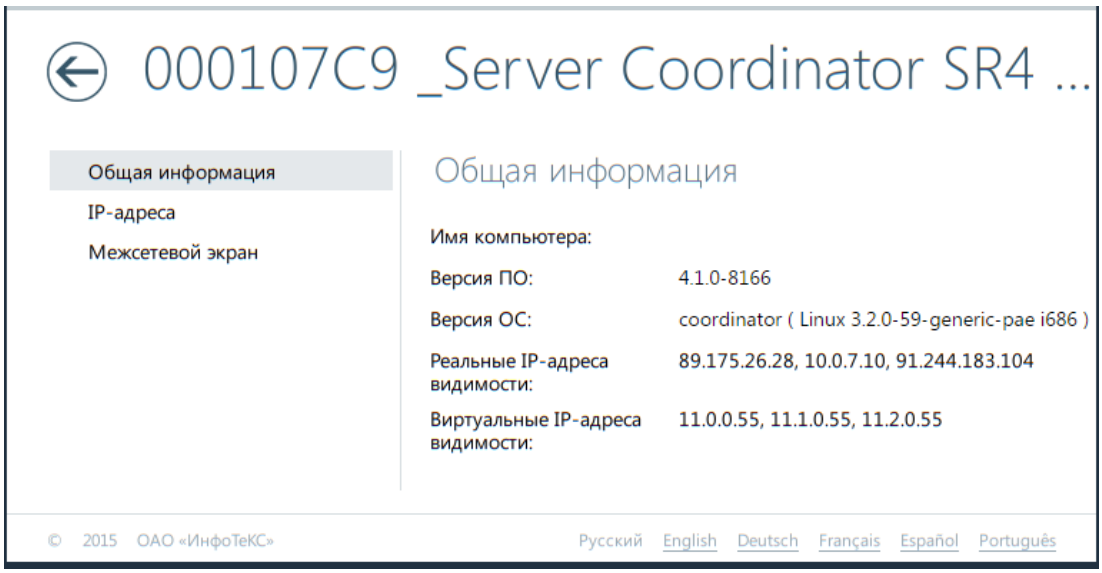

Рисунок 31. Просмотр информации об узле ViPNet

Примечание. Информация о версиях ПО ViPNet и ОС, установленных на узле, появится только после проверки соединения с данным узлом.

Работа с интегрированным сетевым экраном

Общие сведения

Основные принципы фильтрации трафика

Фильтруется весь IP-трафик, который проходит через сетевой узел ViPNet (см. Глоссарий, стр. 90):

- открытый (незашифрованный) трафик;
- защищенный (зашифрованный) трафик.

Рисунок 32. Виды IP-трафика

Наибольшую опасность представляет трафик из открытой сети, поскольку в случае атаки достаточно сложно обнаружить ее источник и принять оперативные меры по ее пресечению.

И открытый, и защищенный трафик может быть локальным или широковещательным. Под локальным трафиком понимается входящий или исходящий трафик конкретного узла (то есть когда сетевой узел является отправителем или получателем IP-пакетов). Под широковещательным трафиком имеется в виду передача узлом IP-пакетов, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть когда пакеты передаются всем узлам определенного сегмента сети).

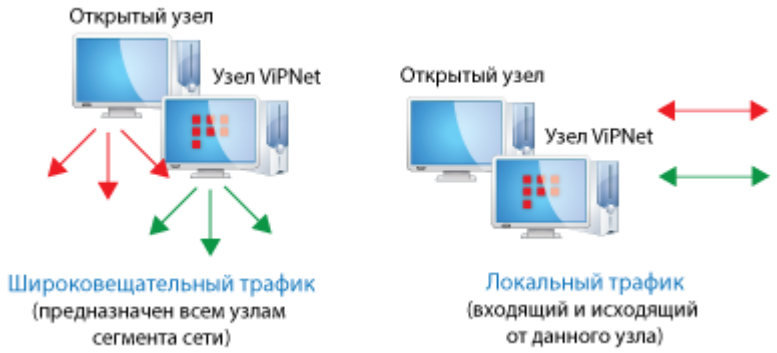

Рисунок 33. Виды защищенного и открытого трафика

Все входящие и исходящие открытые и защищенные IP-пакеты проходят комплексную проверку в соответствии с сетевыми фильтрами. Если IP-пакет соответствует параметрам одного из имеющихся сетевых фильтров, то он пропускается или блокируется в соответствии с этим фильтром. Если пакет не соответствует ни одному из заданных фильтров, то он блокируется.

Схематично последовательность фильтрации IP-пакетов представлена ниже:

Рисунок 34. Фильтрация IP-трафика

Общие сведения о сетевых фильтрах

Существуют сетевые фильтры как для защищенного, так и для открытого трафика. Они выполняют следующие функции:

- Фильтры открытой сети на защищенном узле могут разрешать либо запрещать обмен IP-трафиком с открытыми узлами.

  Примечание. Под открытыми узлами понимаются узлы, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика.

- Фильтры защищенной сети могут ограничивать обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь.

Все сетевые фильтры делятся на следующие категории:

- Фильтры, определенные специальными конфигурациями (см. «Конфигурация сетевого экрана ViPNet Terminal» на стр. 89).

- Фильтры, поступившие в составе политик безопасности из программы ViPNet Policy Manager (см. Глоссарий, стр. 88).
- Предустановленные фильтры и фильтры, заданные администратором узла с помощью веб-интерфейса ViPNet Terminal.
- Фильтры по умолчанию.

Фильтры, определенные специальными конфигурациями сетевого экрана, имеют более высокий приоритет, чем все остальные фильтры, и применяются в первую очередь. Они ограничивают трафик, который запрещен в конфигурациях сетевого экрана ViPNet Terminal.

После фильтров конфигураций следуют фильтры, поступившие из программы ViPNet Policy Manager. Далее размещаются предустановленные фильтры и фильтры, заданные администратором узла с помощью веб-интерфейса ViPNet Terminal. Администраторы могут изменить или удалить их. Самыми последними фильтрами являются фильтры по умолчанию. Данная категория представлена одним сетевым фильтром, блокирующим IP-трафик, который не соответствует ни одному из сетевых фильтров из категорий выше.

Последовательность применения сетевых фильтров в порядке убывания приоритета изображена на схеме ниже.

Рисунок 35: Приоритет применения сетевых фильтров

Сетевые фильтры имеют следующие особенности:

- Фильтры включают в себя следующие параметры:
  - Действие, применяемое к IP-пакетам. Фильтры могут пропускать или блокировать IP-пакеты, соответствующие заданным параметрам.
  - Источник и назначение IP-пакетов, на которые распространяется действие фильтра.
  - Протоколы фильтрации IP-пакетов.
  - Расписание действия.
- Для задания параметров фильтра могут использоваться группы объектов.

- IP-пакеты проверяются в соответствии с расположением фильтров в списке, по порядку сверху вниз. Когда пакет блокируется или пропускается первым подходящим фильтром, последующие фильтры уже не оказывают никакого влияния на данный пакет.
- В веб-интерфейсе фильтры располагаются в порядке убывания их приоритета согласно схеме выше.

Использование групп объектов

Группы объектов — это средство, позволяющее упростить создание сетевых фильтров в ViPNet Terminal. Группы объектов объединяют нескольких объектов одного типа (например, несколько IP-адресов). При создании фильтров администратор сети ViPNet может указать группу вместо перечисления нескольких отдельных объектов.

Группы объектов могут включать следующие типы объектов:

- Группы узлов ViPNet — могут содержать любую комбинацию идентификаторов защищенных узлов, используются при создании фильтров защищенной сети.
- Группа IP-адресов — содержит любую комбинацию IP-адресов и диапазонов IP-адресов, используется в фильтрах открытой сети.
- Группа протоколов — содержит любую комбинацию сетевых протоколов и портов, используется в фильтрах открытой и защищенной сетей.
- Группа расписания — содержит любую комбинацию параметров, определяющих время действия фильтра, используется в фильтрах открытой и защищенной сетей.

Каждая группа объектов относится к одному из следующих видов:

- Системные группы объектов — настроенные по умолчанию группы с фиксированными именами, которые могут использоваться для задания адресов отправителей и получателей IP-пакетов в фильтрах, а также при создании пользовательских групп объектов. Такие группы объектов не отображаются в списках групп, их нельзя ни изменить, ни удалить.
- Группы объектов из программы ViPNet Policy Manager (см. Глоссарий, стр. 88) — группы, получаемые в составе политик безопасности, и используемые в соответствующих фильтрах. Такие группы нельзя ни удалять, ни изменять, ни использовать для задания параметров пользовательских фильтров и групп объектов.
- Пользовательские группы объектов — группы, создаваемые пользователем на узле, а также несколько групп, настроенных по умолчанию. Такие группы можно использовать для задания параметров сетевых фильтров, а также при создании других пользовательских групп объектов. При необходимости их можно удалить.

Группы отличаются друг от друга составом объектов, которые они включают. При этом для группы объектов могут быть заданы исключения. Группа объектов и исключения группы объектов могут содержать другие группы объектов того же вида и системные группы объектов.

Вы можете создавать и изменять пользовательские группы объектов следующими способами:

- С помощью командного интерпретатора.

- С помощью веб-интерфейса ViPNet Terminal.

Просмотр сетевых фильтров

С помощью веб-интерфейса вы можете просмотреть сетевые фильтры (см. Глоссарий, стр. 90), которые заданы на вашем узле ViPNet Terminal. Для этого выполните следующие действия:

1 В многооконном режиме работы нажмите кнопку и в меню выберите пункт **Настройка**, откроется начальная страница настройки ViPNet Terminal (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29).

2 На начальной странице щелкните плитку **Межсетевой экран**.

3 На странице **Сетевые фильтры** выберите вкладку, соответствующую нужному типу сетевых фильтров.

На панели просмотра отобразится список сетевых фильтров выбранного типа в порядке убывания их приоритета.

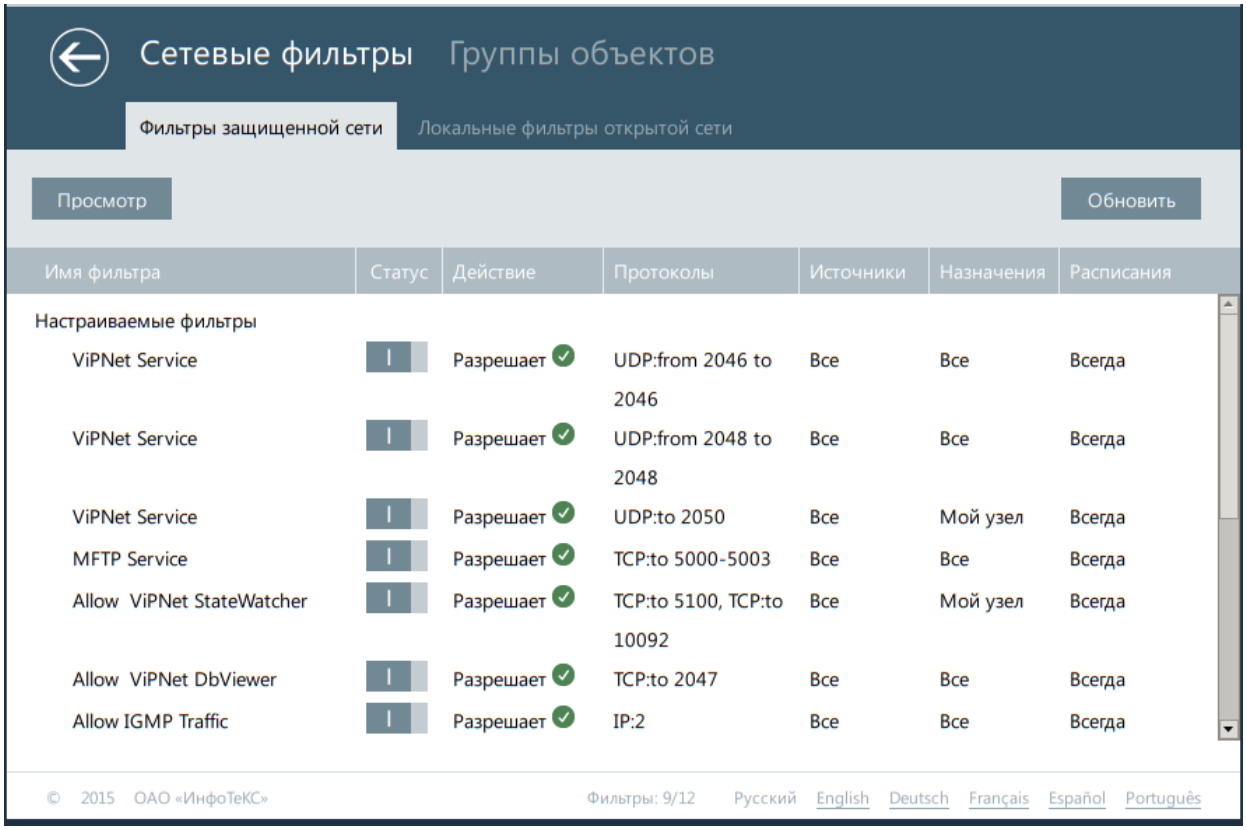

Рисунок 36. Просмотр фильтров защищенной сети

4 Для просмотра подробной информации о фильтре дважды щелкните его в списке.

Примечание. Редактирование сетевых фильтров возможно только в режиме администратора (см. документ «ViPNet Terminal. Руководство администратора»).

Просмотр групп объектов

С помощью веб-интерфейса вы можете просматривать имеющиеся на вашем сетевом узле группы объектов, которые могут быть использованы при создании сетевых фильтров. Для этого выполните следующие действия:

1 В многооконном режиме работы нажмите кнопку и в меню выберите пункт **Настройка**, откроется начальная страница настройки ViPNet Terminal (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29).

2 На начальной странице щелкните плитку **Межсетевой экран**.

3 На странице **Группы объектов** выберите вкладку с нужным типом групп объектов.

На панели просмотра отобразится список групп объектов выбранного типа. В списке отображаются системные группы объектов, группы, созданные пользователем, и группы, полученные из программы ViPNet Policy Manager.

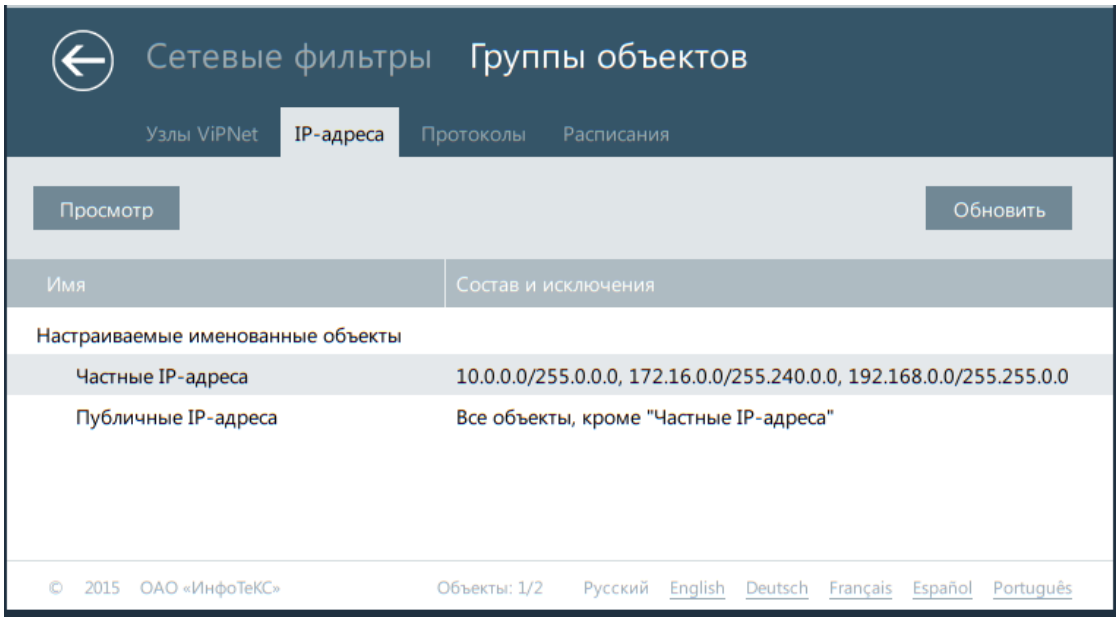

Рисунок 37. Просмотр групп IP-адресов

4 Для просмотра подробной информации о группе дважды щелкните нужную группу в списке.

Примечание. Редактирование групп объектов возможно только в режиме администратора (см. документ «ViPNet Terminal. Руководство администратора»).

Работа с конфигурациями сетевого экрана

Описание конфигураций сетевого экрана

В ПО ViPNet Terminal имеются следующие стандартные конфигурации сетевого экрана (см. «Конфигурация сетевого экрана ViPNet Terminal» на стр. 89):

- **VPN и Интернет**. При выборе этой конфигурации разрешена работа с защищенными ресурсами сети ViPNet и доступ к открытым ресурсам Интернета.
- **VPN**. При выборе этой конфигурации разрешена работа с защищенными ресурсами сети ViPNet, запрещен доступ к открытым ресурсам Интернета.
- **Интернет**. При выборе этой конфигурации разрешен доступ к открытым ресурсам Интернета, запрещена работа с защищенными ресурсами сети ViPNet.
- **Блокировать сеть.** При выборе этой конфигурации блокируются все входящие и исходящие соединения. Работа в защищенной сети ViPNet и в Интернете невозможна.
- **Отключить защиту.** При выборе этой конфигурации прекращается шифрование и фильтрация трафика ViPNet-драйвером. Работа с ресурсами защищенной сети ViPNet невозможна, однако есть доступ к ресурсам Интернета. При этом все настроенные на узле сетевые фильтры применяться не будут.
- **Интернет через шлюз**. При выборе этой конфигурации доступ к открытым ресурсам Интернета осуществляются через координатор, выполняющий роль сервера открытого Интернета. Работа с защищенными ресурсами сети ViPNet запрещена. Конфигурация доступна только при наличии в справочниках связи с координатором, который настроен для работы в качестве сервера открытого Интернета. В этом случае конфигурация «Интернет» не отображается.

  Используйте данную конфигурацию для работы, например, находясь в общественном месте, где для доступа к Интернету используется сеть Wi-Fi или 3G. Так как все соединения с узлами открытой сети осуществляются через координатор, то для администратора точки доступа они будут невидимы, что исключает возможность перехвата трафика.

Примечание. В ПО ViPNet Terminal предусмотрены только стандартные конфигурации сетевого экрана. Пользователи не могут создавать новые конфигурации или изменять параметры уже имеющихся.

Смена конфигурации

Чтобы сменить конфигурацию сетевого экрана, выполните следующие действия:

1 В многооконном режиме работы нажмите кнопку и в меню выберите пункт **Настройка**, откроется начальная страница настройки ViPNet Terminal (см. «Начало работы с веб-интерфейсом ViPNet Terminal» на стр. 29).

2 На начальной странице в правом верхнем углу окна щелкните значок .

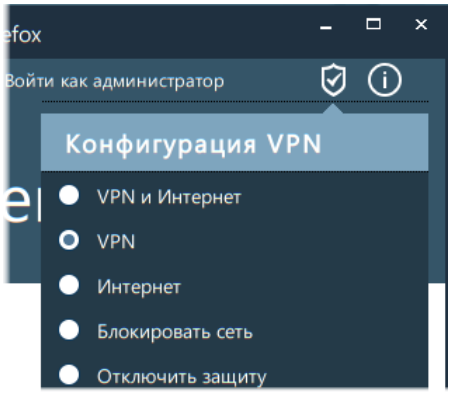

Рисунок 38: Смена конфигураций сетевого экрана ViPNet Terminal

3 В меню **Конфигурация VPN** выберите одну из доступных конфигураций сетевого экрана.

Примечание. Список доступных конфигураций зависит от расположения узла в сети ViPNet.

Подробнее о конфигурациях ViPNet Terminal см. раздел Описание конфигураций сетевого экрана (на стр. 72).

4

Сценарии работы в терминальной сессии

Использование звуковых устройств в терминальной сессии 75

Использование съемных носителей в терминальной сессии 76

Использование электронной подписи в терминальной сессии 77

Печать на локальном принтере в терминальной сессии 78

Установка принтера 79

Использование звуковых устройств в терминальной сессии

Если при работе в терминальной сессии требуется воспроизводить на локальном компьютере звук из приложений, запущенных на терминальном сервере, выполните следующие действия:

1. Убедитесь, что на терминальном сервере разрешено перенаправление аудиоустройств. Информацию о настройке перенаправления устройств можно найти в документации используемого терминального сервера.
2. На компьютере с программным обеспечением ViPNet Terminal включите перенаправление звуковых устройств (см. «Настройка перенаправления звуковых устройств на терминальный сервер» на стр. 34).
3. Подключите к компьютеру звуковые устройства, например наушники и микрофон.

Примечание. Если вы используете ViPNet Terminal в варианте исполнениях K или T (см. «Варианты исполнения ViPNet Terminal» на стр. 14), для подключения микрофона с разъемом «мини-джек» следует использовать гнездо на передней панели компьютера.

Использование съемных носителей в терминальной сессии

Если на компьютере с программным обеспечением ViPNet Terminal и на терминальном сервере разрешено перенаправление съемных носителей, при работе в терминальной сессии вы сможете использовать съемные носители, подключенные к локальному компьютеру. Используемые съемные носители должны иметь файловую систему FAT32.

Чтобы использовать съемный носитель при работе в терминальной сессии:

1 На компьютере с программным обеспечением ViPNet Terminal включите перенаправление съемных носителей (см. «Настройка перенаправления USB-устройств» на стр. 62).

2 Включите компьютер и запустите терминальную сессию (см. «Графический интерфейс ViPNet Terminal» на стр. 24).

3 Подключите носитель к компьютеру.

Носитель будет автоматически перенаправлен на терминальный сервер. На сервере он будет отображаться как сетевой диск, в имени которого указан идентификатор вашего сетевого узла, например: `W на tc_15e90013`.

Примечание. Если съемный носитель не отображается на терминальном сервере, отключите и снова подключите носитель.

4 Выполните необходимые действия с файлами, находящимися на съемном носителе.

5 По окончании работы с файлами закройте все приложения, в которых были открыты эти файлы, и окна проводника, в которых отображается содержимое съемного носителя.

Внимание! Не отключайте съемный носитель во время чтения или записи данных. Перед извлечением съемного носителя рекомендуется подождать около пяти минут, так как синхронизация файлов на терминальном сервере и на съемном носителе занимает некоторое время.

Использование электронной подписи в терминальной сессии

Если вы подключаетесь к терминальному серверу по протоколу RDP или ICA и у вас имеется устройство аутентификации, на котором сохранен контейнер ключей электронной подписи (см. Глоссарий, стр. 89), вы можете использовать электронную подпись при работе в терминальной сессии. Для этого требуется, чтобы на терминальном сервере были установлены криптопровайдер ViPNet CSP и драйвер используемого устройства. В настройках ViPNet Terminal должно быть разрешено перенаправление устройства аутентификации.

Для работы с электронной подписью выполните следующие действия:

1. На компьютере с программным обеспечением ViPNet Terminal включите перенаправление устройств аутентификации (см. «Настройка перенаправления USB-устройств» на стр. 62).
2. Включите компьютер и запустите терминальную сессию (см. «Графический интерфейс ViPNet Terminal» на стр. 24).
3. Подключите устройство аутентификации к компьютеру.
4. В окне настройки криптопровайдера ViPNet CSP добавьте контейнер ключей, который хранится на устройстве аутентификации, в список используемых контейнеров. Также установите сертификат ключа проверки электронной подписи (см. Глоссарий, стр. 90) в системное хранилище.

   Подробнее об установке контейнера и сертификата см. документацию к приложению ViPNet CSP.
5. Используйте сертификат для формирования электронной подписи в различных приложениях.

   Для получения подробной информации об использовании электронной подписи в тех или иных приложениях обратитесь к документации этих приложений. Применение электронной подписи в программах Microsoft Office описано в документе «ViPNet CSP. Руководство пользователя».

Печать на локальном принтере в терминальной сессии

В процессе работы часто возникает необходимость распечатать какие-либо документы. Если вы работаете в терминальной сессии (см. Глоссарий, стр. 90), вы используете ресурсы терминального сервера и можете распечатывать документы с помощью принтера, подключенного к серверу. Однако на практике терминальный сервер может быть значительно удален от вашего компьютера, и желательно использовать локальный принтер, подключенный к компьютеру, или какой-либо доступный сетевой принтер. Для этого требуется:

- На обоих компьютерах установить драйвер принтера.
- В параметрах ПО ViPNet Terminal и на терминальном сервере разрешить перенаправление принтера.
- В ПО ViPNet Terminal установить принтер (см. «Установка принтера» на стр. 79).

При выполнении указанных условий локальный принтер будет доступен для печати.

Чтобы в терминальной сессии распечатать документ на локальном принтере, выполните следующие действия:

1. Подключитесь к терминальному серверу, при работе с которым вы хотите использовать принтер.
2. В используемом приложении отправьте документ на печать и выберите локальный принтер, подключенный к компьютеру с ПО ViPNet Terminal.

   Вы можете найти ваш принтер на терминальном сервере по имени порта принтера, которое содержит идентификатор вашего сетевого узла, например `tc_10e10920`.
3. Если необходимо очистить очередь печати:
   - При работе в полноэкранном режиме нажмите сочетание клавиш **Ctrl+Alt+Backspace**.
   - При работе в многооконном режиме используйте возможности системы печати CUPS (см. Глоссарий, стр. 87). Также очередь печати автоматически очищается при перезапуске графической сессии.

Установка принтера

Чтобы установить принтер, выполните следующие действия:

1 Если вы хотите установить локальный принтер, подключите его к USB-разъему компьютера.

Внимание! Принтер следует подключить к компьютеру до начала его установки и не отключать в течение всего времени работы принтера.

---

2 В многооконном режиме работы нажмите кнопку .

3 В открывшемся меню выберите пункт **Принтеры**. В окне веб-браузера Firefox будет открыта страница системы печати CUPS (Common UNIX Printing System).

Примечание. Если во время работы с системой печати CUPS потребуется аутентификация, укажите имя пользователя `user` и пароль пользователя сетевого узла ViPNet Terminal. Если для аутентификации на сетевом узле используется внешнее устройство, в качестве пароля укажите `token`.

---

4 На странице CUPS перейдите на вкладку **Администрирование**.

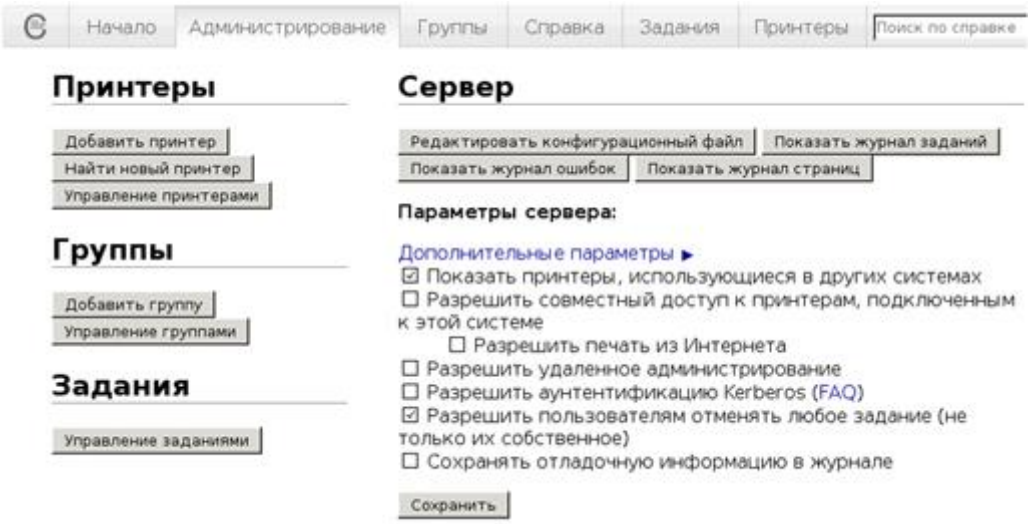

Рисунок 39. Страница системы печати CUPS

5 Чтобы добавить принтер, выполните следующие действия:

- Нажмите кнопку **Найти новый принтер**.
- В списке найденных принтеров выберите ваш принтер и нажмите кнопку **Добавить этот принтер**.

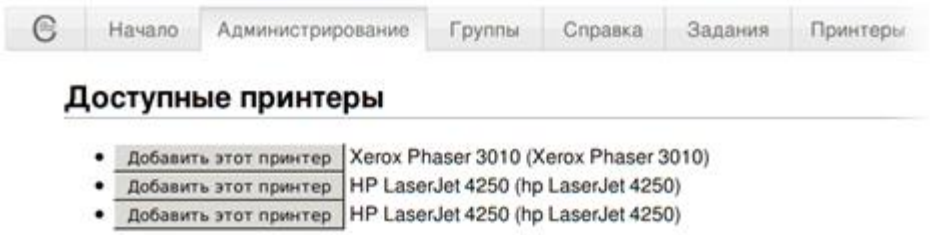

Рисунок 40. Список найденных принтеров

Если принтер, который вы хотите подключить, не определяется автоматически:

- Нажмите кнопку **Добавить принтер**.
- Выберите в списке нужный принтер и нажмите кнопку **Продолжить**.

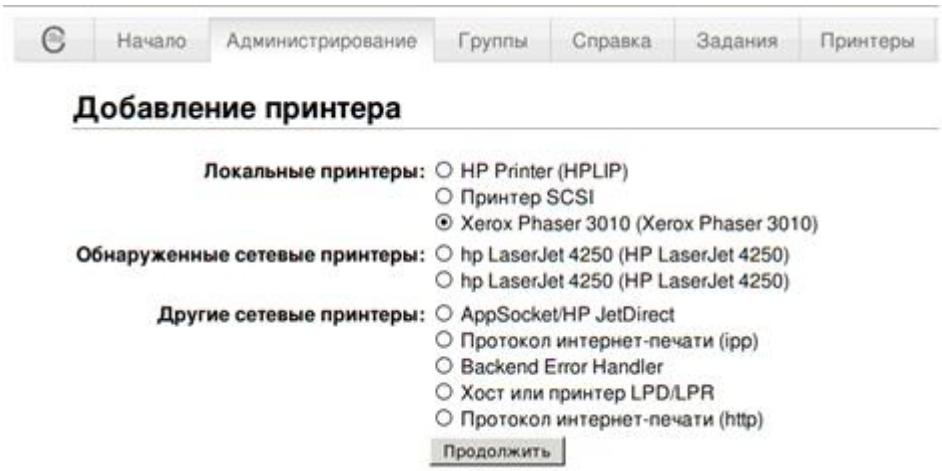

Рисунок 41. Принтеры, доступные для добавления

Внимание! Поиск сетевых принтеров доступен только в конфигурациях **VPN и Интернет**, **Интернет**, **Отключить защиту** (см. «Описание конфигураций сетевого экрана» на стр. 72). Причем для первых двух конфигураций необходимо, чтобы администратор добавил сетевой фильтр, разрешающий групповую рассылку (исходящие соединения на системную группу объектов MultiCast).

В конфигурации **Отключить защиту** и для добавления сетевого принтера вручную фильтр для групповой рассылки не требуется.

---

6 На странице **Добавление принтера** введите описание принтера и нажмите кнопку **Продолжить**.

7 На следующей странице выберите в списке производителя принтера и нажмите кнопку **Продолжить**. Затем выберите в списке модель принтера и нажмите кнопку **Добавить принтер**.

Примечание. Если у вас имеется файл PPD для устанавливаемого принтера, поместите этот файл на съемный USB-носитель и подключите его к компьютеру. На странице **Добавление принтера** нажмите кнопку **Обзор** и укажите путь к файлу PPD. Например: `/mnt/drive/A/printer.ppd`.

---

8 На странице **Установить параметры по умолчанию**, если требуется, измените параметры печати. Затем нажмите кнопку **Сохранить параметры по умолчанию**.

9 Для печати пробной страницы на вкладке **Принтеры** выберите установленный принтер, затем в списке **Обслуживание** выберите пункт **Печать пробной страницы**.

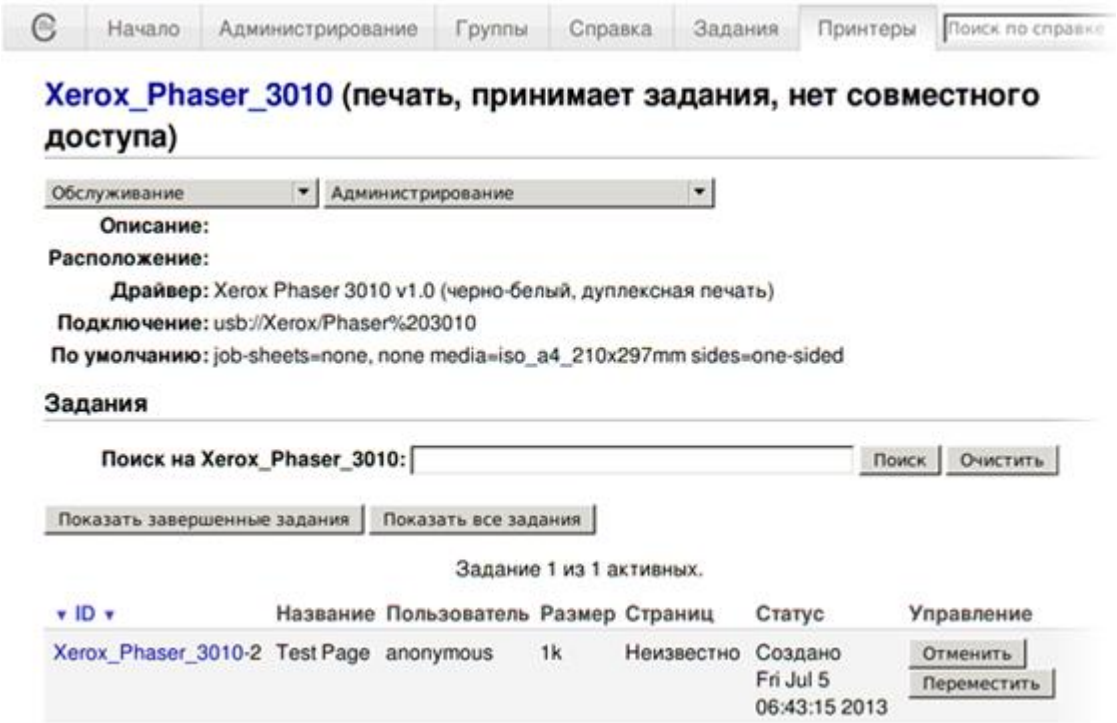

Рисунок 42. Свойства установленного принтера

10 Если печать пробной страницы прошла успешно, в списке **Администрирование** выберите пункт **Установить как принтер по умолчанию**.

В результате:

- При подключении к терминальному серверу Citrix ваш принтер будет установлен на терминальном сервере автоматически.

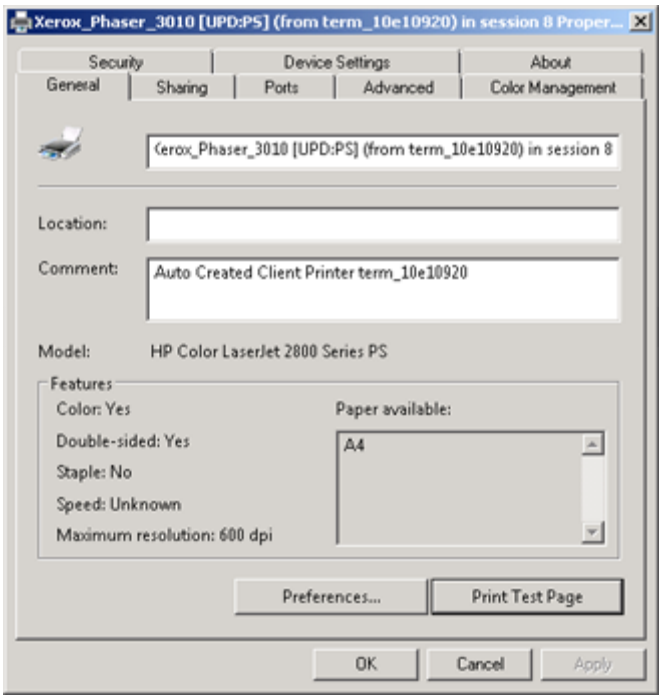

Рисунок 43. Свойства принтера на терминальном сервере Citrix

- При подключении к терминальному серверу по протоколу RDP при помощи клиента FreeRDP (см. «Настройка дополнительных параметров подключения к терминальному серверу» на стр. 62) ваш принтер будет установлен на терминальном сервере автоматически.

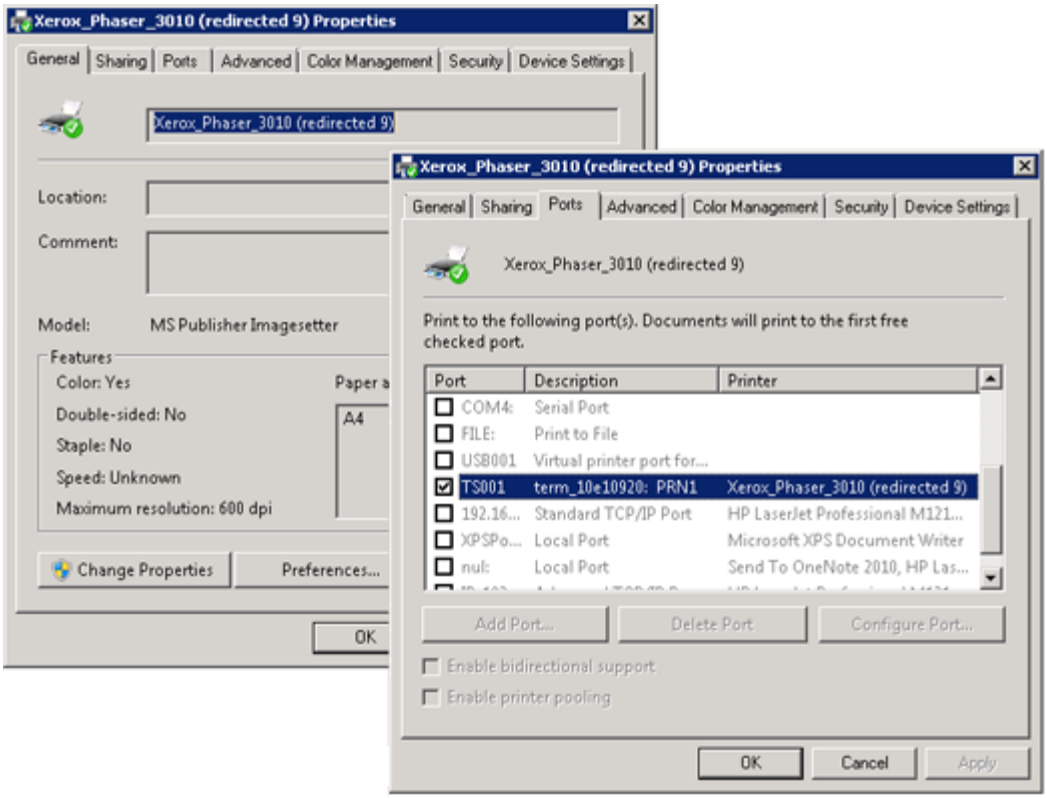

Рисунок 44. Свойства принтера на терминальном сервере Windows Server

- При подключении к терминальному серверу по протоколу RDP при помощи клиента Rdesktop (см. «Настройка дополнительных параметров подключения к терминальному серверу» на стр. 62) установите принтер вручную, выбрав порт принтера с идентификатором вашего сетевого узла.

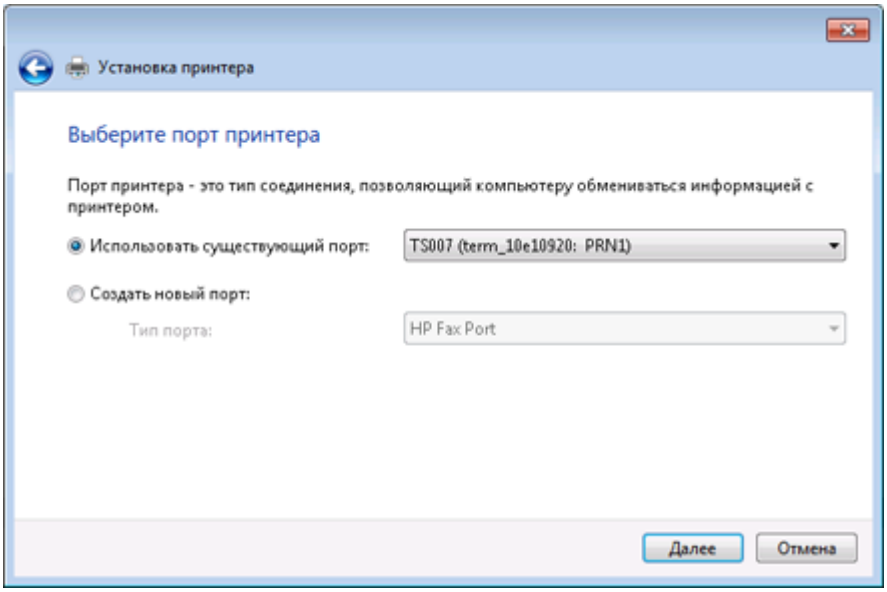

Рисунок 45. Установка принтера на терминальном сервере

Участие в видеоконференциях

Внимание! Функция недоступна в минимальном варианте ПО ViPNet Terminal.

Программное обеспечение ViPNet Terminal включает в себя следующие клиенты видеоконференций:

- TrueConf, разработанный компанией TrueConf.
- Vinteo, разработанный компанией Vinteo.

Вызов и начало работы с этими клиентами описаны в следующих разделах:

- Участие в видеоконференции TrueConf (на стр. 84).
- Участие в видеоконференции Vinteo (на стр. 85).

Участие в видеоконференции TrueConf

Чтобы начать работу с клиентом TrueConf, выполните следующие действия:

1 В многооконном режиме работы нажмите кнопку и в появившемся меню выберите пункт **Видеоконференция** > **TrueConf**.

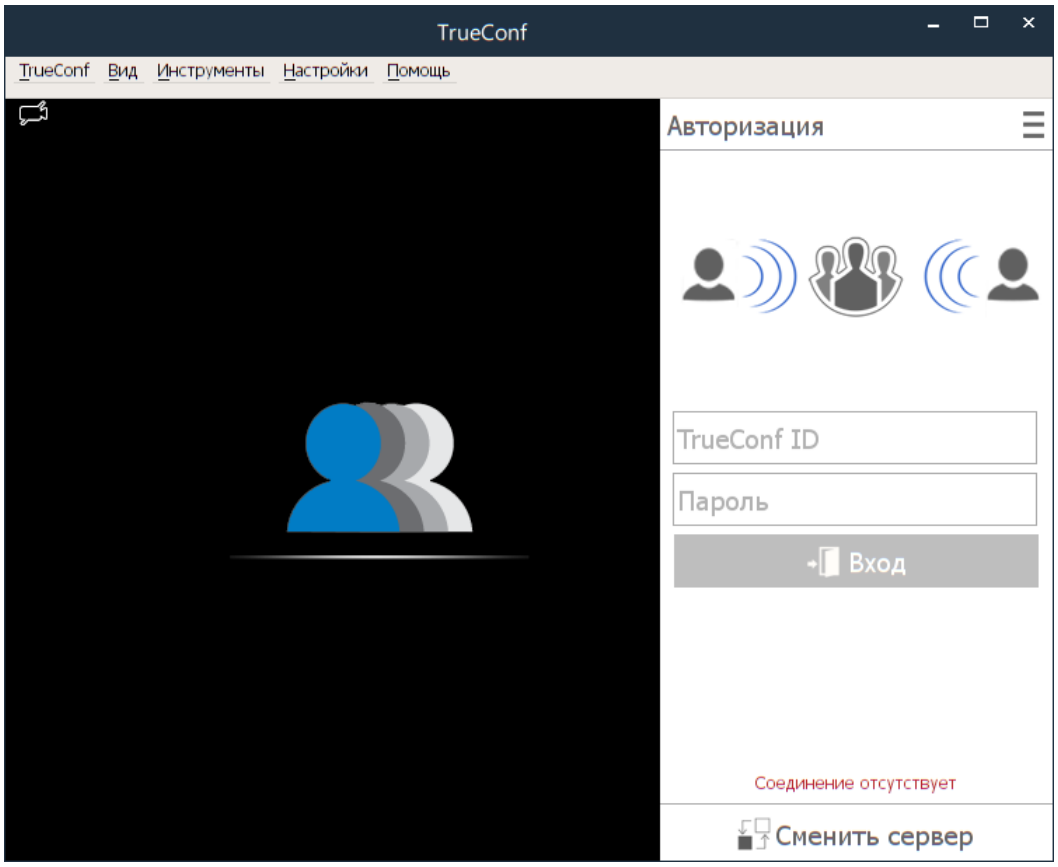

Рисунок 46. Начало работы с клиентом видеоконференций TrueConf

2 В окне **TrueConf** задайте необходимые настройки оборудования и подключитесь к серверу видеоконференций TrueConf.

Примечание. Подробнее о работе видеоконференций TrueConf см. документацию на веб-сайте этого продукта (http://trueconf.ru/support/online-help/).

Участие в видеоконференции Vinteo

Чтобы начать работу с клиентом Vinteo, выполните следующие действия:

1 В многооконном режиме работы нажмите кнопку и в появившемся меню выберите пункт **Видеоконференция** > **Vinteo**.

2 В окне **Vinteo Desktop** в меню **Vinteo Desktop** выберите пункт **Параметры**.

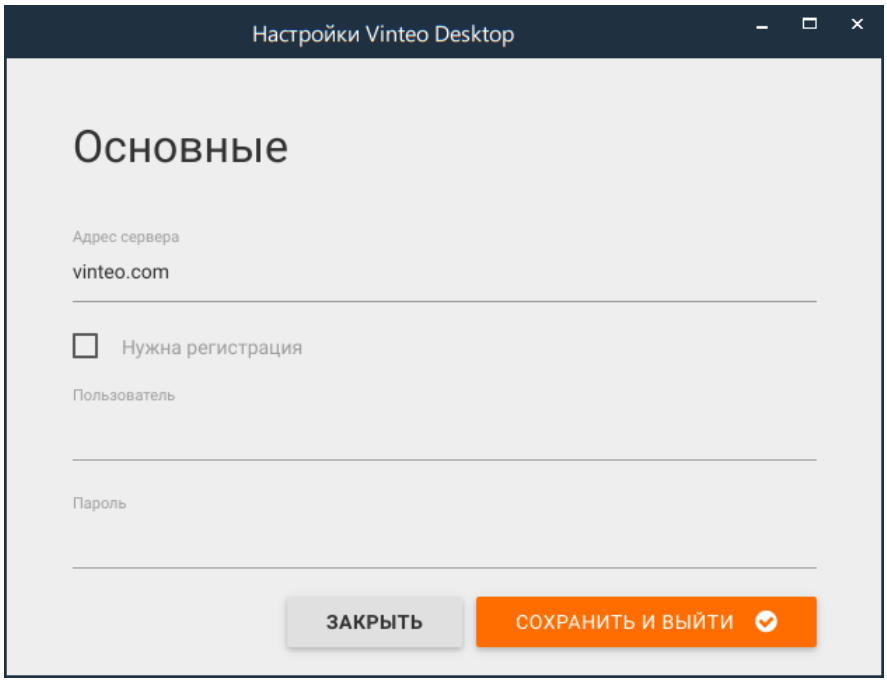

Рисунок 47. Начало работы с клиентом видеоконференций Vinteo

3 В окне **Настройки Vinteo Desktop** задайте необходимые данные и подключитесь к серверу видеоконференций Vinteo.

Примечание. Подробнее о работе видеоконференций Vinteo см. документацию на веб-сайте этого продукта (http://vinteo.ru/download/).

A

Глоссарий

3G

Технология мобильной связи третьего поколения, которая используется для скоростного мобильного доступа в Интернет.

CUPS

Система печати для UNIX-подобных операционных систем (Common UNIX Printing System).

DHCP-сервер

Сервер, автоматически администрирующий IP-адреса клиентов и выполняющий соответствующую настройку для сети.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование делается для повышения отказоустойчивости системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

Ethernet

Стандарт передачи данных в локальной компьютерной сети с помощью кабеля.

LTE

Технология мобильной связи четвертого поколения, которая представляет собой усовершенствование технологии 3G и используется для скоростного мобильного доступа в Интернет.

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

ViPNet Policy Manager

Программа, которая входит в состав программного комплекса ViPNet. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Wi-Fi

Технология беспроводного доступа в Интернет с использованием радиоканалов.

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ проверки электронной подписи

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ проверки электронной подписи является открытой (не секретной) частью пары асимметричных ключей.

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ электронной подписи является закрытой (секретной) частью пары асимметричных ключей.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Terminal с помощью ряда специальных команд.

Контейнер ключей

Файл, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Конфигурация сетевого экрана ViPNet Terminal

Фиксированный набор параметров работы узла ViPNet Terminal в сети, таких как режим фильтрации трафика и доступа к защищенной и открытой сетям. Набор доступных конфигураций определяет администратор сети ViPNet.

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках

сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Прокси-сервер

Программа, транслирующая соединения по некоторым протоколам из внутренней сети во внешнюю и выступающая при этом как посредник между клиентами и сервером.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Терминальная сессия

Сеанс удаленной работы с приложениями, выполняющимися на терминальном сервере.

Терминальный сервер

Выделенный компьютер, предоставляющий вычислительные ресурсы клиентам, которые подключаются к терминальному серверу по сети. Преимущества работы в терминальном режиме включают снижение расходов на программное и аппаратное обеспечение, уменьшение затрат времени на администрирование, повышение уровня защиты от внутренних злоумышленников.

Тонкий клиент

Компьютер, предназначенный для доступа к приложениям и данным, которые размещаются на терминальном сервере.

Туннелирование

Технология, позволяющая защитить соединение с участием открытых узлов при передаче данных через Интернет и другие публичные сети. Туннелирование заключается в шифровании трафика открытых узлов координаторами.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

B

Указатель

3

3G - 38, 41

C

CUPS - 78

D

DNS-сервер - 44

E

Ethernet - 38

L

LTE - 38, 42

N

NTP-сервер - 45

V

ViPNet Policy Manager - 68, 69

W

Wi-Fi - 38, 39

А

Аппаратная платформа Kraftway Credo VV18 - 14

В

Варианты исполнения ViPNet Terminal - 21, 22, 63, 75
Виртуальная защищенная сеть - 26

Г

Графический интерфейс ViPNet Terminal - 21, 23, 76, 77

Д

Добавление терминального сервера - 47
Дополнительные параметры подключения к терминальному серверу Citrix в - 50
Дополнительные параметры подключения к терминальному серверу Citrix в обычном режиме - 50
Дополнительные параметры подключения к терминальному серверу Windows Server - 50
Дополнительные параметры подключения к терминальному серверу по протоколу HTTP или HTTPS - 50

Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами IBS - 50
Дополнительные параметры подключения к терминальному серверу с виртуальными рабочими столами VMware - 50

И

Изменение списка DNS-серверов - 39
Изменение списка NTP-серверов - 33, 39
Изменение списка доступных терминальных серверов - 10, 29, 50
Использование звуковых устройств в терминальной сессии - 10
Использование съемных носителей в терминальной сессии - 10
Использование электронной подписи в терминальной сессии - 10

К

Контейнер ключей - 77
Конфигурация сетевого экрана ViPNet Terminal - 67, 72

М

Многооконный режим работы - 24, 35, 48

Н

Настройка дополнительных параметров подключения к терминальному серверу - 49, 82, 83
Настройка параметров экрана - 24
Настройка перенаправления USB-устройств - 10, 49
Настройка перенаправления звуковых устройств на терминальный сервер - 75
Настройка подключения к сети - 21, 23, 30
Настройка системного времени - 21, 23
Настройка системных параметров - 30
Начало работы с веб-интерфейсом ViPNet Terminal - 25, 32, 33, 35, 36, 38, 39, 41, 42, 43, 45, 46, 47, 61, 70, 71, 72

О

Описание конфигураций сетевого экрана - 80
Основные возможности ViPNet Terminal - 35

П

Печать на локальном принтере в терминальной сессии - 10
Полноэкранный режим работы - 24, 51, 53, 56, 58, 60
Прокси-сервер - 35

Р

Работа с интегрированным сетевым экраном - 29
Работа со списком узлов защищенной сети - 29

С

Сертификат ключа проверки электронной подписи - 77
Сетевой узел ViPNet - 66
Сетевой фильтр - 70

Т

Таблица маршрутизации - 43
Терминальная сессия - 25, 78
Терминальный сервер - 9, 47
Тонкий клиент - 9

У

Установка принтера - 25, 78
Участие в видеоконференции TrueConf - 84
Участие в видеоконференции Vinteo - 84