TERMIDESK

Вариант лицензирования «TermideskTerminal»

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-02 90 02

Версия 5.0. Выпуск от мая 2024

Настройка программного комплекса

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

Настоящий документ является второй частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk). Документ предназначен для администраторов системы и сети.

Во второй части руководства приведена настройка Termidesk, рассмотрены взаимодействие компонентов, разграничение функций по администрированию. Для того чтобы получить информацию об установке программного комплекса, необходимо обратиться к первой части руководства администратора - СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса».

1.2 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

2 . ПОЛЬЗОВАТЕЛИ И КОМПОНЕНТЫ TERMIDESK

2.1 . Разграничение функций

Предусмотрено следующее разграничение функций по управлению Termidesk:

- функции администратора Termidesk;
- функции пользователя Termidesk;
- функции оператора Termidesk.

Администратору Termidesk доступны настройка и управление программным комплексом после успешного прохождения процедуры идентификации и аутентификации. По умолчанию с администратором ассоциируется локальный пользователь операционной системы (ОС) с полномочиями администратора на узле с установленным Termidesk.

> ⓘ Termidesk интегрирован со встроенным комплексом средств защиты информации ОС Astra Linux Special Edition. Идентификация и аутентификация, а также защита аутентификационной информации осуществляется средствами ОС.

Также поддерживаются следующие централизованные сетевые хранилища данных о субъектах и их полномочиях:

- FreeIPA;
- SAML;
- IP-аутентификация;
- Microsoft Active Directory (MS AD) или LDAP;
- RADIUS.

Пользователь Termidesk использует компонент «Клиент» для получения доступа к виртуальному рабочему месту (BPM).
Оператор Termidesk задается администратором Termidesk. Оператору Termidesk доступен ограниченный администратором Termidesk список полномочий по доступу в графический интерфейс управления.

2.2 . Схема взаимодействия компонентов и приложений

Схема взаимодействия компонентов Termidesk и приложений представлена на рисунке (см. Рисунок 1).

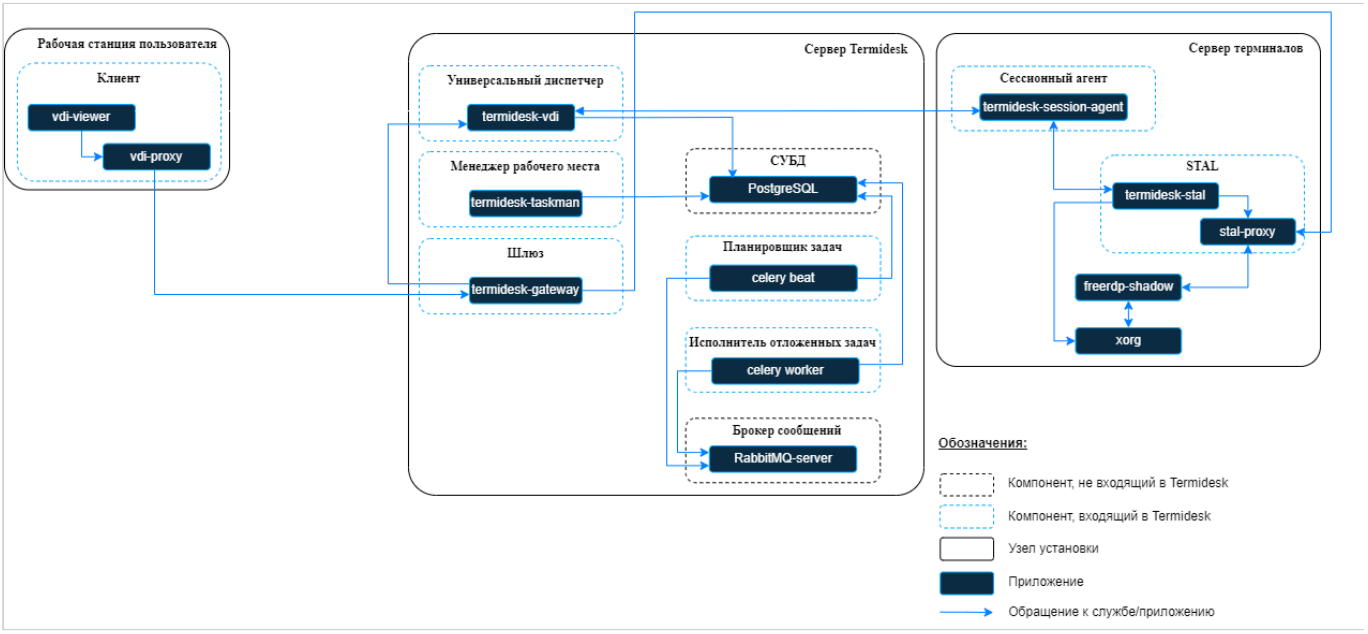

Рисунок 1 – Схема взаимодействия компонентов и процессов

2.3 . Схема сетевого взаимодействия компонентов Termidesk

Схема взаимодействия между сетевыми портами и компонентами Termidesk представлена на рисунке (см. Рисунок 2).

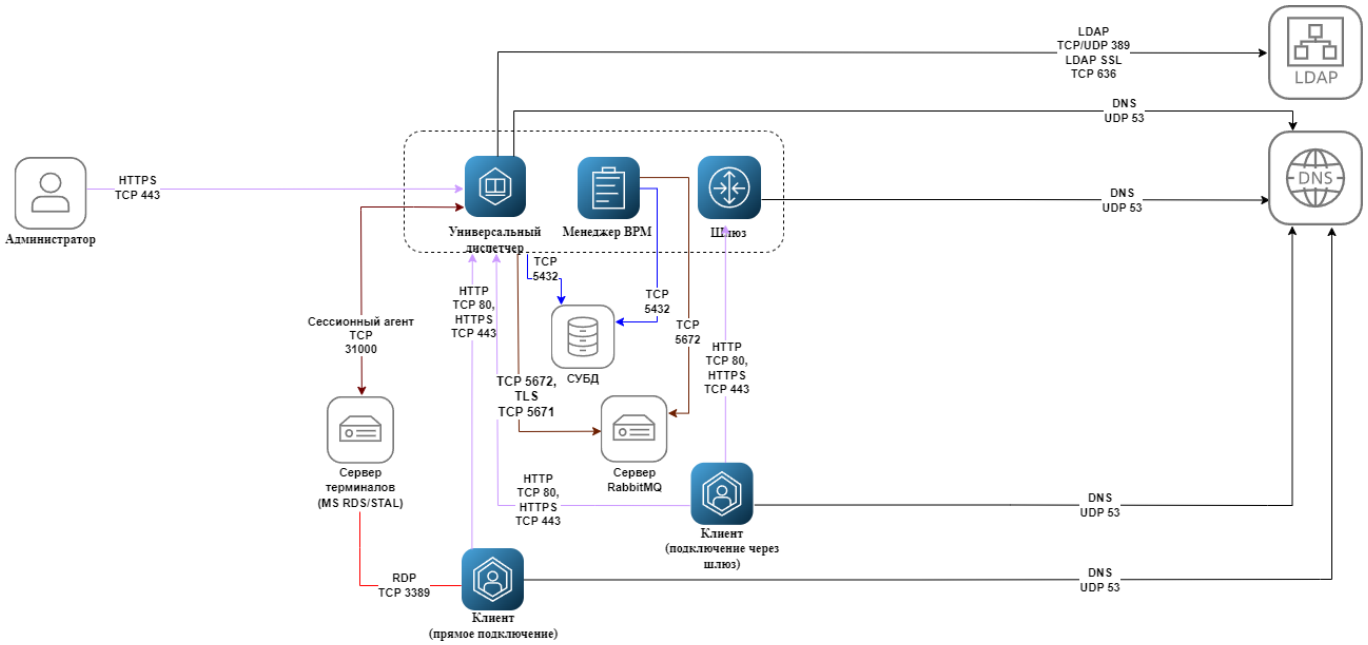

Рисунок 2 – Схема сетевого взаимодействия компонентов Termidesk

Общий перечень узлов и компонентов Termidesk представлен в таблице (см. Таблица 1).

Таблица 1 – Перечень узлов и компонентов

Компонент	Наименование на схеме	Узел установки	Наименование пакета установки
«Универсальный диспетчер»	Универсальный диспетчер	Отдельный узел для установки	`termidesk-vdi`

Компонент	Наименование на схеме	Узел установки	Наименование пакета установки
«Менеджер рабочих мест»	Менеджер BPM	Отдельный узел для установки или установка совместно с диспетчером	`termidesk-vdi`
«Шлюз»	Шлюз	Отдельный узел для установки или установка совместно с диспетчером	`termidesk-vdi`
«Сессионный агент»	Сессионный агент	Сервер терминалов (Microsoft Windows Server с ролью «Remote Desktop Services» (далее - MS RDS), Terminal Server Astra Linux (далее - STAL))	`termidesk-session-agent`
«Клиент»	Клиент	Рабочее место пользователя (пользовательская рабочая станция)	`termidesk-client`
«Сервер терминалов Astra Linux»	-	Сервер терминалов Astra Linux (STAL), возможна установка на том же узле, где установлен диспетчер	`stal`

2.4 . Последовательность сетевых запросов компонентов Termidesk

Последовательность сетевых запросов с указанием перечня портов для компонентов Termidesk и элементов инфраструктуры представлена на рисунке (см. Рисунок 3).

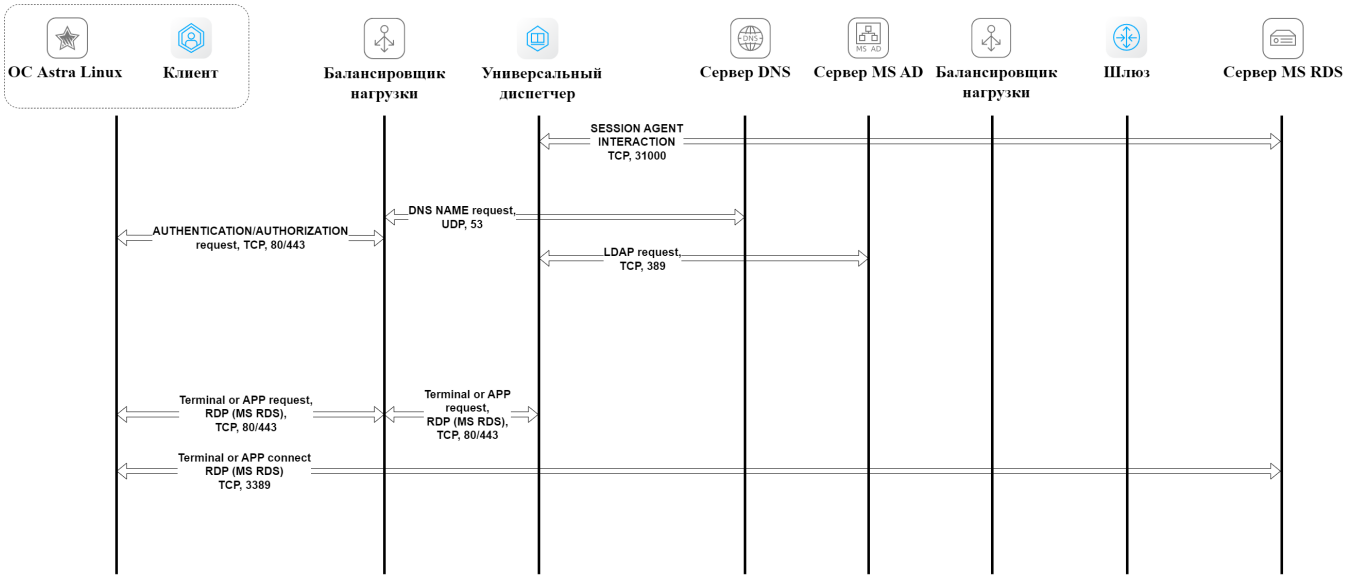

Рисунок 3 – Общая последовательность сетевых запросов

Последовательность сетевых запросов с указанием перечня портов при аутентификации и авторизации пользователя через компонент «Клиент» представлена на рисунке (см. Рисунок 4).

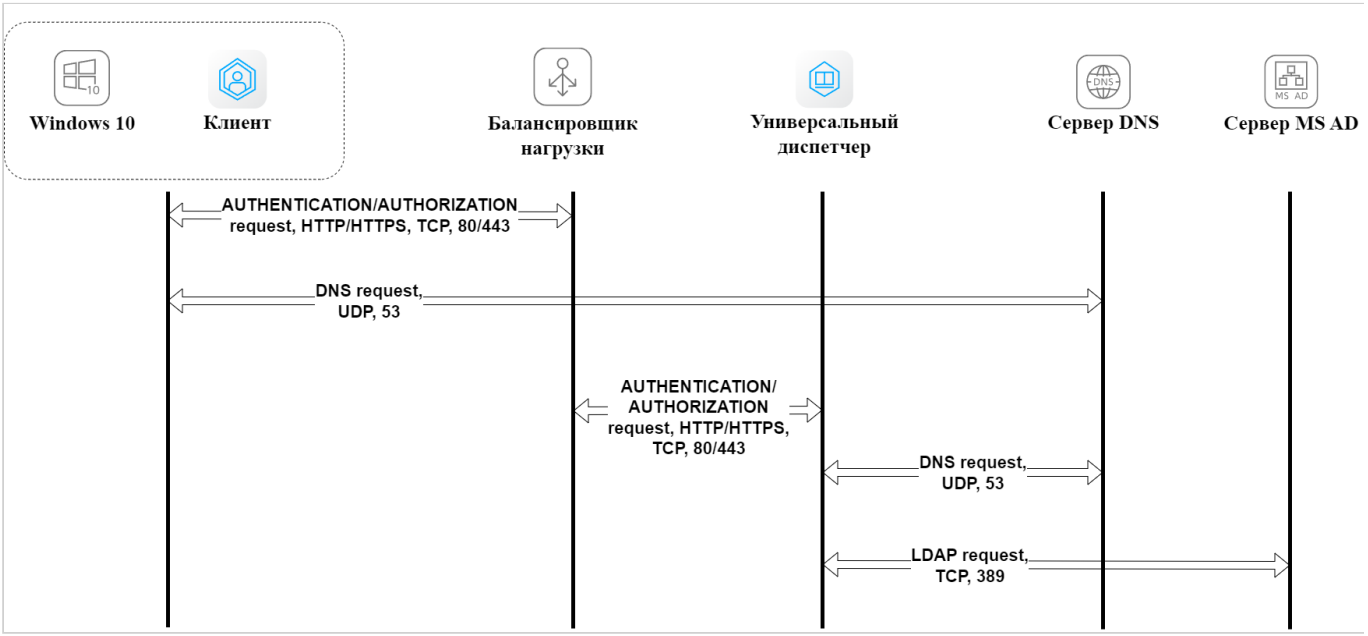

Рисунок 4 – Последовательность сетевых запросов при аутентификации и авторизации

2.5 . Перечень сетевых портов компонентов Termidesk

Перечень сетевых портов, используемых компонентами Termidesk, приведен в таблице (см. Таблица 2).

Таблица 2 – Перечень сетевых портов, используемых компонентами Termidesk

Служба	Протокол	Порт
«Универсальный диспетчер»		
HTTP	TCP	80
LDAP	TCP/UDP	389
HTTPS	TCP	443
LDAP SSL	TCP	636
AMQP (RabbitMQ)	TCP	5672
AMQPS (RabbitMQ)	TCP	5671
POSTGRESQL	TCP	5432
VDI (`termidesk-vdi`)	TCP	8000
SESSION AGENT (`TermideskSessionAgent`)	TCP	31000
RPC INTERACTION	TCP	43900-44000
DNS	UDP	53
«Менеджер рабочих мест»		
POSTGRESQL	TCP	5432
AMQP (RabbitMQ)	TCP	5672
AMQPS (RabbitMQ)	TCP	5671

Служба	Протокол	Порт
HEALTH_CHECK	TCP	8100
«Шлюз»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
WSPROXY_HEALTHCHECK	TCP	8101
WSPROXY (`termidesk-wsproxy`)	TCP	5099
SPICE	TCP	5900-6166
DNS	UDP	53
Программное обеспечение termidesk-viewer (устанавливается с компонентом «Клиент»)		
HTTP	TCP	80
HTTPS	TCP	443
VNC	TCP	5900-59XX*
SPICE	TCP	5900-59XX*
RDP	TCP	3389
«Сессионный агент»		
SESSION AGENT HTTP/HTTPS (`TermideskSessionAgent`)	TCP	31000
«Клиент»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
CLIENT (`termidesk-client`)	TCP	49152-65535**
«Виртуальный модуль Termidesk»		
ETCD	TCP/UDP	2379, 2380
«Сервер терминалов Astra Linux» (STAL)		
RDP	TCP	3389
«Удаленный помощник»		
HTTP	TCP	80
HTTPS	TCP	443
STUN	TCP	19302
WebRTC	TCP/UDP	1024-65535

2.6 . Перечень разрешающих правил межсетевого экрана, необходимых для работы компонентов Termidesk

На межсетевом экране, использующемся в организации, нужно задать следующие разрешающие правила (см. Таблица 3) для работы компонентов Termidesk.

В таблице приняты обозначения:

- «Узел-источник» - узел, являющийся инициатором сетевого соединения;
- «Узел-приемник» - узел, являющийся принимающей стороной сетевого соединения;
- «Протокол» - протокол транспортного уровня или уровня приложения, используемый в рамках соединения;
- «Порт приемника» - сетевой порт, прослушиваемый принимающей стороной.

Сетевой порт, открываемый узлом-источником для установления соединения, назначается динамически из диапазона 49152–65535, который определен настройками стека TCP/IP в ОС. В стеке TCP/IP ОС эти значения могут быть изменены.

Таблица 3 – Перечень правил межсетевого экрана

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Универсальный диспетчер»	`localhost`	TCP	8000	Работа веб-сервера «Универсального диспетчера» для обслуживания входящих подключений. Порт открывается на `localhost`
	Контроллеры доменов аутентификации	TCP/UDP	389	LDAP
		TCP	3268	LDAP
		TCP	636, 3269	LDAPS
	Сервер DNS	UDP	53	DNS
	«Сессионный агент»	TCP	31000	Для обслуживания подключений к серверам терминалов, на которых установлен «Сессионный агент»
	СУБД	TCP	5432	Для обслуживания запросов к СУБД
	Сервер RabbitMQ	TCP	5672, 5671 (TLS)	Для обслуживания запросов к RabbitMQ

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
	«Шлюз»	TCP	8102	Для обслуживания запросов проверок состояния (health check) «Шлюза»
	«Менеджер рабочих мест»	TCP	8100	Для обслуживания запросов проверок состояния (health check) «Менеджера рабочих мест»
Рабочее место администратора	«Универсальный диспетчер»	TCP	443	Защищенное подключение к порталу Termidesk
	«Удаленный помощник» (серверная часть)	TCP	80, 443	Защищенное подключение к серверной части «Удаленного помощника»
«Менеджер рабочих мест»	`localhost`	TCP	8100	Для обслуживания запросов проверок состояния (health check) «Менеджера рабочих мест». Порт открывается на `localhost`
	СУБД	TCP	5432	Для обслуживания запросов к СУБД
	Сервер RabbitMQ	TCP	5672, 5671 (TLS)	Для обслуживания запросов к RabbitMQ
«Шлюз»	`localhost`	TCP	5099	Для обслуживания входящих подключений к «Шлюзу». Порт открывается на `localhost`, при распределенной установке - на IP-адресе «0.0.0.0»

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
	`localhost`	TCP	8102	Для обслуживания запросов проверок состояния (health check) «Шлюза». Порт открывается на `localhost`
	Сервер DNS	UDP	53	DNS
«Клиент»	Сервер DNS	UDP	53	DNS
	«Универсальный диспетчер»	TCP	80, 443	Для обслуживания подключений к «Универсальному диспетчеру»
	Сервер терминалов	TCP	3389	Для обслуживания подключений RDP к серверу терминалов
		TCP	43900-44000	Для корректной работы технологии единого входа (SSO) при прямом подключении к BPM (не через «Шлюз»)
«Сервер терминалов Astra Linux»	Сервер DNS	UDP	53	DNS
	Контроллеры доменов аутентификации	TCP/UDP	389	LDAP
		TCP	3268	LDAP
		TCP	636, 3269	LDAPS
«Виртуальный модуль Termidesk»	«Виртуальный модуль Termidesk»	TCP/UDP	2379, 2380	Подключение ETCD для хранения и синхронизации конфигураций между узлами «Виртуального модуля Termidesk»
«Удаленный помощник» (клиентская часть)	«Удаленный помощник» (серверная часть)	TCP/UDP	80, 443	Для обслуживания подключений к серверной части «Удаленного помощника»

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
	Сервер STUN	TCP	19302	Для обслуживания подключений к серверу STUN (stun:// stun.l.google.com: 19302)
«Удаленный помощник» (серверная часть)	«Удаленный помощник» (клиентская часть)	TCP	1024-65535	Для обслуживания подключений к клиентской части «Удаленного помощника»

3 . НАЧАЛО РАБОТЫ

3.1 . Последовательность ввода в действие Termidesk Terminal

Общая последовательность шагов для ввода в действие Termidesk Terminal состоит в следующем:

- подготовка сетевой инфраструктуры в соответствии с требованиями раздела **Требования к среде функционирования** документа СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса»;
- установка Termidesk в зависимости от выбранной конфигурации: комплексная или распределенная (см. разделы и подразделы **Подготовка среды функционирования**, **Установка и настройка отделяемых компонентов на одном узле**, **Распределенная установка программного комплекса** документа СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса»). Ввод в домен (при необходимости, согласно схеме сетевой инфраструктуры предприятия);
- при использовании сервера терминалов на базе ОС Astra Linux Special Edition - установка компонента STAL (см. подраздел **Установка STAL** документа СЛЕТ.10001-02 90 06 «Руководство администратора. Настройка компонента «Сервер терминалов»). Рекомендуется использовать отдельный узел (физический или виртуальный) для сервера терминалов и не совмещать его установку с сервером Termidesk;
- установка компонента «Сессионный агент» на сервер терминалов (см. подраздел **Установка сессионного Агента** документа СЛЕТ.10001-02 90 04 «Руководство администратора. Настройка компонента «Агент»);
- переход в графический интерфейс Termidesk и добавление поставщика ресурсов «Сервер терминалов» в Termidesk (см. раздел **Добавление сервера терминалов (MS RDS и STAL) в качестве поставщика ресурсов**);
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов) (см. раздел **Аутентификация пользователей**);
- создание шаблона BPM для поставщика «Сервер терминалов» в Termidesk (см. подраздел **Шаблоны BPM для серверов терминалов**);
- добавление протоколов доставки, которые будут использоваться для подключения к BPM (см. раздел **Протоколы доставки**);
- создание и настройка фонда BPM в Termidesk (см. раздел **Фонд рабочих мест**)
- назначение групп в созданном ранее фонде (см. подраздел **Назначение групп доступа фонду BPM**);

- назначение протоколов доставки в созданном ранее фонде (см. подраздел **Назначение протоколов фонду BPM**).

4 . ПОСТАВЩИКИ РЕСУРСОВ

4.1 . Общие сведения о поставщиках ресурсов

Поставщик ресурсов в Termidesk варианта лицензирования «Termidesk Terminal» - это терминальный сервер, предоставляющий вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения ВРМ.

Веб-интерфейс Termidesk с установленной ролью «Портал администратора» обеспечивает следующие операции управления поставщиками ресурсов:

- добавление;
- редактирование;
- удаление;
- техобслуживание;
- просмотр сведений;
- организация шаблона ВРМ.

Для добавления в Termidesk поставщика ресурсов следует перейти «Компоненты - Поставщики ресурсов», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка необходимого поставщика.

Каждый поставщик ресурсов описывается перечнем параметров, требуемых Termidesk для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации надо использовать экранную кнопку **[Сохранить]**.

Для редактирования информации о созданном поставщике ресурсов следует перейти «Компоненты - Поставщики ресурсов», затем выбрать необходимого поставщика и нажать экранную кнопку **[Изменить]**.

Для удаления созданного поставщика ресурсов следует перейти «Компоненты - Поставщики ресурсов», затем выбрать необходимого поставщика и нажать экранную кнопку **[Удалить]**.

⚠ Поставщик ресурсов может быть удален только в том случае, если на нем не производится размещение фондов ВРМ.

4.2 . Добавление сервера терминалов (MS RDS и STAL) в качестве поставщика ресурсов

Для добавления следует перейти «Компоненты - Поставщики ресурсов», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Сервер терминалов».

⚠ Для взаимодействия с сервером терминалов (MS RDS или STAL) необходимо установить компонент «Сессионный агент» в соответствии с подразделом **Установка сессионного Агента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент».
Работа с сервером терминалов MS RDS поддерживается только при условии развернутой полнофункциональной инфраструктуры MS RDS. Если такой инфраструктуры нет, то рекомендуется воспользоваться решением, основанным на поставщике ресурсов «метапровайдер».

⚠ STAL реализуется компонентом «Сервер терминалов Astra Linux», который может быть установлен на узел совместно с Termidesk, в соответствии с подразделом **Установка STAL** документа СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов Astra Linux».

Для добавления в Termidesk сервера терминалов администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 4).

Таблица 4 – Данные для добавления сервера терминалов

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Адрес сессионного агента»	**FQDN** узла, на котором установлен сессионный агент Termidesk ⚠ Для инфраструктуры MS RDS в этом параметре обязательно нужно указывать не IP-адрес, а FQDN узла. Для STAL можно указать внешний IP-адрес узла. Если STAL установлен на одном узле с Termidesk, нужно также указывать внешний IP-адрес узла. Перед изменением FQDN или IP-адреса STAL необходимо завершить все активные сессии. После смены FQDN или IP-адреса STAL активные сессии, связанные с предыдущим FQDN или IP-адресом, становятся недоступными. Для восстановления доступа к STAL необходимо удалить предыдущие сессии и выполнить новое подключение.
«Порт сессионного агента»	Номер порта «Сессионного агента» Termidesk. По умолчанию номер порта 31000
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	Субъект, имеющий полномочия для управления сервером терминалов. Для подключения STAL в домене MS AD необходимо указывать логин локального администратора ОС узла, на котором установлен STAL. В ином случае тест соединения для поставщика может пройти успешно, но шаблон рабочего места при этом добавить не получится
«Пароль»	Набор символов, подтверждающий назначение полномочий

Параметр	Описание
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к «Сессионному агенту». По умолчанию выключено. При включении параметра на сервере терминалов должны быть добавлены валидные сертификаты и установлена опция USE_HTTPS в значение «True» в конфигурационном файле «Сессионного агента». В случае необходимости использовать протокол HTTP нужно отключить данный параметр и установить опцию USE_HTTPS в значение «False» конфигурационном файле «Сессионного агента»
«Валидация сертификата»	Выбор проверки подлинности сертификата при запросах к «Сессионному агенту». По умолчанию выключено

⚠ Если после попытки проверить введенные данные экранной кнопкой **[Тест]** появляются сообщения об ошибке, то при создании шаблона BPM будет блокироваться возможность его сохранения (создания).

⚠ Для корректного подключения через компонент «Клиент» к серверу терминалов необходимо задать параметр «Механизм обеспечения безопасности на уровне сети (RDP)» в политиках конкретного фонда BPM («Рабочие места - Фонды») в соответствии с выбранным сервером:

- «TLS» или «RDP» - для подключения к STAL;
- «NLA» - для подключения к MS RDS.

4.3 . Режим техобслуживания поставщика ресурсов

Режим техобслуживания предназначен для проведения плановых регламентных или аварийных работ поставщика ресурсов. В режиме техобслуживания Termidesk не использует поставщика ресурсов для размещения фондов BPM.

Для перевода поставщика ресурсов в режим техобслуживания следует перейти «Компоненты - Поставщики ресурсов» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 5). Затем подтвердить включение режима (см. Рисунок 6).

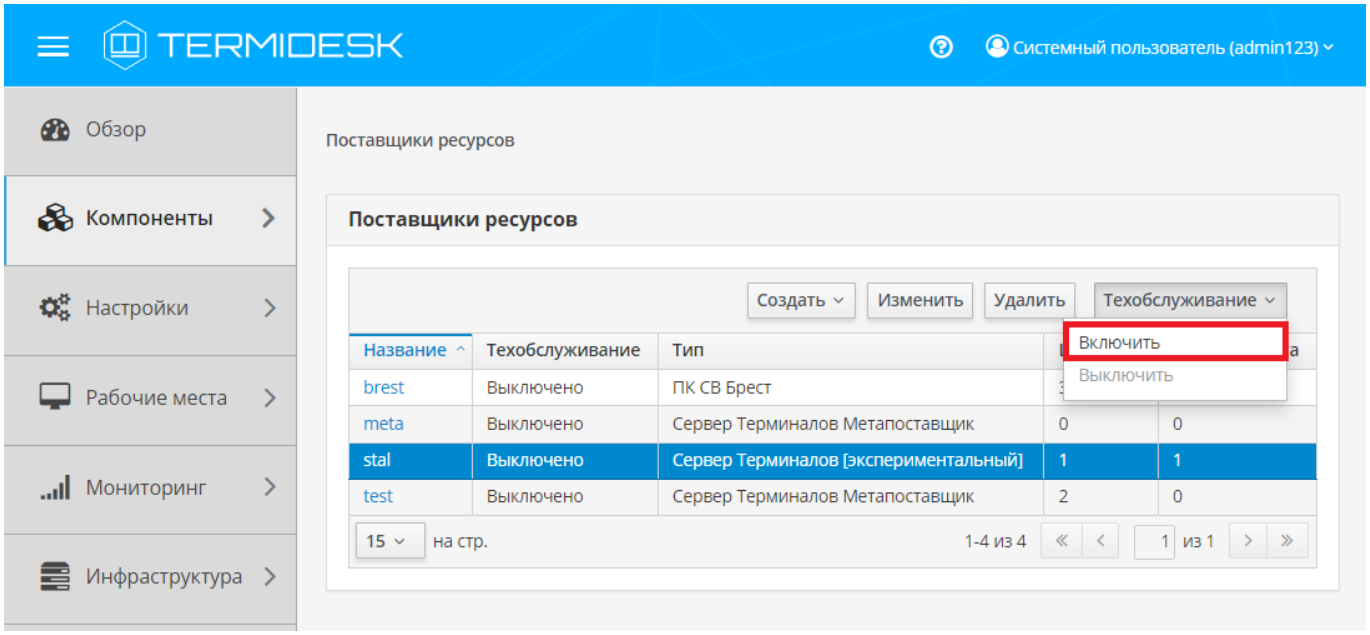

Рисунок 5 – Включение режима техобслуживания поставщика ресурсов

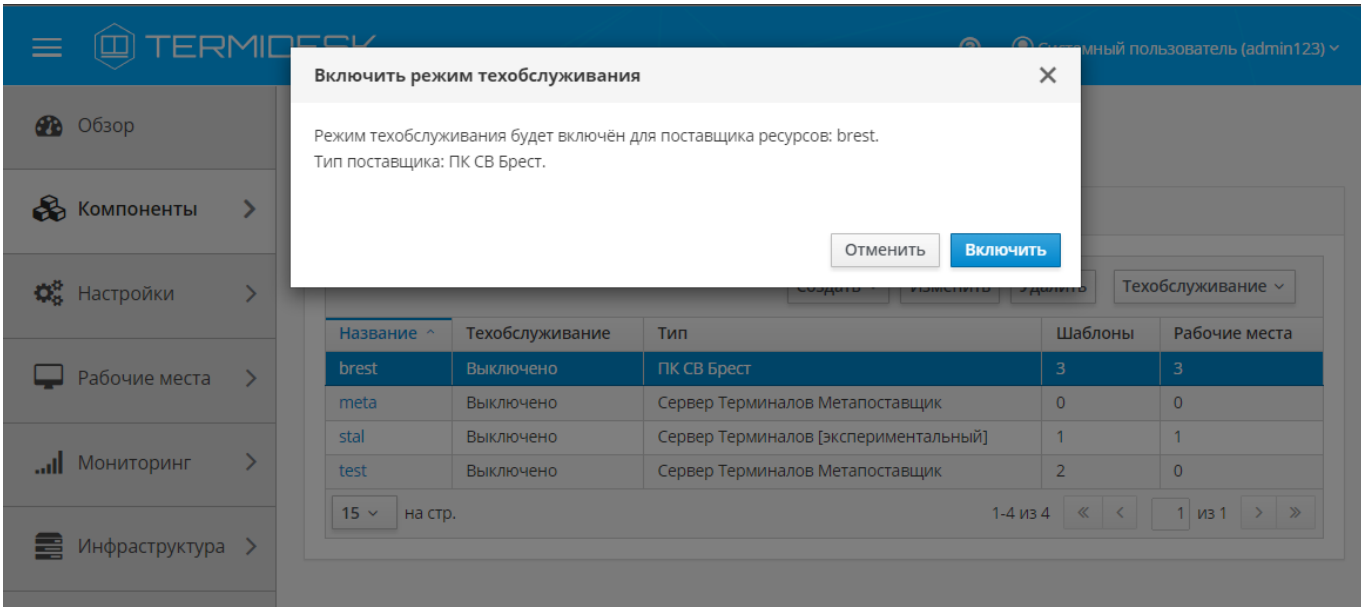

Рисунок 6 – Подтверждение включения режима техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Техобслуживание» списка поставщиков ресурсов.

Для отключения режима техобслуживания нужно выбрать поставщика ресурсов, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить».

По завершении техобслуживания поставщик ресурсов может быть снова использован Termidesk для размещения фондов ВРМ.

5 . АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

5.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

В Termidesk поддерживаются следующие домены аутентификации:

- FreeIPA;
- SAML;
- IP-аутентификация;
- MS AD или LDAP;
- RADIUS;
- OIDC.

Поддержка некоторых доменов аутентификации может добавляться в режиме экспериментальных функций.

Для добавления в Termidesk домена аутентификации в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка нужный домен аутентификации.
Каждый домен аутентификации описывается перечнем параметров, требуемых для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

> ⚠ Следует предусмотреть, что в целях безопасности учетная запись для биндинга (подключения) к домену не должна иметь прав на удаление или изменение объекта типа «пользователь».

Созданный домен аутентификации можно отредактировать. Для этого в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем пометить необходимый домен аутентификации и нажать экранную кнопку [Изменить] (см. Рисунок 7).

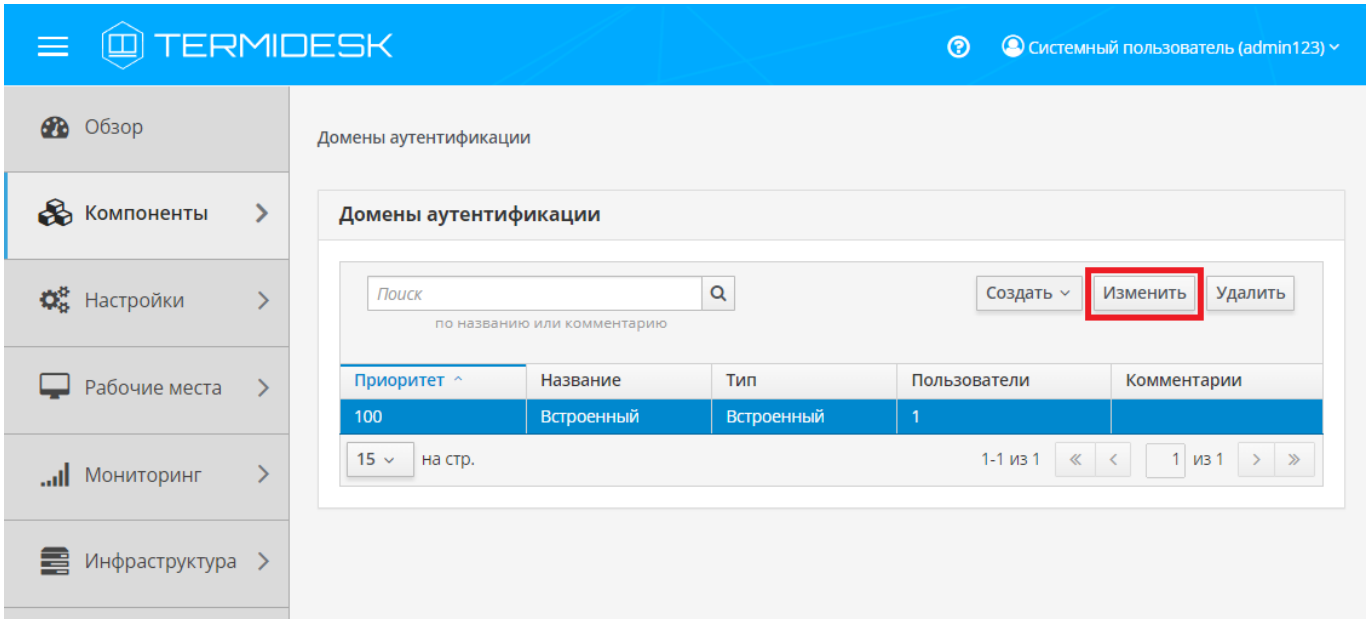

Рисунок 7 – Окно выбора домена аутентификации для редактирования

Созданный домен аутентификации можно при необходимости удалить. Для этого в графическом интерфейсе управления следует перейти «Компоненты - Домены аутентификации», затем пометить нужный домен аутентификации и нажать экранную кнопку **[Удалить]**.

5.2 . Добавление аутентификации через FreeIPA

5.2.1 . Получение и добавление файла keytab

`Keytab`-файлы используются для аутентификации в системах, использующих `Kerberos`. Для получения `keytab`-файла на контроллере домена и добавления его на сервер, где установлен Termidesk, необходимо выполнить ряд действий.

Действия на контроллере домена (например, FreeIPA):

- получить доступ к контроллеру домена в режиме интерфейса командной строки;
- получить `kerberos-ticket` для пользователя с полномочиями администратора домена при помощи команды:

```
:~$ sudo kinit admin
```

- выполнить команду для добавления узла:

```
:~$ sudo ipa host-add --force --ip-address=192.0.2.30 disp.termidesk.local
```

где:

`--force` - флаг для принудительного создания;

`--ip-address` - задание IP-адреса целевого узла;

`192.0.2.30` - IP-адрес сервера, где установлен Termidesk,

`disp.termidesk.local` - мнимый FQDN узла в текущем домене (в примере `termidesk.local`);

> ⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре предприятия.
> Мнимый FQDN означает, что он не обязательно должен быть привязан к действительно существующему узлу.

- выполнить команду добавления службы для нового сервисного аккаунта:

```
:~$ sudo ipa service-add HTTP/disp.termidesk.local
```

- создать файл `termidesk.keytab` для сервисного аккаунта:

```
:~$ sudo ipa-getkeytab -s freeipa.termidesk.local -p HTTP/disp.termidesk.local -k /home/
user/termidesk.keytab
```

где:

`-s freeipa.termidesk.local` - задание FQDN сервера-контроллера домена FreeIPA;

`-p HTTP/disp.termidesk.local` - указание ранее созданного субъекта-службы;

`-k /home/user/termidesk.keytab` - сохранение в файл `termidesk.keytab`;

> ⚠ Неважно, для какого узла создан `keytab`, необходимо само его наличие.

- передать полученный файл `termidesk.keytab` на узел Termidesk, например, воспользовавшись командой:

```
:~$ sudo scp termidesk.keytab localuseruser@192.0.2.30:termidesk.keytab
```

где:

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес сервера, где установлен Termidesk.

После передачи файла на узле Termidesk необходимо выполнить следующее:

- переместить файл `termidesk.keytab` в каталог `/etc/opt/termidesk-vdi`:

```
:~$ sudo mv /home/user/termidesk.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

```
:~$ sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/termidesk.keytab
```

- перезапустить службу `termidesk-vdi`:

```
:~$ sudo systemctl restart termidesk-vdi
```

5.2.2 . Перечень параметров для добавления аутентификации через FreeIPA

Для добавления администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «FreeIPA».

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 5).

Таблица 5 – Данные для добавления аутентификации через FreeIPA

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией. Неважно, для какого узла создан `keytab`, необходимо само его наличие
«Сервер FreeIPA»	FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях
«Проверка SSL»	Проверка использования SSL
«Группа администраторов»	Название группы, членам которой предоставляются права администрирования Termidesk

ⓘ При добавлении второго домена аутентификации FreeIPA (или доменов, основанных на FreeIPA, например, программного комплекса «ALD PRO») необходимо создать новый файл `keytab` и задать ему имя, отличное от уже существующего.
Добавление второго домена аутентификации не отличается от добавления первого.

ⓘ Termidesk не реализует непосредственно механизм аутентификации.

5.3 . Добавление аутентификации через ALD

⚠ Добавление программного комплекса «ALD PRO» в качестве домена аутентификации производится через добавление FreeIPA.

Для добавления аутентификации через Astra Linux Directory (далее - ALD) администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Astra Linux Directory».

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (see page 0).

Таблица 6 – Данные для добавления аутентификации через ALD

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла keytab**). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией. Неважно, для какого узла создан `keytab`, необходимо само его наличие
«Группа администраторов»	Название группы, членам которой предоставляются права администрирования Termidesk
«Сервер LDAP (ALD)»	Доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях
«Таймаут подключения»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Base DN»	Корень поиска в домене аутентификации

5.4 . Добавление аутентификации через SAML

Провайдер SAML - это единая точка входа пользователей в распределенной системе, позволяющей аутентифицироваться в разных и несвязных между собой частях системы посредством веб-браузера. Независимо от того, какой используется тип биндинга (binding), всегда происходит перенаправление на страницу аутентификации «Провайдер SAML».

Для добавления аутентификации через SAML администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «SAML».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 7).

Таблица 7 – Данные для добавления аутентификации через SAML

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Приоритет использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«ID клиента»	Уникальный идентификатор клиента на сервисе аутентификации SAML
«URL метаданных»	URL для подключения к сервису аутентификации SAML
«Проверка SSL»	Строгая проверка SSL-сертификатов
«Тип биндинга»	Способ отправки ответа сервисом SAML на запрос аутентификации. Поддерживаются следующие типы: `HTTP-Redirect`, `HTTP-POST`
«Response Binding Type»	Выбор типа биндинга для обратного перенаправления в SAML-запросе. Поддерживаются следующие типы: `HTTP-Redirect`, `HTTP-POST`
«Приватный ключ»	Набор символов приватного ключа для подписи SAML-запросов
«Формат Name ID»	Формат сопоставления идентификаторов имен SAML у поставщиков удостоверений и поставщиков услуг
«Group Attr Name»	Тип атрибута пользователя (обычно в этом поле указывается значение `Group`)
«Таймаут»	Время ожидания ответа от SAML, в секундах

Для работы с сертификатами при получении метаданных от домена аутентификации SAML необходимо установить корневой сертификат центра сертификации и настроить Termidesk на работу с сертификатами (см. подраздел **Установка корневого сертификата центра сертификации**).

5.5 . Добавление аутентификации OIDC

OpenID Connect (OIDC) - это механизм, позволяющий приложению связаться со службой идентификации (Identity provider, IdP), получить данные о пользователе и вернуть их обратно в приложение. Таким образом OIDC обеспечивает аутентификацию администраторов и пользователей без необходимости ввода логина и пароля.
Служба идентификации IdP (например, keycloak) должна быть предварительно настроена в инфраструктуре предприятия для возможности использования OIDC как домена аутентификации.

Для добавления аутентификации OIDC администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «OIDC аутентификация».
Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 8).

Таблица 8 – Данные для добавления аутентификации через OIDC

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Приоритет использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«ID клиента»	Уникальный идентификатор приложения, полученный от службы идентификации IdP. Пример: `openid-test-cl`
«Client secret»	Ключ приложения, полученный от службы идентификации IdP
«Authorization endpoint»	URL-адрес авторизации службы идентификации IdP. Пример: `http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth`
«Token endpoint»	URL-адрес получения токена службы идентификации IdP. Пример: `http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token`
«Userinfo endpoint»	URL-адрес получения информации о пользователе от службы идентификации IdP. Пример: `http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/userinfo`
«JWKS URI»	URL-адерс получения сертификатов службы идентификации IdP. Пример: `http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/certs`

5.6 . Добавление IP-аутентификации

Домен «IP аутентификация» позволяет определять назначение прав на основе сетевых адресов. Для добавления IP-аутентификации администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «IP аутентификация».

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 9).

Таблица 9 – Данные для добавления IP-аутентификации

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Разрешить проксирование»	Разрешить субъектам доставку BPM, находящихся за прокси-сервером

5.7 . Добавление аутентификации через MS AD (LDAP)

Для добавления аутентификации LDAP администратору Termidesk следует перейти «Компоненты - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «MS Active Directory (LDAP)».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 10).

Таблица 10 – Данные для добавления аутентификации через MS AD (LDAP)

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Сервер LDAP»	IP-адрес или доменное имя сервера, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба домена аутентификации

Параметр	Описание
«Использовать SSL»	Использовать защищенное соединение при взаимодействии с доменом аутентификации
«Учетная запись»	Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к LDAP. Пример: `CN=admin,OU=user,DC=test,DC=desk`
«Пароль учетной записи»	Набор символов, подтверждающий полномочия объекта для подключения к серверу LDAP
«Таймаут»	Время ожидания (в секундах) ответа ресурса, являющегося источником сведений о субъектах и их полномочиях
«Корень поиска»	Корень поиска в домене аутентификации в формате DN. Пример: `DC=test,DC=desk`
«Имя класса пользователя»	Атрибут класса пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «Person»)
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «SamAccountName»)
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми (для корректного заполнения данного поля необходимо указать значение «name»)
«Имя атрибута группы»	Атрибут принадлежности к группе в домене аутентификации (для корректного заполнения данного поля необходимо указать значение «group»)
«Атрибут имени группы»	Идентификатор группы, к которой относится субъект в домене аутентификации. Если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей», то необходимо указать значение «distinguishedname». Если указанные параметры отключены, то можно использовать значение «cn». При использовании значения «distinguishedname» при добавлении группы в домен аутентификации по пути «Компоненты - Домены аутентификации - Наименование домена - Группы» нужно задавать длинные имена групп, например: `CN=Корневая группа,CN=Users,DC=test,DC=desk`. При использовании значения «cn» нужно использовать короткие имена групп. Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена
«Атрибут членства в группе»	Идентификатор группы для назначения полномочий субъекту (для корректного заполнения данного поля необходимо указать значение «member»)
«Атрибут групп для LDAP-запросов»	Атрибут, определяющий группы пользователя при запросах к службе каталогов. Возможные значения: «objectClass», «objectCategory»
«Использовать рекурсивный поиск групп»	При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно. Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать

Параметр	Описание
«Использовать обратный порядок проверки членства пользователей»	Проверка соответствия членства пользователя в группах домена аутентификации членству в группах Termidesk. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы». При большом количестве групп непосредственно в домене аутентификации MS AD (LDAP) нужно включить этот параметр. В этом случае сначала будет проверяться вхождение пользователя в группы в Termidesk (в том числе рекурсивно), затем будет происходить проверка найденных групп на сервере MS AD (LDAP). При выключении этого параметра применяется настройка выбора Атрибут групп для LDAP-запросов: «objectClass» или «objectCategory». При включении этого параметра всегда применяется настройка выбора Атрибут групп для LDAP-запросов: «objectClass».

5.8 . Добавление домена аутентификации RADIUS

Для добавления домена аутентификации RADIUS необходимо включить экспериментальный параметр `experimental.radiusauth.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk**.

После включения экспериментального параметра администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Radius».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 11).

Таблица 11 – Данные для добавления аутентификации Radius

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Radius сервер»	IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях (сервер RADIUS)
«Аутентификационный порт»	Порт для обработки запросов на аутентификацию
«Секрет»	Набор символов (пароль), подтверждающий подключение к серверу RADIUS
«Таймаут»	Максимальное время ожидания (в секундах) для установки соединения

Валидация заданных параметров экранной кнопкой **[Тест]** проверяет корректность заданного имени сервера (возможность получить IP-адрес, используя DNS), доступность сервера (корректный порт, работоспособность сервера RADIUS).

После добавления домена аутентификации RADIUS необходимо перейти в созданный объект и указать актуальный список групп, пользователи которых могут производить вход в Termidesk.
При дальнейшей эксплуатации сервер Termidesk, обрабатывая запрос на аутентификацию, получает актуальный список групп пользователя и сравнивает со своей конфигурацией. Если ни одного совпадения не обнаружено, то пользователю будет отказано в доступе.

⚠ Конфигурация сервера RADIUS должна учитывать передачу списка групп пользователя в атрибуте с ключом 25 (Class) в ответе со статусом авторизации.

Для корректного получения списка групп на Termidesk сервер RADIUS может быть настроен следующим образом:

⚠ Пример настройки приведен для сервера freeRADIUS.

- файл `/etc/freeradius/3.0/mods-enabled/ldap` должен содержать конструкцию вида:

```
ldap {
...
  update {
      ...
      reply:memberOf                  += 'memberOf'
  }
...
}
```

- в файл `/etc/freeradius/3.0/dictionary` необходимо добавить строку:

```
ATTRIBUTE       memberOf                3001    string
```

- в файле `/etc/freeradius/3.0/sites-enabled/default` необходимо найти секцию `post-auth` и добавить регулярное выражение, фильтрующее название группы из получаемых от сервера атрибутов:

```
foreach &reply:memberOf {
       if ("%{Foreach-Variable-0}" =~ /CN=([^,=]+)/) {
             update reply { Class += "%{1}" }
           }
```

- в файле `/etc/freeradius/3.0/mods-enabled/exec` указать для параметра `wait` значение `yes`:

```
wait = yes
```

5.9 . Добавление аутентификации через внутреннюю БД

Для добавления аутентификации пользователей через внутреннюю БД необходимо установить в Termidesk плагин расширения `termidesk_internaldbauth` в соответствии с подразделом **Установка плагинов расширений**.

После установки плагина расширения администратору Termidesk следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Внутренняя БД, эксперим.».
Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 12).

Таблица 12 – Данные для добавления аутентификации через внутреннюю БД

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk
«Разные пользователи для хостов»	Для пользователя, выполняющего вход с разных хостов, будут созданы разные учетные записи
«Обратный просмотр DNS»	Для подключающихся хостов будет производиться обратный просмотр DNS для определения имени хоста по его IP-адресу
«Разрешить проксирование»	Запросы через прокси-сервер будут осуществляться от пересылаемого IP-источника

5.10 . Действия над группами в домене аутентификации

Группы – перечень объектов домена аутентификации, определяющих разрешения пользователей на доступ к фондам BPM. Перечень групп, доступных для добавления в Termidesk, запрашивается у домена аутентификации.

Доступны следующие действия над группами домена аутентификации:

- создание - добавление существующей в службе каталогов группы в Termidesk;
- редактирование;
- удаление;
- просмотр сведений таблицы «Группы».

ⓘ Редактирование и удаление групп в домене аутентификации в веб-интерфейсеTermidesk не приводит к каким-либо изменениям объекта в службе каталогов.

Для добавления группы следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Группы» выделить строку с именем пользователя и нажать экранную кнопку **[Создать]**. Для добавления будут доступны два типа групп:

- «Группа» (см. Рисунок 8) - стандартная группа, которая создана в службе каталогов и будет добавлена в Termidesk;
- «Метагруппа» (см. Рисунок 9) - группа, которая объединяет несколько стандартных групп в Termidesk.

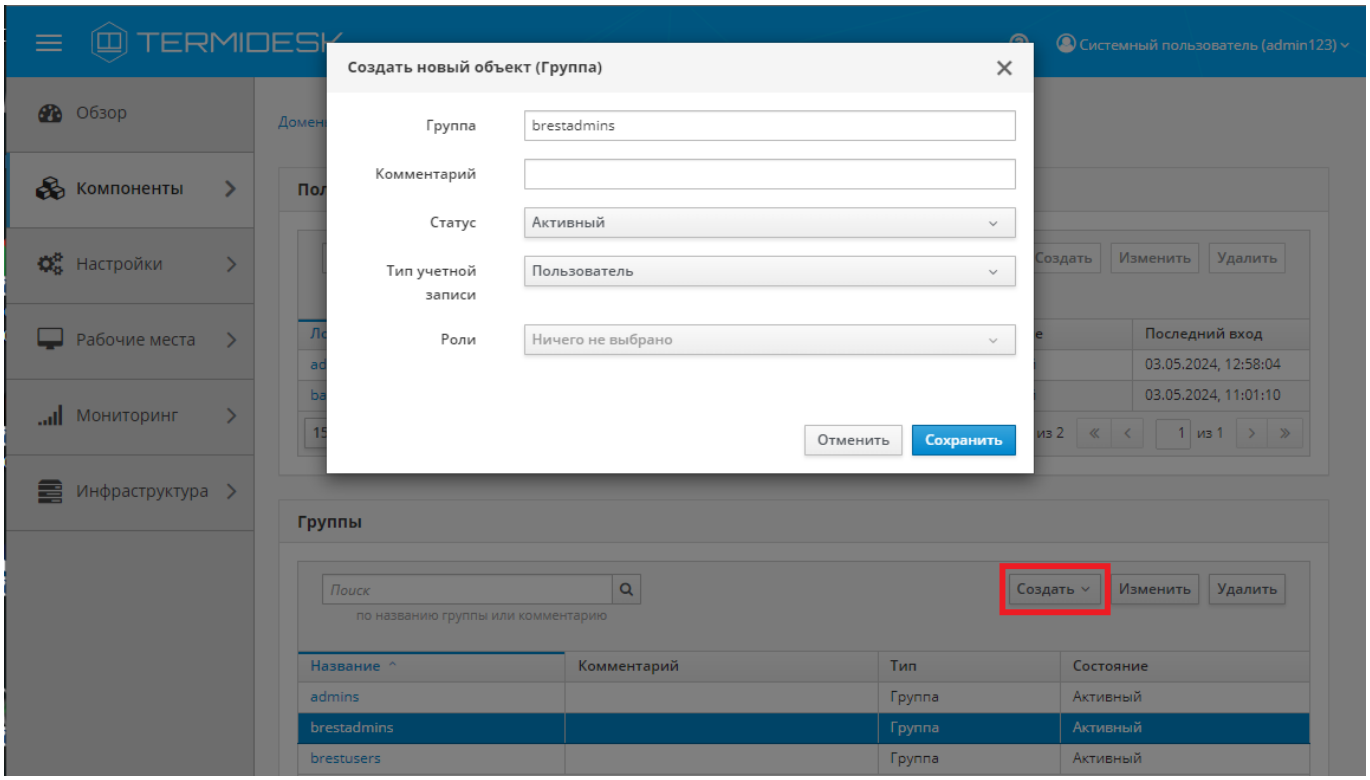

Рисунок 8 – Окно добавления группы домена аутентификации

Для добавления группы администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 13).

Таблица 13 – Данные для добавления группы домена аутентификации

Параметр	Описание
«Группа»	Наименование группы, полученное от домена аутентификации. Для выбора группы из списка доступных необходимо начать ввод ее наименования
«Комментарий»	Информационное сообщение, используемое для описания группы

Параметр	Описание
«Статус»	Характеристика состояния субъектов группы при доступе к фонду BPM. Доступные значения: ▪ «Активный» - субъекты группы могут аутентифицироваться в Termidesk; ▪ «Неактивный» - субъекты группы не могут аутентифицироваться в Termidesk; ▪ «Временно заблокирован» - субъекты группы не могут аутентифицироваться в Termidesk. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Настройки - Системные параметры - Безопасность» (см. подраздел **Параметры безопасности Termidesk**)
«Тип учетной записи»	Служебные функции субъектов группы при доступе к Termidesk. Доступные значения параметра: ▪ «Пользователь» - субъекты группы не будут иметь доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым; ▪ «Персонал» - субъекты группы будут иметь доступ к странице «Обзор» и будут обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Настройки - Управление ролями» (см. подраздел **Назначение служебных функций администраторам**); ▪ «Администратор» - субъекты группы будут иметь полный доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым
«Роли»	Назначение служебных функций пользователям группы. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Настройки - Управление ролями»

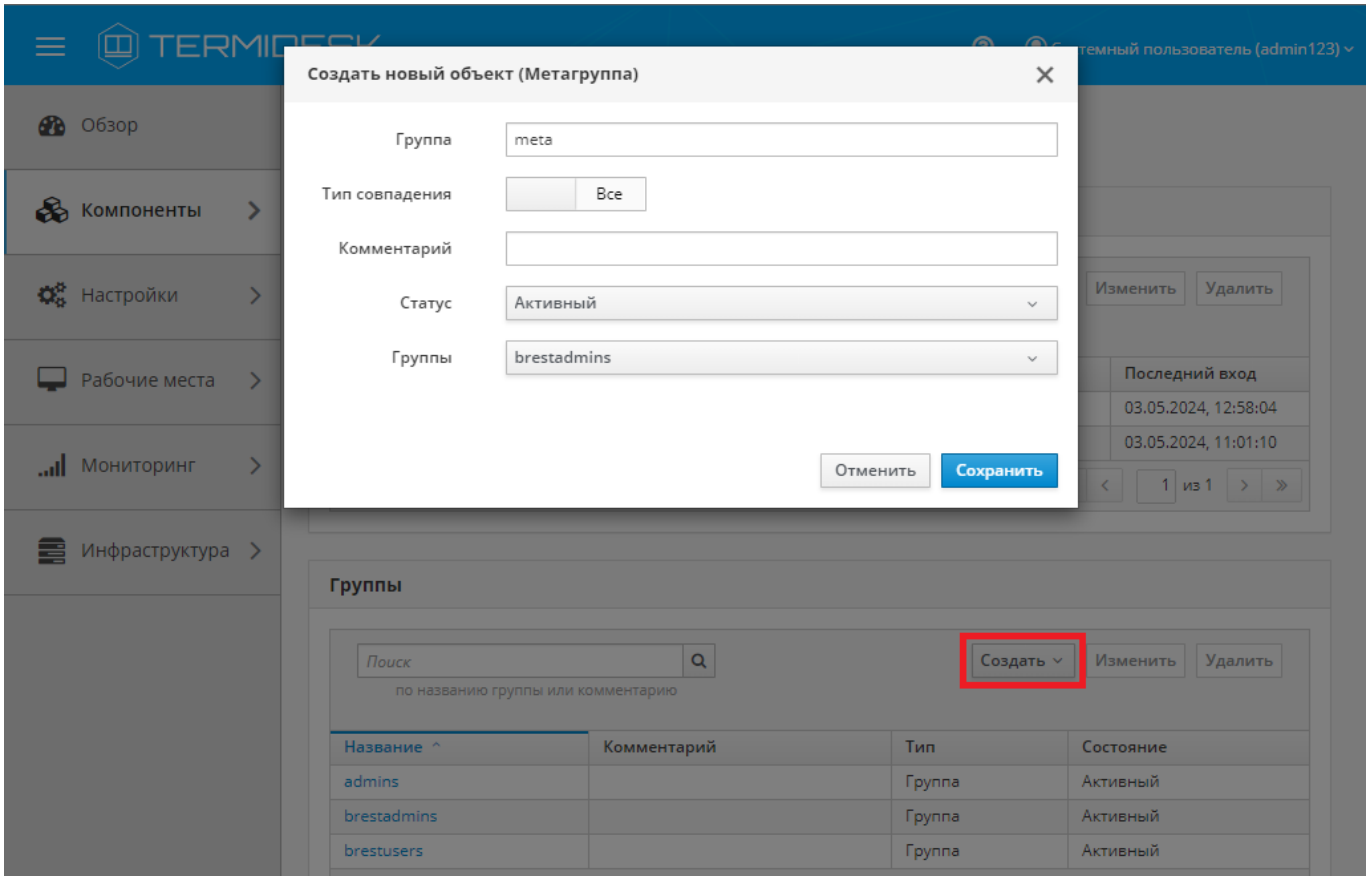

Рисунок 9 – Окно добавления метагруппы домена аутентификации

Для добавления метагруппы администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 14).

Таблица 14 – Данные для добавления метагруппы домена аутентификации

Параметр	Описание
«Группа»	Наименование группы
«Тип совпадения»	Выбор способа определения принадлежности группы к метагруппе. Доступные значения: ▪ «Любой» - любая из групп, перечисленных в параметре «Группы»; ▪ «Все» (значение по умолчанию) - все группы, перечисленные в параметре «Группы»
«Комментарий»	Информационное сообщение, используемое для описания метагруппы
«Статус»	Характеристика состояния субъектов метагруппы при доступе к фонду BPM. Доступные значения: ▪ «Активный» - субъекты метагруппы могут аутентифицироваться в Termidesk; ▪ «Неактивный» - субъекты метагруппы не могут аутентифицироваться в Termidesk
«Группы»	Наименования групп, к которым должна примениться метагруппа

Для редактирования группы следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Группы» выделить строку с именем пользователя и нажать экранную кнопку **[Изменить]**. В режиме редактирования невозможно изменить идентификатор группы домена аутентификации, поскольку он получен автоматически от службы каталогов.
Для удаления группы используется экранная кнопка **[Удалить]**.

5.11 . Действия над пользователями в домене аутентификации

Пользователи – перечень объектов, имеющих в рамках домена аутентификации служебные функции на использование фондов BPM.

После входа пользователя в «Портал пользователя» Termidesk доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование;
- удаление;
- просмотр сведений.

> Редактирование и удаление пользователя в домене аутентификации в веб-интерфейсе Termidesk не приводит к каким-либо изменениям объекта в службе каталогов.
> Termidesk хранит информацию о назначении прав пользователя в БД, поэтому в случае, если пользователь должен быть исключен из группы администрирования Termidesk, то необходимо удалить пользователя из группы непосредственно в доменной службе каталогов и на стороне Termidesk одновременно.

Для редактирования информации о пользователе следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации.
В открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя и нажать экранную кнопку [Изменить] (см. Рисунок 10).

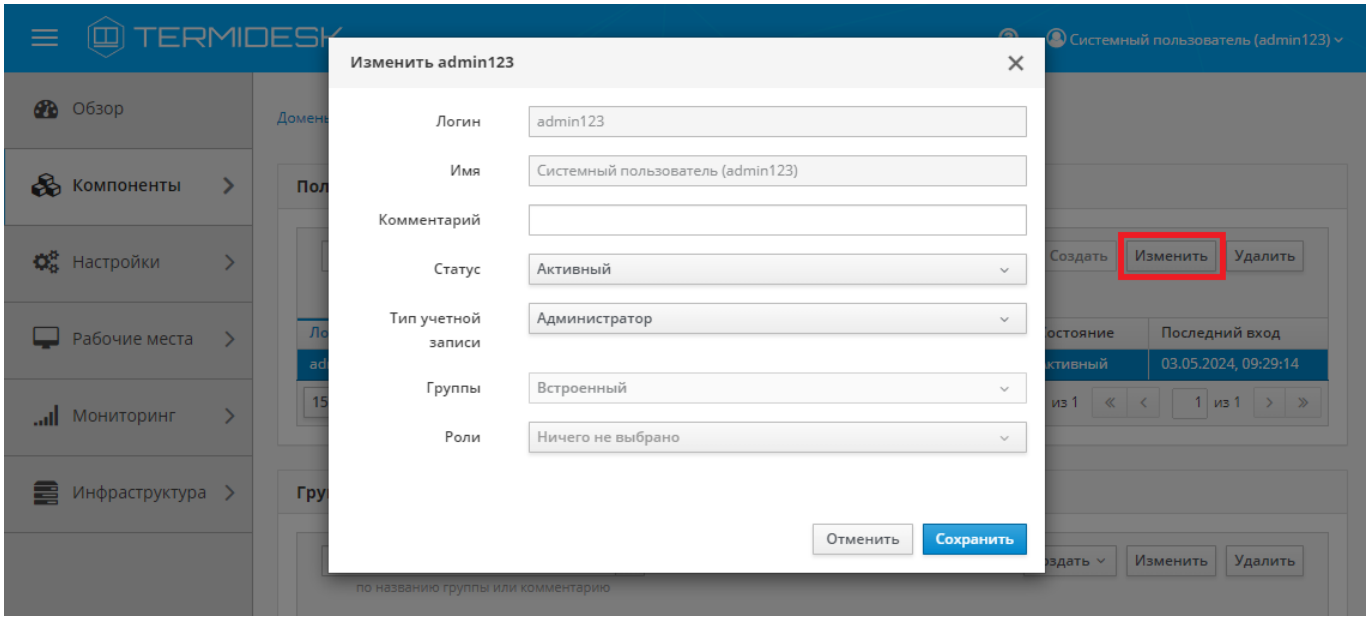

Рисунок 10 – Окно редактирования пользователя домена аутентификации

Для редактирования пользователя администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 15).

Таблица 15 – Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Логин»	Идентификатор субъекта в домене аутентификации
«Имя»	Отображаемое имя субъекта в Termidesk
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Статус»	Характеристика состояния субъекта при доступе к фонду ВРМ. Доступные значения: ▪ «Активный» - субъект может аутентифицироваться в Termidesk; ▪ «Неактивный» - субъект не может аутентифицироваться в Termidesk; ▪ «Временно заблокирован» - субъект не может аутентифицироваться в Termidesk. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Настройки - Системные параметры - Безопасность» (см. подраздел **Параметры безопасности Termidesk**)

Параметр	Описание
«Тип учетной записи»	Служебные функции субъекта при доступе к Termidesk. Значение наследуется от группы, в которую входит пользователь. При этом по умолчанию тип учетной записи устанавливается в значение с более высоким уровнем прав. Пример: если пользователь одновременно состоит в группе с типом учетной записи «Администратор» и группе с типом «Пользователь», то по умолчанию для пользователя будет установлен тип учетной записи «Администратор». Доступные значения параметра: ▪ «Пользователь» - субъект не будет иметь доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет пустым; ▪ «Персонал» - субъект будет иметь доступ к странице «Обзор» и будет обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Настройки - Управление ролями» (см. подраздел **Назначение служебных функций администраторам**); ▪ «Администратор» - субъект будет иметь полный доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет пустым
«Группы»	Наименования групп, используемых для определения разрешений по доступу к фондам BPM. Список групп пользователя будет получен автоматически от домена аутентификации
«Роли»	Назначение служебной функции указанному пользователю. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Настройки - Управление ролями»

Для удаления пользователя из домена аутентификации необходимо перейти в «Компоненты - Домены аутентификации», в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя и нажать экранную кнопку **[Удалить]**.

5.12 . Управление аутентификацией на основе адресов сети

Аутентификация на основе адресов сети используется для предоставления доступа к BPM, базируясь на IP-адресе источника, с которого производится запрос к фонду BPM.

Для добавления диапазона сети администратору Termidesk следует перейти «Компоненты - Сети», нажать экранную кнопку **[Создать]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 16).

Таблица 16 – Данные для добавления аутентификации на основе адресов сети

Параметр	Описание
«Название»	Текстовое наименование источника сведений о субъектах и их полномочиях
«Диапазон»	Диапазон сетевых адресов, которые будут использоваться для идентификации субъекта

Созданные таким образом диапазоны можно отредактировать, для этого нужно пометить желаемый диапазон адресов, а затем нажать экранную кнопку **[Изменить]**.

Для удаления созданного диапазона необходимо пометить желаемый диапазон адресов, а затем нажать экранную кнопку **[Удалить]**.

⚠ Диапазон сетевых адресов может быть удален только в том случае, если он не используется фондом BPM.

6 . ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА

6.1 . Общие сведения о BPM

BPM - это гостевая ОС, доступ к которой реализуется с помощью протокола удаленного доступа.
Termidesk выполняет подготовку BPM на основе заданных шаблонов BPM. Каждый поставщик ресурсов поддерживает свой набор типов шаблонов BPM.
Шаблоны серверов терминалов предполагают создание BPM на основе терминального доступа или доступа к опубликованным на сервере терминалов приложениям.
Для добавления шаблона BPM следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.
Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, а затем из выпадающего списка выбрать поддерживаемый в Termidesk способ формирования шаблона BPM.
Созданные шаблоны BPM можно редактировать, для этого надо выбрать шаблон, а затем нажать экранную кнопку **[Изменить]**.
Созданные шаблоны можно удалить, для этого надо выбрать шаблон, а затем нажать экранную кнопку **[Удалить]**.

⚠ Шаблон может быть удален только в том случае, если он не используется фондом BPM.

6.2 . Отображение списка BPM из всех фондов

6.2.1 . Отображение списка BPM

Для более эффективного администрирования Termidesk предусмотрено отображение BPM из всех фондов, в том числе назначенные BPM, а также созданные и размещенные в кеше.
Для получения списка необходимо перейти «Рабочие места - Индивидуальные рабочие места» (см. Рисунок 11) или перейти по ссылке «Рабочие места» из функции «Обзор» (см. Рисунок 12). По умолчанию записи в представленном списке (см. Рисунок 13) будут упорядочены согласно столбцу «Дата создания» по убыванию. Подробная информация об управлении состоянием ВМ и ее индикации содержится в подразделе **Управление ВМ в назначенном фонде BPM**, информация по назначению владельца BPM приведена в подразделе **Назначение владельца BPM**.

⚠ Отображение списка будет доступно администратору, если у него есть разрешение «Просмотр фондов рабочих мест».

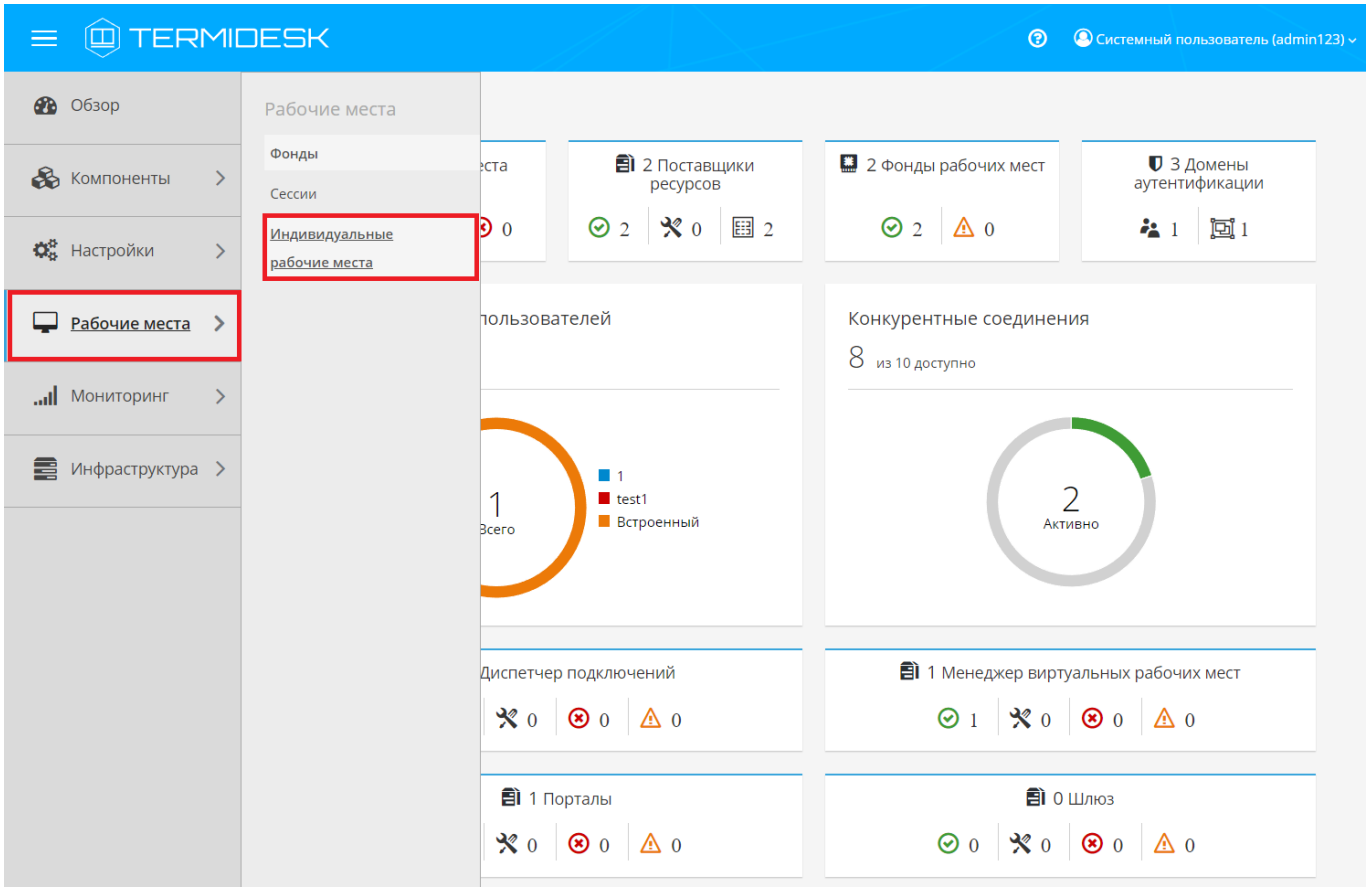

Рисунок 11 – Переход к списку BPM через «Рабочие места - Индивидуальные рабочие места»

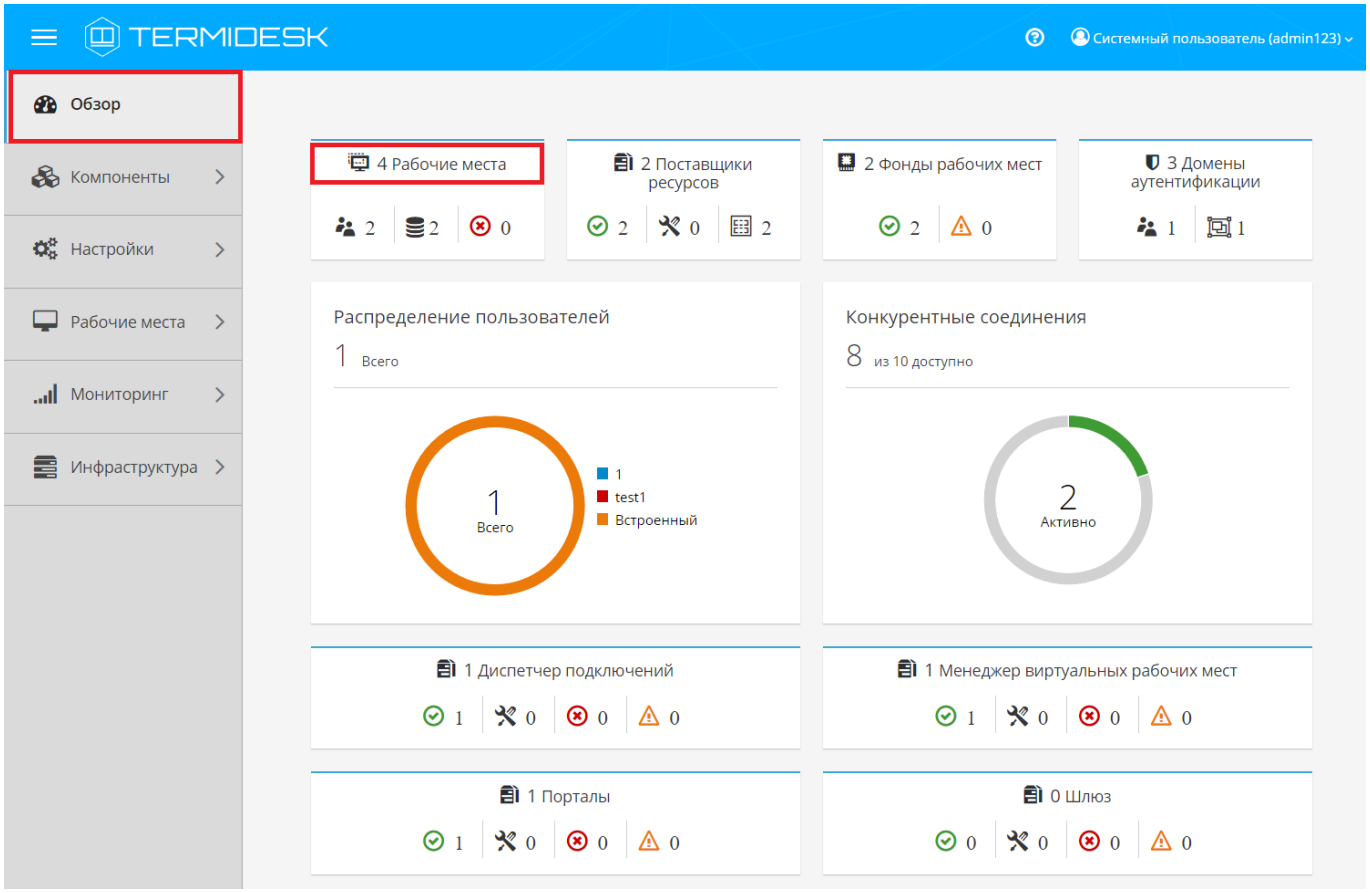

Рисунок 12 – Переход к списку BPM через функцию «Обзор»

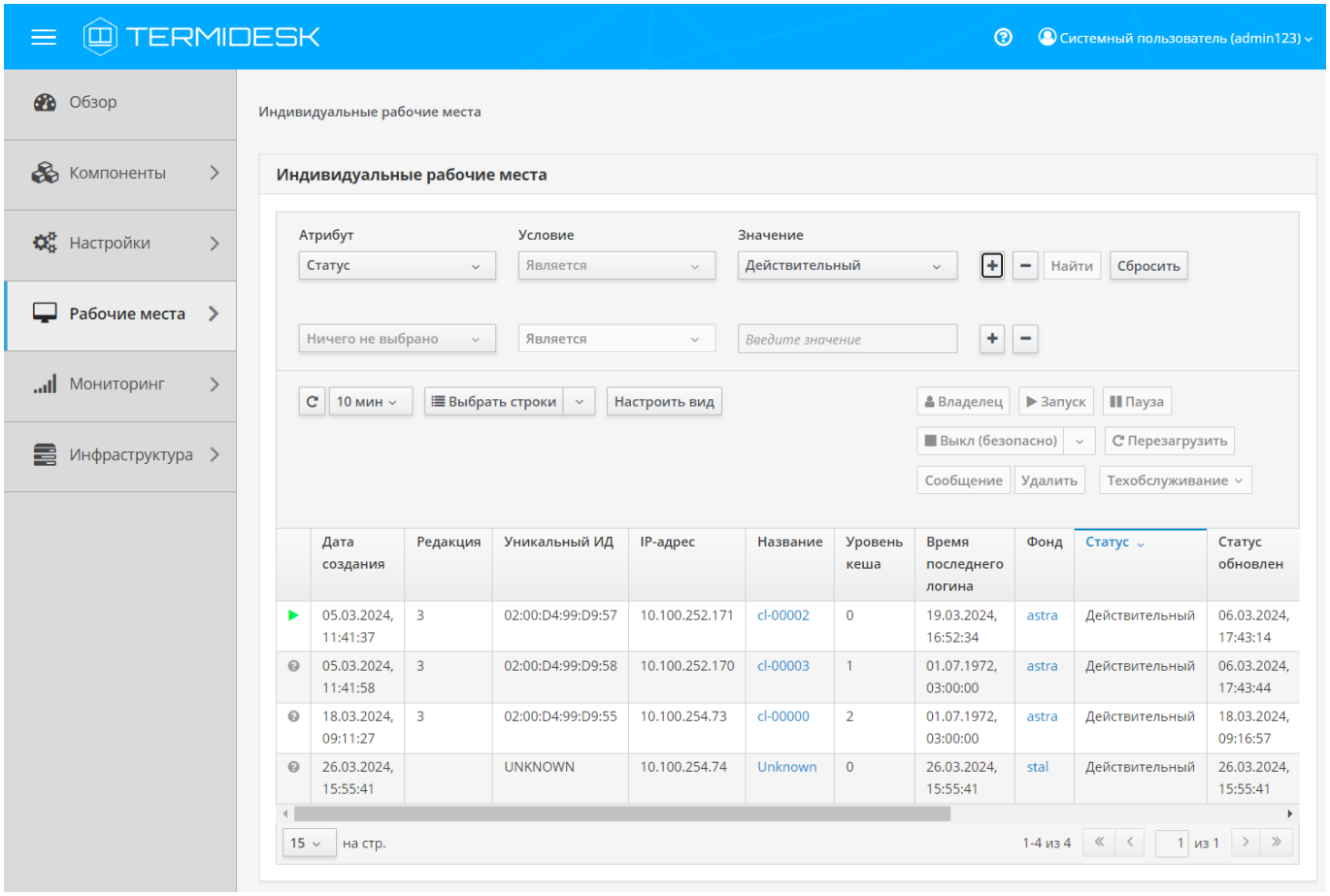

Рисунок 13 – Пример отображения списка BPM

Записи в списке поддерживают функцию множественного выбора и выполнения операций над несколькими объектами одновременно. Выполнить операцию над несколькими объектами можно только тогда, когда она допустима для всех выбранных объектов.

Существуют варианты выбора записей таблицы, доступные через выпадающий список экранной кнопки **[Выбрать строки]**, а именно:

- выделить все строки таблицы, активировав «Выбрать все»;
- выделить все строки на текущей странице таблицы, активировав «Выбрать все на стр.»;
- сбросить выделение строк, активировав «Сбросить».

Для множественного выделения записей можно зажать и удерживать клавиши **<CTRL>** или **< SHIFT>**. Для сброса множественного выделения нужно активировать функцию «Сбросить» экранной кнопки **[Выбрать строки]** или нажать на произвольную строку таблицы.

В случае изменения ширины столбцов или их порядка произойдет сброс ранее выполненного выделения.

Для обновления значений таблицы используется графический элемент  . Для задания периода обновления или его отключения следует использовать выпадающий список (см. Рисунок 14) со значениями интервала в минутах, расположенный рядом с указанным элементом.

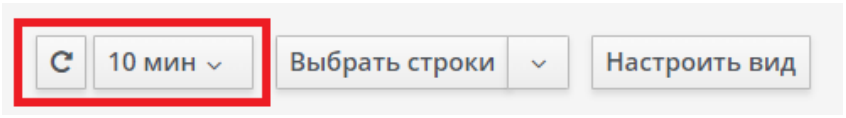

Рисунок 14 – Обновление значений таблицы

Внешний вид таблицы списка BPM можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов (см. Рисунок 15), которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нужно нажать экранную кнопку **[Сохранить]**. При попытке убрать выбор со всех пунктов и нажатия экранной кнопки **[Сохранить]** отобразится сообщение «Нельзя скрыть все колонки таблицы» и изменение не применится. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

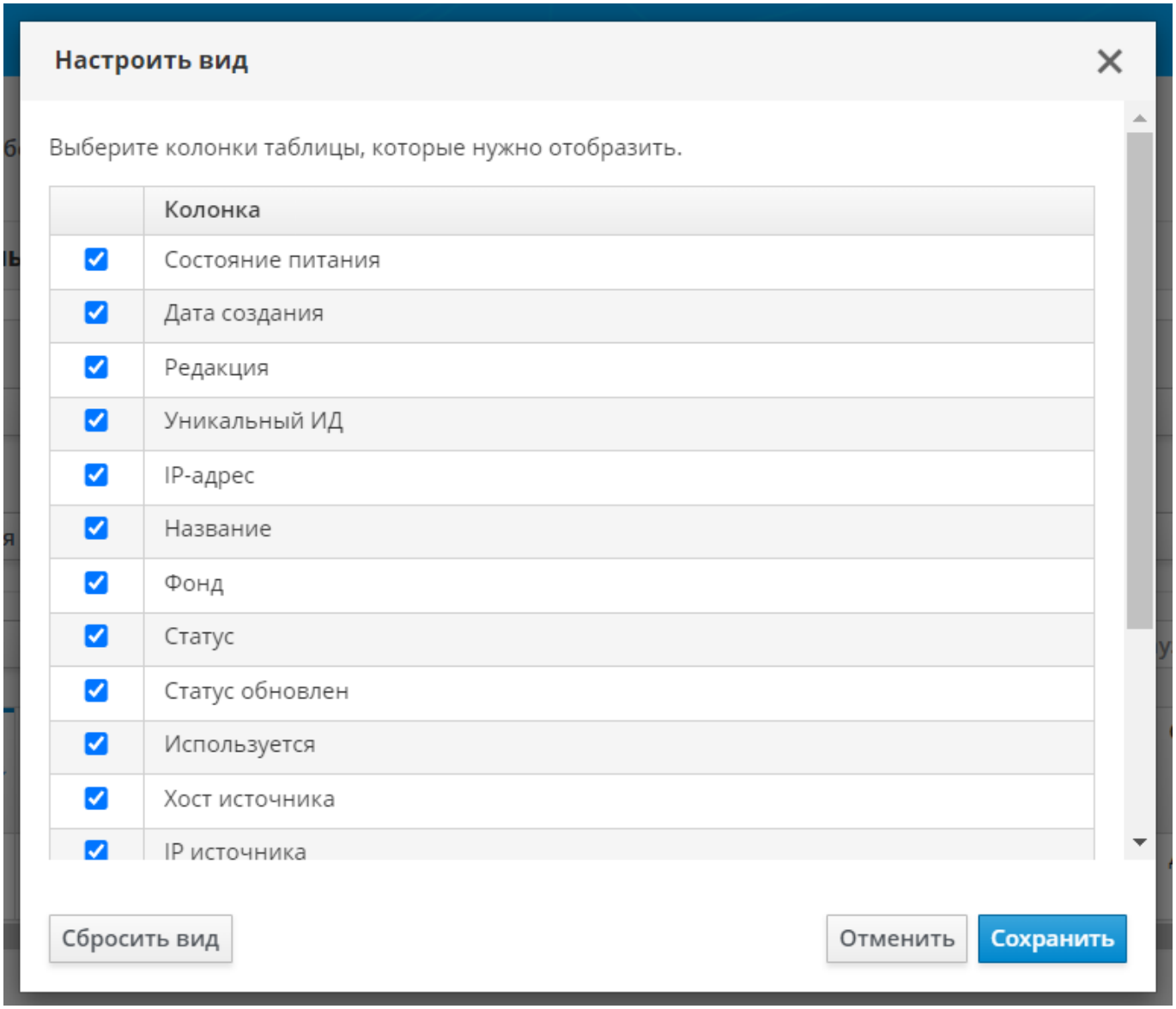

Рисунок 15 – Выбор столбцов для отображения

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская кнопку мыши, перенести его в нужное расположение (см. Рисунок 16). Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;

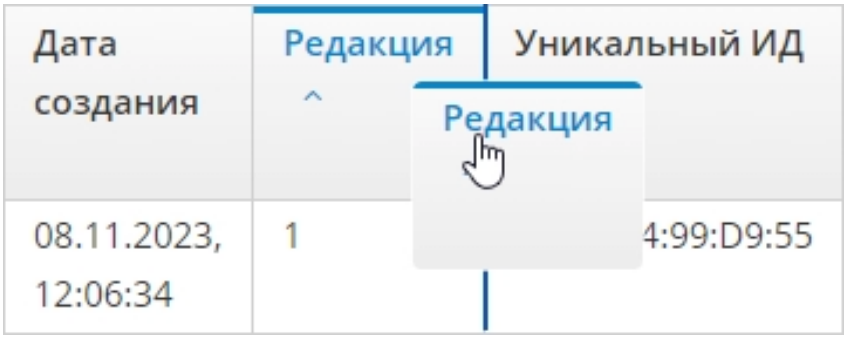

Рисунок 16 – Изменение порядка следования столбцов

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца (см. Рисунок 17).

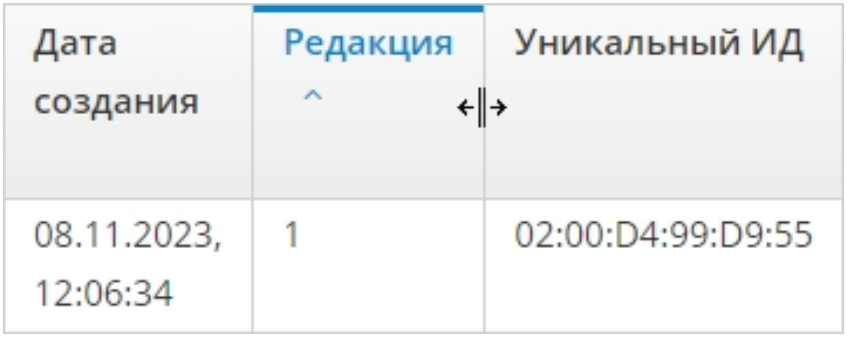

Рисунок 17 – Изменение ширины столбцов

Для сброса ранее выполненных изменений внешнего вида таблицы необходимо нажать экранную кнопку **[Сбросить порядок колонок]**.

Основные параметры списка BPM приведены в таблице (см. Таблица 17).

Таблица 17 – Основные параметры списка BPM

Параметр	Описание
«Дата создания»	Временная метка выполнения публикации BPM
«Редакция»	Порядковый номер версии публикации
«Уникальный ИД»	Уникальный идентификатор BPM: MAC-адрес или номер сессии
«IP-адрес»	IP-адрес, назначенный BPM
«Название»	Наименование BPM и ссылка на его журнал
«Уровень кеша»	Уровень кеша, на котором находится BPM
«Время последнего логина»	Временная метка последней успешной аутентификации пользователя
«Фонд»	Наименование фонда BPM и ссылка на него
«Статус»	Флаг использования публикации BPM из фонда BPM
«Статус обновлен»	Временная метка обновления статуса

Параметр	Описание
«Используется»	Флаг назначения ВРМ. Значение «Нет» свидетельствует о том, что ВРМ находится в кеше
«Хост источника»	Наименование инициатора выдачи ВРМ
«IP источника»	IP-адрес инициатора выдачи ВРМ
«Владелец»	Субъект, запросивший выдачу ВРМ
«Версия агента»	Версия компонента «Агент», установленного в гостевой ОС ВРМ

Для отправки сообщения во все назначенные пользователям ВРМ фонда, к которому принадлежит выбранная в списке ВРМ, нужно нажать экранную кнопку **[Сообщение]**. Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка». ВМ при этом необязательно должна находиться в состоянии «Включена» (например, ВМ может быть в состоянии «Приостановлена»).

6.2.2 . Фильтрация списка ВРМ

Для списка ВРМ доступна механика фильтрации (см. Рисунок 13). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Найти]**. Для сброса всех установленных параметров нужно нажать экранную кнопку **[Сбросить]**.

Подробное описание механики фильтрации списка ВРМ приведено в таблице (см. Таблица 18).

ⓘ При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

⚠ При применении нескольких одинаковых фильтров к списку, фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 18 – Параметры фильтрации

Атрибут	Условия	Значение
«Дата создания»	Формирование списка ВРМ по времени создания: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»
«Редакция»	Формирование списка ВРМ: ▪ «Является» - включая указанную редакцию; ▪ «Не является» - исключая указанную редакцию	Ручной ввод

Атрибут	Условия	Значение
«Уникальный ИД»	Формирование списка BPM: ▪ «Является» - по указанному идентификатору; ▪ «Не является» - исключая указанный идентификатор; ▪ «Начинается с» - по начальной части идентификатора; ▪ «Оканчивается на» - по конечной части идентификатора; ▪ «Содержит» - включая указанную часть идентификатора	Ручной ввод
«IP-адрес»	Формирование списка BPM: ▪ «Является» - по указанному IP-адресу инициатора выдачи BPM; ▪ «Не является» - исключая указанный IP-адрес инициатора выдачи BPM; ▪ «Начинается с» - по начальной части IP-адреса инициатора выдачи BPM; ▪ «Оканчивается на» - по конечной части IP-адреса инициатора выдачи BPM; ▪ «Содержит» - включая указанную часть IP-адреса инициатора выдачи BPM	Ручной ввод
«Название»	Формирование списка BPM: ▪ «Является» - по указанному наименованию BPM; ▪ «Не является» - исключая указанное наименование BPM; ▪ «Начинается с» - по начальной части наименования BPM; ▪ «Оканчивается на» - по конечной части наименования BPM; ▪ «Содержит» - включая указанную часть наименования BPM	Ручной ввод
«Фонд»	Формирование списка BPM: ▪ «Является» - по указанному наименованию фонда BPM; ▪ «Не является» - исключая указанное наименование фонда BPM; ▪ «Начинается с» - по начальной части наименования фонда BPM; ▪ «Оканчивается на» - по конечной части наименования фонда BPM; ▪ «Содержит» - включая указанную часть наименования фонда BPM	Ручной ввод
«Статус»	Формирование списка BPM: ▪ «Является» - по указанному статусу BPM; ▪ «Не является» - исключая указанный статус BPM	▪ «Подготовка»; ▪ «Действительный»; ▪ «Удаление»; ▪ «Удаляется»; ▪ «Удален»; ▪ «Ошибка»; ▪ «Отменяется»; ▪ «Отменено»

Атрибут	Условия	Значение
«Статус обновлен»	Формирование списка BPM по времени обновления статуса: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»
«Используется»	Формирование списка BPM: ▪ «Является» - по используемым BPM; ▪ «Не является» - исключая используемые BPM	▪ «Да»; ▪ «Нет»
«Хост источника»	Формирование списка BPM: ▪ «Является» - по указанному наименованию инициатора выдачи BPM; ▪ «Не является» - исключая указанное наименование инициатора выдачи BPM; ▪ «Начинается с» - по начальной части наименования инициатора выдачи BPM; ▪ «Оканчивается на» - по конечной части наименования инициатора выдачи BPM; ▪ «Содержит» - включая указанную часть наименования инициатора выдачи BPM	Ручной ввод
«IP источника»	Формирование списка BPM: ▪ «Является» - по указанному IP-адресу инициатора выдачи BPM; ▪ «Не является» - исключая указанный IP-адрес инициатора выдачи BPM; ▪ «Начинается с» - по начальной части IP-адреса инициатора выдачи BPM; ▪ «Оканчивается на» - по конечной части IP-адреса инициатора выдачи BPM; ▪ «Содержит» - включая указанную часть IP-адреса инициатора выдачи BPM	Ручной ввод
«Владелец»	Формирование списка BPM: ▪ «Является» - по указанному субъекту, инициировавшего выдачу BPM; ▪ «Не является» - исключая указанный субъект, инициировавшего выдачу BPM; ▪ «Начинается с» - по начальной части субъекта, инициировавшего выдачу BPM; ▪ «Оканчивается на» - по конечной части субъекта, инициировавшего выдачу BPM; ▪ «Содержит» - включая указанную часть субъекта, инициировавшего выдачу BPM	Ручной ввод

Атрибут	Условия	Значение
«Версия агента»	Формирование списка ВРМ: ▪ «Является» - по указанной версии Агента; ▪ «Не является» - исключая указанную версию Агента; ▪ «Начинается с» - по начальной части версии Агента; ▪ «Оканчивается на» - по конечной части версии Агента; ▪ «Содержит» - включая указанную часть версии Агента	Ручной ввод
«Состояние»	Формирование списка ВРМ: ▪ «Является» - по указанному состоянию ВМ; ▪ «Не является» - исключая указанное состояние ВМ	▪ «Выключена»; ▪ «Включена»; ▪ «Спящий режим»; ▪ «Неизвестно»
«Уровень кеша»	Формирование списка ВРМ: ▪ «Является» - по указанному уровню кеша; ▪ «Не является» - исключая указанный уровень кеша	▪ «0»; ▪ «1»; ▪ «2»
«Время последнего логина»	Формирование списка по времени последнего запуска ВРМ: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»

6.3 . Шаблоны ВРМ для серверов терминалов

6.3.1 . Шаблон ВРМ для доступа к серверу терминалов MS RDS

Для добавления шаблона администратору Termidesk следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «RDS Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 19).

Таблица 19 – Данные для добавления шаблона для доступа к терминалу MS RDS

Параметр	Описание
«Название»	Текстовое наименование шаблона ВРМ
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона ВРМ
«Терминал»	Наименование существующего терминала MS RDS

6.3.2 . Шаблон BPM для доступа к опубликованным приложениям MS RDS

Для добавления шаблона администратору следует в графическом интерфейсе управления перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «RDS Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 20).

Таблица 20 – Данные для добавления шаблона для доступа к приложениям MS RDS

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«RDS коллекция»	Название существующей в инфраструктуре MS RDS коллекции опубликованных приложений
«Удаленное приложение»	Наименование опубликованного в коллекции приложения

6.3.3 . Шаблон BPM для доступа к серверу терминалов STAL

Для добавления шаблона администратору Termidesk следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «STAL Terminal Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 21).

Таблица 21 – Данные для добавления шаблона для доступа к терминалу STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM

6.3.4 . Шаблон BPM для доступа к опубликованным приложениям STAL

Для добавления шаблона администратору Termidesk следует перейти «Компоненты - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов сервера терминалов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «STAL Remote App Service», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 22).

Таблица 22 – Данные для добавления шаблона для доступа к приложениям STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона BPM
«Удаленное приложение»	Наименование опубликованного в коллекции приложения

6.4 . Настройка технологии единого входа

6.4.1 . Активация технологии единого входа на сервере терминалов MS RDS

Для включения SSO на MS RDS необходимо выполнить следующую последовательность шагов:

- на контроллере домена MS AD создать групповую политику с названием SSO;
- в созданную групповую политику внести следующие изменения:
  - в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Система - Передача учетных данных», выбрать параметр «Разрешить передачу учетных данных, установленных по умолчанию» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local» (см. Рисунок 18), где `disp.termidesk.local` - имя узла с «Универсальным диспетчером» Termidesk. Далее нажать экранные кнопки **[OK]** и **[Применить]**;

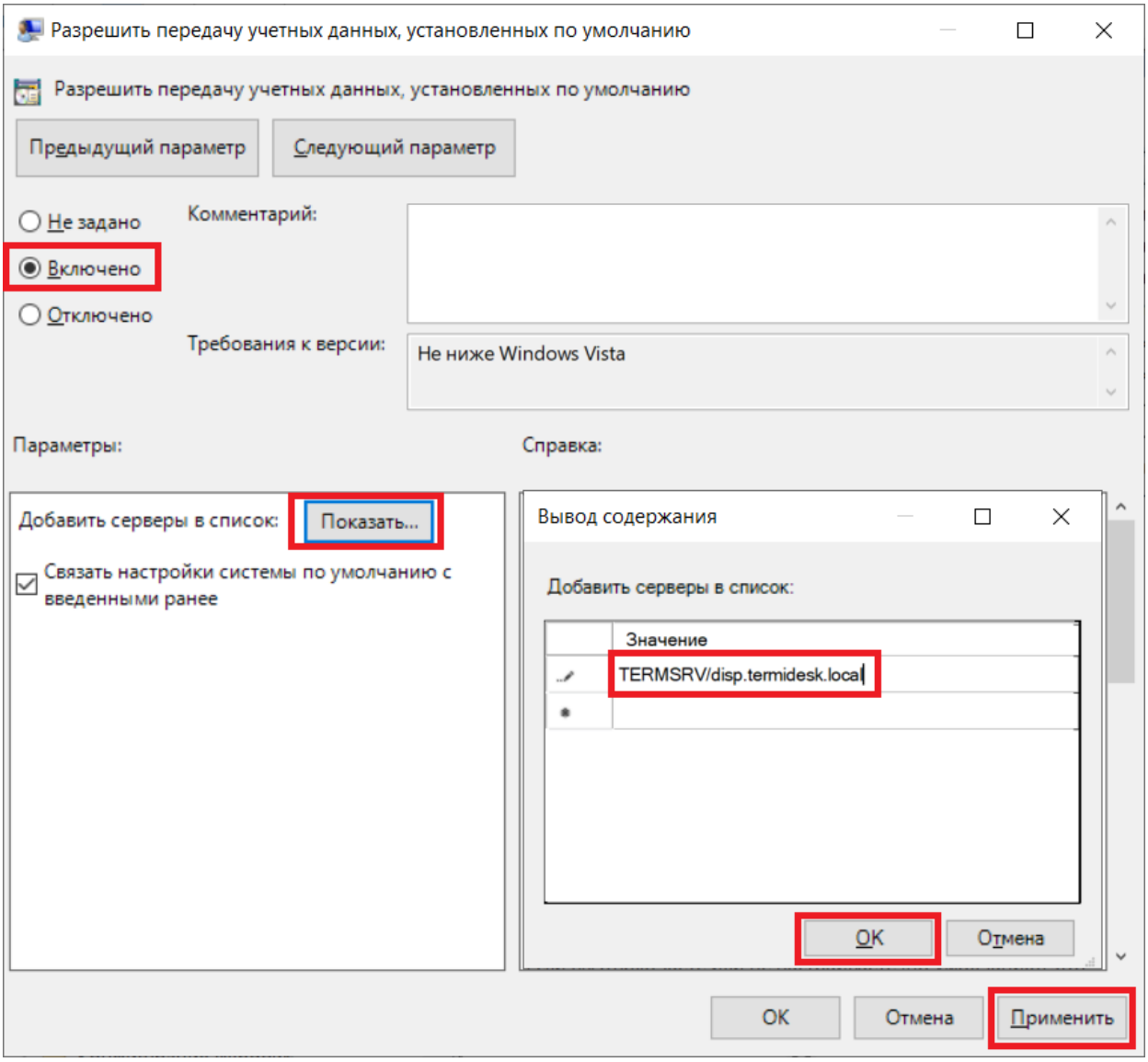

Рисунок 18 – Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

- в этом же списке выбрать параметр «Разрешить передачу новых учетных данных с проверкой подлинности сервера «только NTLM» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local» (см. Рисунок 18). Далее нажать экранные кнопки **[OK]** и **[Применить]**;
- в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Клиент подключения к удаленному рабочему столу», выбрать параметр «Запрашивать учетные данные на клиентском компьютере» и присвоить ему значение «Отключено».

По умолчанию время гарантированного автоматического применения изменений соответствует интервалу 90 – 120 минут после обновления файлов групповых политик на контроллере домена. Если необходимо форсировать применение политики, то на контроллере домена, MS RDS и рабочих станциях пользователей необходимо выполнить команду `gpupdate /force`.

6.5 . Аутентификация пользователей через носитель TouchMemory

Компонент «Клиент» Termidesk поддерживает аутентификацию пользователя через носитель TouchMemory, а именно - через программный продукт «Сетевой модуль ТМ-аутентификации WinNET» производства ООО «Фирма ИнфоКрипт».

Поддерживаемые ОС:

- для пользовательской рабочей станции: ОС Microsoft Windows, Debian (только с графическим окружением GNOME);
- для BPM: ОС Microsoft Windows.

Для реализации функционала администратору необходимо установить в гостевую ОС BPM:

- ПО WinNET 3.1, при установке выбрать значение «Сервер с MsTS»;
- ПО Vitamin (сервер).

7 . УПРАВЛЕНИЕ ПАРМЕТРАМИ ГОСТЕВЫХ ОС

⚠ Раздел приведен в качестве справки. При настройке Termidesk в варианте лицензирования Termidesk Terminal параметры гостевых ОС не используются.

7.1 . Общие сведения

Параметры гостевых ОС позволяют произвести автоматическую и идентичную настройку одной или нескольких гостевых ОС для использования в фонде ВРМ.

Веб-интерфейс Termidesk с установленной ролью «Портал администратора» обеспечивает следующие операции управления параметрами гостевых ОС:

- добавление;
- редактирование;
- удаление;
- просмотр сведений.

Для добавления параметров конфигурации гостевой ОС следует перейти «Компоненты - Параметры гостевых ОС», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка тип ОС.

Созданные конфигурации можно редактировать, для этого нужно пометить необходимые параметры ОС, а затем нажать экранную кнопку **[Изменить]**.

Созданные конфигурации можно удалить, для этого нужно пометить необходимые параметры ОС, а затем нажать экранную кнопку **[Удалить]**.

⚠ Параметры конфигурации гостевой ОС могут быть удалены только в том случае, если они не используются фондом ВРМ.

7.2 . Параметры гостевой ОС Microsoft Windows

7.2.1 . Конфигурация без домена

Для добавления в Termidesk параметров гостевой ОС Microsoft Windows 7 или Microsoft Windows 10 без ввода в домен администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 23).

Таблица 23 – Данные для гостевой ОС Microsoft Windows без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

7.2.2 . Конфигурация при вводе в домен MS AD

Для добавления в Termidesk параметров гостевой ОС Microsoft Windows 7 или Microsoft Windows 10 с последующим вводом в домен администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 24).

Таблица 24 – Данные для гостевой ОС Microsoft Windows при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя службы каталогов MS AD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению ВРМ к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«OU»	Идентификатор организационной единицы, в которую будет добавлены ВРМ

7.3 . Параметры гостевой ОС Linux

7.3.1 . Конфигурация без домена

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux без ввода в домен администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 25).

Таблица 25 – Данные для гостевой ОС Linux без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

7.3.2 . Конфигурация при вводе в домен MS AD

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен MS AD администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 26).

Таблица 26 – Данные для гостевой ОС Linux при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Идентификатор домена MS AD

Параметр	Описание
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий
«OU»	Идентификатор организационной единицы, в которую будет добавлены BPM (опционально). Следует учесть, что при вводе гостевой ОС в домен MS AD: ▪ если учетная запись BPM находится не в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN); ▪ если учетная запись BPM находится в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «CN=Computers,DC=domain,DC=local», т.е. должен использоваться Common Name (CN)

⚠ Для ввода BPM с ОС Astra Linux в домен MS AD необходимо в базовое BPM установить пакет `astra-ad-sssd-client`.

7.3.3 . Конфигурация при вводе в домен FreeIPA

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен FreeIPA администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 27).

Таблица 27 – Данные для гостевой ОС Linux при вводе в домен FreeIPA

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен аутентификации»	Идентификатор домена FreeIPA
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий

⚠ Для ввода BPM с ОС Astra Linux в домен FreeIPA необходимо в базовое BPM установить пакет `astra-freeipa-client`.

7.3.4 . Конфигурация при вводе в домен ALD

Для добавления в Termidesk параметров гостевой ОС на базе GNU/Linux при вводе в домен ALD администратору Termidesk необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 28).

Таблица 28 – Данные для гостевой ОС Linux при вводе в домен ALD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен аутентификации»	Идентификатор домена ALD
«Аккаунт»	Идентификатор субъекта, имеющий полномочия по добавлению BPM к домену
«Пароль»	Набор символов, подтверждающий назначение полномочий

7.4 . Действие при выходе пользователя из ОС

Termidesk поддерживает назначение действий с BPM при выходе пользователя из сессии.

Для назначения действия в графическом интерфейсе управления следует перейти «Настройки - Глобальные политики - Действие при выходе пользователя из ОС», затем нажать экранную кнопку **[Изменить]** и выбрать один из следующих вариантов:

- «Удалять рабочее место» - удалить BPM после выхода пользователя;
- «Нет» - не производить действий с BPM (сохранять состояние).

Совместно с политикой «Действие при выходе пользователя из ОС» применяется политика «Удаление рабочего места после», которая может принимать следующие значения:

- «После события выхода пользователя из ОС»;
- «После события завершения синхронизации профиля».

⚠ Обработка значения «После события завершения синхронизации профиля» не поддерживается в агенте BPM версии 4.1. Функционал приведен для справки.

7.5 . Изменение изображения гостевых ОС

Графические изображения в Termidesk применяются для визуальной идентификации используемых гостевых ОС в фондах BPM.

Для добавления графического изображения следует перейти «Настройки - Галерея» и нажать экранную кнопку **[Создать]**.

В окне добавления изображения нужно заполнить наименование добавляемого объекта, а также добавить само изображение, нажав экранную кнопку **[Выберите изображение]**.

Требования к изображению:

- размер: от 16x16 до 256x256 пикселей;
- соотношение сторон: 1:1;
- поддерживаемые форматы: `.ico`, `.jpeg`, `.jpg`, `.png`.

После добавления изображений гостевых ОС в Termidesk пользователь, подключившись к «Универсальному диспетчеру» Termidesk через компонент «Клиент», увидит их в своем интерфейсе (см. Рисунок 19).

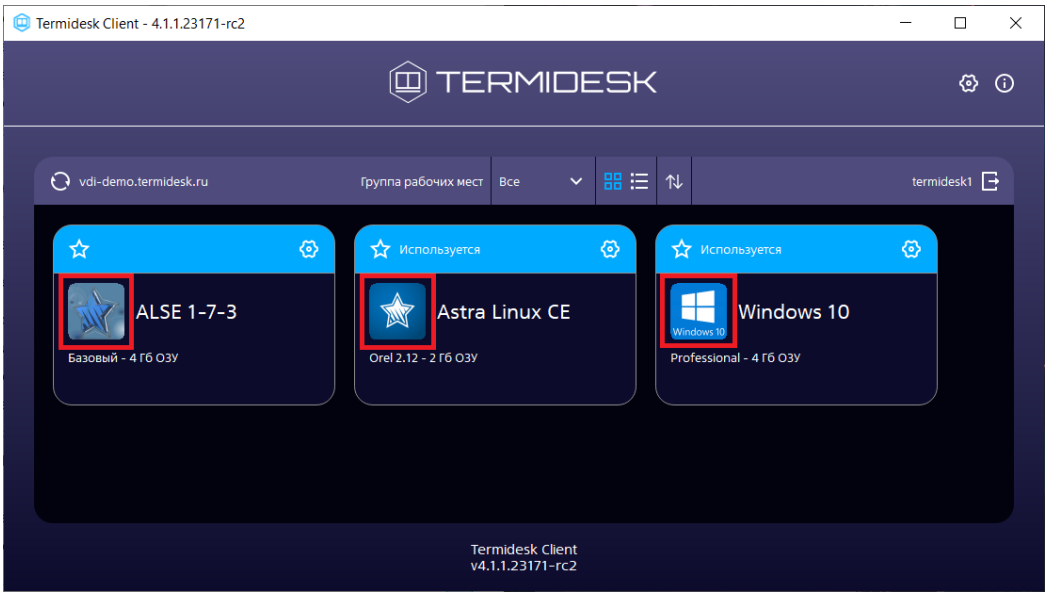

Рисунок 19 – Отображение назначенных изображений в сеансе пользователя

8 . ФОНД РАБОЧИХ МЕСТ

8.1 . Общие сведения о фонде BPM

Фонд BPM – это совокупность подготовленных BPM для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей.

Для отображения списка фондов BPM следует перейти «Рабочие места - Фонды». Основные параметры списка приведены в таблице (см. Таблица 29).

Таблица 29 – Параметры списка фондов

Параметр	Описание
«Фонд рабочих мест»	Наименование фонда BPM
«Статус»	Состояние готовности фонда BPM
«Места»	Общее количество BPM в фонде
«Готовятся»	Количество подготавливаемых BPM
«Выбор протокола»	Флаг возможности выбора пользователем протокола доставки при работе с фондом BPM. Значение определяется политикой фонда BPM «Выбор пользователем протокола доставки»
«Группа рабочих мест»	Принадлежность фонда группе рабочих мест
«Шаблон»	Шаблон BPM, примененный в фонде
«Комментарий»	Информационное сообщение, используемое для описания назначения фонда BPM

Для добавления нового фонда BPM следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**.

Созданные фонды можно редактировать, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Изменить]**.

Созданные фонды можно удалить, для этого нужно пометить название фонда, а затем нажать экранную кнопку **[Удалить]**.

Экранная кнопка **[Политики]**, доступная при выборе названия фонда, открывает параметры выбранного фонда. Совокупность параметров аналогична представленной в «Настройки - Глобальные политики».

После добавления фонда BPM можно перейти к его детальному просмотру. Для этого в сводной таблице окна «Фонды» в столбце «Название» следует нажать на наименование фонда BPM.

На открывшейся странице будут представлены следующие разделы:

- «Рабочие места» – список ВМ и информация о подготовленных BPM, используемых субъектами;

- «Пользователи и группы» – имена пользователей и наименование групп, используемые для определения разрешений по доступу к фондам BPM;
- «Протоколы доставки» – доступные протоколы удаленного доступа, используемые при доставке BPM;
- «Публикации» – актуальная информация о созданном фонде BPM. Раздел будет отсутствовать, если фонд используется для публикации приложений или для доступа к терминальным сессиям;
- «Журнал» – системные сообщения, связанные с жизненным циклом фонда BPM.

Настройка отдельных глобальных параметров по управлению фондами BPM (например, «Максимальное количество рабочих мест, удаляемых единовременно из фонда рабочих мест») доступна в общих системных параметрах Termidesk (см. подраздел **Общие системные параметры Termidesk**).

8.2 . Добавление фонда рабочих мест

8.2.1 . Добавление фонда BPM

Для добавления фонда BPM следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Виртуальные машины».

Откроется мастер публикации фонда (см. Рисунок 20). Необходимо заполнить параметры, указанные в таблице, (см. Таблица 30) и нажать экранную кнопку **[Далее]**. При нажатии экранной кнопки **[Отменить]**, или клавиши **<Esc>**, или иконки «Крестик», на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

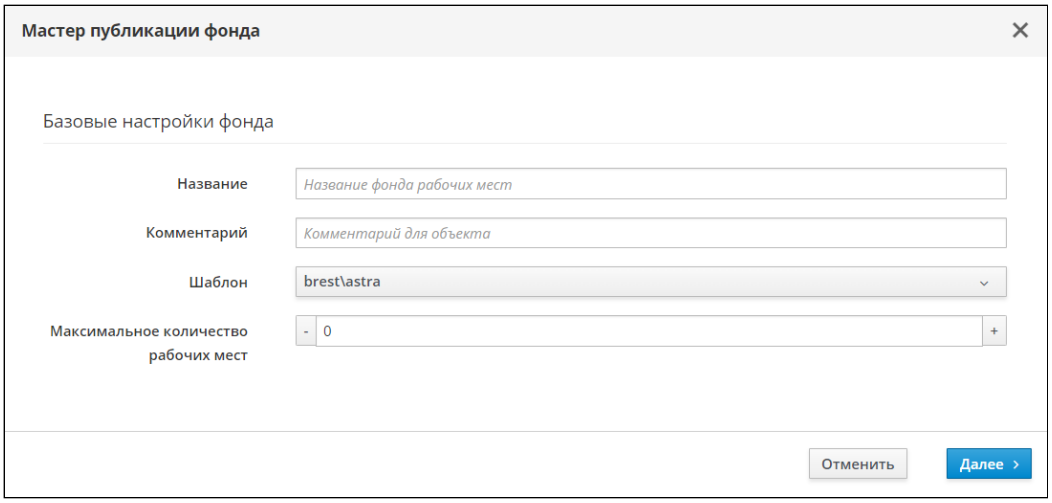

Рисунок 20 – Базовые настройки фонда в Мастере публикации

Таблица 30 – Базовые настройки фонда

Параметр	Описание
«Название»	Ввести текстовое наименование фонда BPM. Наименование может содержать только латинские буквы, цифры, пробел, дефис и нижнее подчеркивание. Параметр обязателен для заполнения
«Комментарий»	Ввести информационное сообщение, используемое для описания назначения фонда BPM
«Шаблон»	Выбрать из списка шаблон, который будет использоваться при создании BPM
«Максимальное количество рабочих мест»	Задать максимальное количество BPM в фонде. Максимальное число BPM не может быть меньше значения, указанного в параметре «Кеш рабочих мест 1-го уровня» на следующем шаге мастера

Если обязательное поле не было заполнено или есть ошибка при заполнении, оно будет подсвечено красным цветом и будет выведено сообщение об ошибке (см. Рисунок 21) после нажатия экранной кнопки **[Далее]**. Индикация цветом и сообщение не исчезнут после заполнения поля.

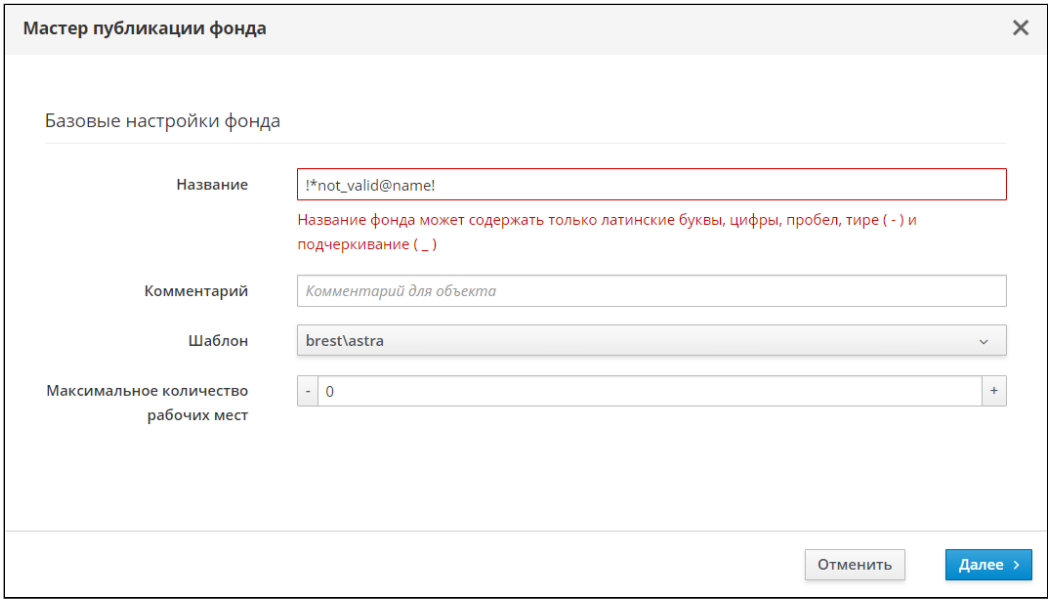

Рисунок 21 – Пример сообщения об ошибке

Далее будет выполнен переход на следующий шаг настройки (см. Рисунок 22) мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. Таблица 31). Поскольку во время перехода выполняется отправка данных на сервер, возможна ситуация, что при возвращении на предыдущий шаг появится сообщение об ошибке, если параметр «Протоколы доставки» не был заполнен. Отправка данных на сервер происходит всегда при переходе между шагами, кроме перехода назад с завершающего этапа.

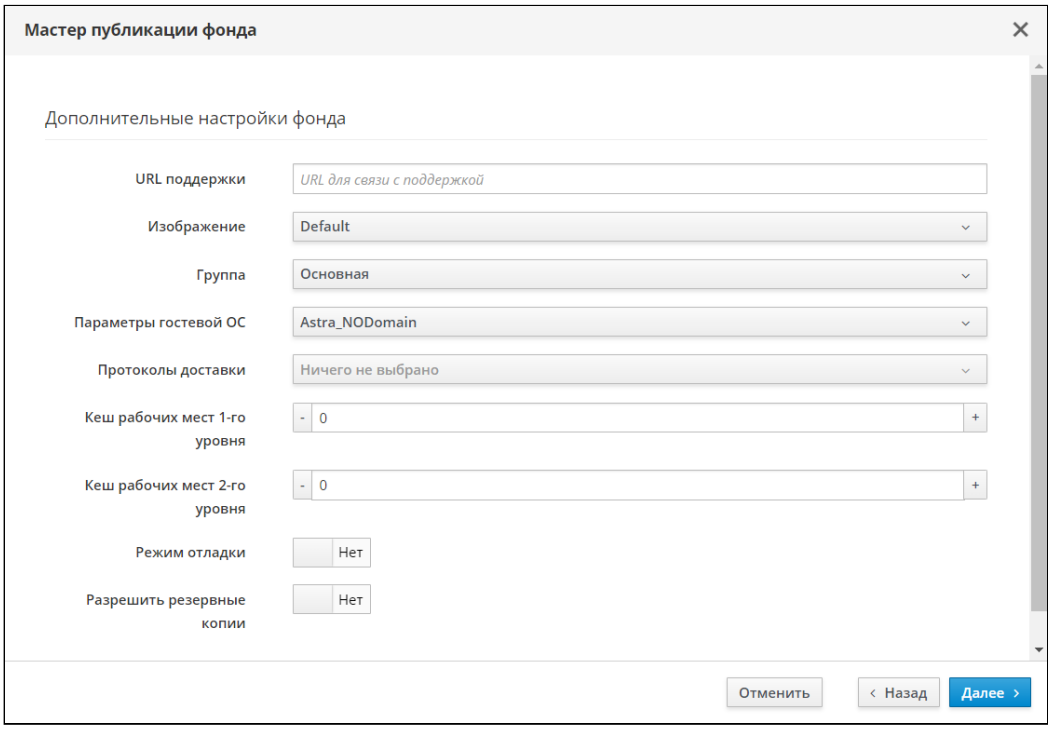

Рисунок 22 – Дополнительные настройки фонда Мастера публикации

Таблица 31 – Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	Ввести URL для связи с технической поддержкой
«Изображение»	Выбрать графическое представление фонда BPM
«Группа»	Выбрать группу рабочих мест, в которой будет отображаться созданный фонд BPM
«Параметры гостевой ОС»	Выбрать параметры конфигурации гостевой ОС, которые будут использованы при создании BPM
«Протоколы доставки»	Выбрать один или несколько протоколов доставки, которые будут доступны для фонда BPM
«Кеш рабочих мест 1-го уровня»	Задать количество созданных, настроенных и запущенных BPM в фонде
«Кеш рабочих мест 2-го уровня»	Задать количество созданных, настроенных и выключенных BPM. Для использования кеша рабочих места 2-го уровня необходимо, чтобы в параметре «Кеш рабочих мест 1-го уровня» было задано хотя бы одно BPM
«Режим отладки»	Активация более подробной детализации логов для фонда BPM, по умолчанию режим отключен. При включении режима Termidesk перестает удалять ВМ в фонде BPM
«Разрешить резервные копии»	Активация режима резервного копирования ВМ фонда BPM при использовании системы Rubackup. По умолчанию режим отключен

После заполнения параметров нужно нажать экранную кнопку **[Далее]**.

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]**. Далее будет отображено временное окно с заблокированными экранными кнопками. При успешном создании фонда в этом же окне должно появиться сообщение (см. Рисунок 23) «Фонд успешно создан!», окно будет автоматически закрыто по истечении 3 секунд.

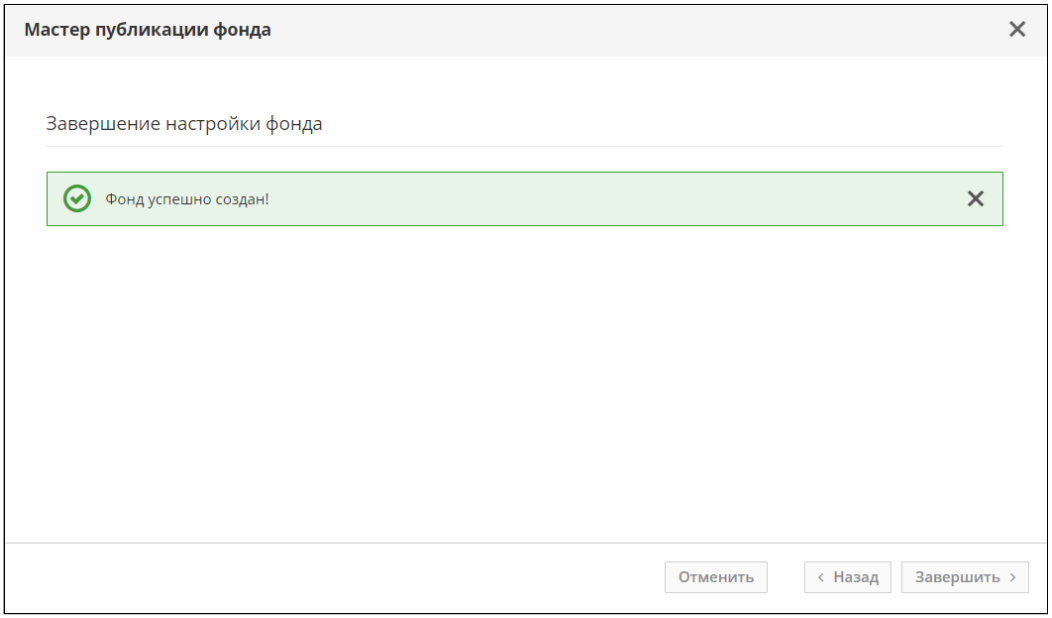

Рисунок 23 – Успешное завершение настройки публикации фонда

8.3 . Политики фонда BPM

Для управления доступом и ресурсами в фондах BPM используются следующие виды политик:

- глобальные - применяются ко всем фондам BPM и устанавливают общие настройки доступа и использования ресурсов пользователями BPM. Для редактирования глобальных политик следует перейти «Настройки - Глобальные политики», выбрать политику и нажать экранную кнопку **[Изменить]**;
- индивидуальные - переопределяют настройки глобальных политик и устанавливают индивидуальные настройки доступа и использования ресурсов пользователями конкретного фонда BPM. Для редактирования индивидуальных политик следует перейти «Рабочие места - Фонды», выбрать нужный фонд BPM, нажать экранную кнопку **[Политики]**, выбрать политику и нажать экранную кнопку **[Изменить]**.

Настройки выбранной политики можно сбросить до значений по умолчанию при помощи экранной кнопки **[Сбросить]**.

Начиная с Termidesk версии 5.0 изменен способ работы и хранения политик фонда ВРМ. Во время обновления распределенной или отказоустойчивой конфигурации установки с Termidesk версии 4.X на версию 5.X изменение политик нужно проводить после обновления на новую версию всех узлов Termidesk.
Если на ВРМ есть сессия пользователя, то политика применится после перезагрузки ВРМ. Для терминального сервера перезагрузка обязательна.

Администратор должен включить соответствующие политики фонда ВРМ для работы перенаправления ресурсов, если при подключении к ВРМ пользователь использует `termidesk-viewer`. При подключении пользователя по протоколу RDP из компонента «Клиент» могут использоваться стандартные утилиты ОС, в этом случае возможность перенаправления регулируется на уровне протокола доставки.

Список доступных политик представлен в таблице (см. Таблица 32).

Таблица 32 – Перечень доступных политик фонда ВРМ

Название политики	Описание
«Буфер обмена в протоколах доставки "RDP" и "SPICE (vdi-viewer, эксперим.)"»	Управление использованием буфера обмена в протоколах доставки. Возможные значения: ▪ «Выключить перенаправление буфера»; ▪ «Двустороннее перенаправление буфера» (по умолчанию); ▪ «Перенаправление буфера только от сервера клиенту»; ▪ «Перенаправление буфера только от клиента серверу»
«Выбор пользователем протокола доставки»	Определяет возможность выбрать протокол доставки пользователем для подключения к ВРМ. Возможные значения: ▪ «Разрешен» (по умолчанию); ▪ «Запрещен»
«Действие при выходе пользователя из ОС»	Определяет действие после выхода пользователя из ОС. Для сервисного фонда ВРМ поставщика ресурсов «метапоставщик» должно быть оставлено значение по умолчанию. Возможные значения: ▪ «Нет» (по умолчанию); ▪ «Удалять рабочее место»; ▪ «Не сохранять изменения» - ВМ будет возвращена к ранее созданному снимку. Значение политики применимо для фондов ВРМ, основанных на шаблонах «Связанный клон oVirt/RHEV», «Связанный клон» или «Полный клон» VMware vSphere. При применении последних двух значений в индивидуальных политиках фонда ВРМ может быть выведено уведомление «Данное значение политики не применимо к выбранному фонду», если у поставщиака ресурсов фонда ВРМ нет возможности создавать снимки ВМ

Название политики	Описание
«Завершать сеанс при достижении лимита времени»	Управление сеансами пользователей при достижении заданного лимита времени: по истечении лимита времени RDP-сессия будет завершена, а не отключена. Если политика имеет значение «Не задано», то она не будет применяться на ВРМ, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «Не задано»; ▪ «Выключено» (по умолчанию); ▪ «Включено»
«Запрос учетных данных при подключении к ВРМ»	Политика определяет, должен ли пользователь вводить логин и пароль на ВРМ при запуске рабочих столов и приложений. В ОС ВРМ при этом должна быть выполнена настройка автоматической авторизации пользователя, как это приведено в подразделе **Настройка технологии единого входа в гостевой ОС ВМ**. Возможные значения: ▪ «Выключен» - запрос учетных данных не происходит; ▪ «Включен»
«Интервал мониторинга кеша перемещаемых профилей пользователей (RDP)»	Политика позволяет ограничить интервал мониторинга (в минутах) размера кеша перемещаемых профилей пользователей для протокола RDP. Политика определяет, как часто проверяется размер всего кеша перемещаемых профилей пользователей, укаханный в политике «Ограничить размер полного кеша перемещаемых профилей пользователей (RDP)». При изменении политики требуется перезагрузка ВРМ или терминальных серверов. Возможные значения (в минутах): от 15 до 10080. Значение по умолчанию: «900»
«Использование механизма RemoteFX (RDP)»	Политика активации механизма RemoteFX для протокола RDP. Если необходимо активировать возможность перенаправления USB-устройств из пользовательской рабочей станции в ВРМ, нужно установить политике значение «Включен». Возможные значения: ▪ «Выключен» (по умолчанию); ▪ «Включен»
«Использовать обязательные профили на сервере узла сеанса удаленных рабочих столов (RDP)»	Политика позволяет указать, используют ли службы удаленных рабочих столов обязательный профиль для всех пользователей, удаленно подключающихся к серверу узла сеанса удаленных рабочих столов. При включении политики службы удаленных рабочих столов используют путь, указанный в политике «Указать путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)», в качестве корневого каталога для обязательного профиля пользователя. Все пользователи, удаленно подключающиеся к серверу узла сеансов удаленных рабочих столов, используют один и тот же профиль пользователя. При отключении политики обязательные профили пользователей не будут использоваться пользователями, удаленно подключающимися к серверу узла сеанса удаленных рабочих столов. При изменении политики требуется перезагрузка ВРМ или терминальных серверов. Возможные значения: ▪ «Выключено» (по умолчанию); ▪ «Включено»

Название политики	Описание
«Лимит времени для активных сеансов служб удаленных рабочих столов (RDP, SPICE, и т.д.)»	Управление лимитом времени для активных сеансов служб удаленных рабочих столов (для протоколов RDP, SPICE, и т.д.). Указывается время, по истечении которого сеанс переходит в отключенное состояние (завершается). Политика применяется в момент авторизации пользователя в BPM. В версиях Termidesk ниже 4.3 параметр задавался при настройке гостевых ОС («Компоненты - Параметры гостевых ОС»). При возврате к версиям Termidesk ниже 4.3 параметр будет выставлен в значение по умолчанию. Если политика имеет значение «Не задано», то она не будет применяться на BPM, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «Нет ограничений» (по умолчанию); ▪ «Не задано»; ▪ выбор: 1 мин, 5 мин, 10 мин, 15 мин, 30 мин, 1 час, 2 часа, 3 часа, 6 часов, 8 часов, 12 часов, 16 часов, 18 часов, 1 день, 2 дня, 3 дня, 4 дня, 5 дней
«Лимит времени для выхода из сеансов RemoteApp»	Управление лимитом времени для выхода из сеансов RemoteApp. Позволяет указать, как долго сеанс пользователя при использовании RemoteApp (удаленное приложение) будет оставаться в отключенном состоянии после закрытия всех программ RemoteApp. Если политика имеет значение «Не задано», то она не будет применяться на BPM, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «Никогда» (по умолчанию); ▪ «Сразу»; ▪ «Не задано»; ▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»
«Лимит времени для отключенной сессии»	Установка лимита времени для отключенной RDP-сессии. Работает совместно с политикой «Завершать сеанс при достижении лимита времени». Если политика имеет значение «Не задано», то она не будет применяться на BPM, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «Нет ограничений» (по умолчанию); ▪ «Не задано»; ▪ выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»
«Масштабирование экрана для протокола RDP»	Политика управления масштабированием экрана для протокола RDP. Возможные значения: ▪ «Выключено» (по умолчанию); ▪ «Включено»

Название политики	Описание
«Механизм обеспечения безопасности на уровне сети (RDP)»	Политика управления обеспечением безопасности на уровне сети для протокола RDP. Для подключения к STAL необходимо использовать значение «TLS» или «RDP». Для подключения к MS RDS необходимо использовать значение «NLA». Политика может быть задана для конкретного фонда BPM на странице самого фонда BPM. Возможные значения: ▪ «Автосогласование» (по умолчанию); ▪ «RDP»; ▪ «TLS»; ▪ «NLA»
«Ограничить размер полного кеша перемещаемых профилей пользователей (RDP)»	Политика позволяет ограничить размер всего кеша перемещаемых профилей пользователей на локальном диске. Для политики необходимо указать максимальный размер (в гигабайтах) для всего кеша перемещаемых профилей пользователей. Когда размер всего кеша перемещаемых профилей пользователей превысит указанный максимальный размер, самые старые (наименее недавно использованные) перемещаемые профили пользователей будут удалены до тех пор, пока размер всего кеша перемещаемых профилей пользователей не станет меньше указанного максимального размера. При изменении политики требуется перезагрузка BPM или терминальных серверов. Зависит от политики «Интервал мониторинга кеша перемещаемых профилей пользователей (RDP)». Возможные значения (в гигабайтах): от 5 до 10000. Значение по умолчанию: «600»
«Отделяемый пользовательский профиль»	Использование отделяемого пользовательского профиля в BPM. Политика применяется при старте BPM. Возможные значения: ▪ «Выключен» (по умолчанию); ▪ «Включен»
«Передача файлов в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Управление передачей файлов в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Возможные значения: ▪ «Разрешена» (по умолчанию); ▪ «Запрещена»
«Перенаправление видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Управление перенаправлением видеокамеры в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Возможные значения: ▪ «Разрешено» (по умолчанию); ▪ «Запрещено»
«Перенаправление смарт-карт в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Управление перенаправлением смарт-карт в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Возможные значения: ▪ «Разрешено» (по умолчанию); ▪ «Запрещено»

Название политики	Описание
«Подключение с отличным именем пользователя»	Политика управления подключением пользователя к ВМ. Применяется в случае, если вводимый в ВМ логин отличен от логина назначенной машины в Termidesk. Возможные значения: ▪ «Разрешено»; ▪ «Запрещено» (по умолчанию)
«Показывать обои»	Управление отображением обоев рабочего стола ВРМ. В текущей версии Termidesk изменение значения политики не вносит изменение в функционирование. Возможные значения: ▪ «Разрешить отображение»; ▪ «Запретить отображение» (по умолчанию)
«Политика простоя рабочего места»	Разрешенное время простоя ВРМ в секундах. Значение «-1» означает неограниченное время простоя. Значение по умолчанию: «-1»
«Политика управления автоподключением устройств (RDP)»	Управление возможностбю автоматически перенаправлять устройства для протокола RDP. Возможные значения: ▪ «Не используется» (по умолчанию); ▪ «Разрешить автоподключение»; ▪ «Запретить автоподключение»
«Политика управления глубиной цвета (RDP)»	Управление максимально допустимым количеством цветов, отображаемых экраном ВРМ. Политика применяется только для протокола RDP. Если политика имеет значение «Не задано», то она не будет применяться на ВРМ, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Для подключения к STAL через стандартную утилиту Windows mstsc необходимо использовать значение «32 бит». Возможные значения: ▪ «15 бит»; ▪ «16 бит» (по умолчанию); ▪ «24 бит»; ▪ «32 бит»; ▪ «Не задано»
«Политика управления композицией рабочего стола (RDP)»	Управление отображением художественных эффектов рабочего стола. Для корректного отображения художественных эффектов в параметре «Политика управления глубиной цвета (RDP)» требуется установить значение «32 бита». Политика применяется только при подключении по протоколу RDP к гостевой ОС Microsoft Windows. Возможные значения: ▪ «Разрешить композицию»; ▪ «Запретить композицию» (по умолчанию)
«Политика управления параметрами перенаправления принтеров»	Управление перенаправлением принтеров в протоколах доставки. Можно запретить перенаправление, разрешить перенаправлять все принтеры или только выбранные пользователем. Возможные значения: ▪ «Не перенаправлять» (по умолчанию); ▪ «Перенаправлять все»; ▪ «Перенаправлять выбранные пользователем»

Название политики	Описание
«Политика управления перенаправлением дисков и папок»	Управление перенаправлением дисков и каталогов. Возможные значения: ▪ «Разрешить перенаправление»; ▪ «Запретить перенаправление» (по умолчанию) ⚠ В текущей версии Termidesk перенаправление дисков и каталогов выполняется всегда.
«Политика управления перенаправлением звука (аудио и микрофон) (RDP)»	Управление перенаправлением звука в протоколе RDP. Возможные значения: ▪ «Не используется» (по умолчанию); ▪ «Разрешить перенаправление»; ▪ «Запретить перенаправление»
«Политика управления перенаправлением последовательных портов (RDP)»	Управление перенаправлением последовательных портов. Политика применяется только для протокола RDP. Возможные значения: ▪ «Разрешить перенаправление»; ▪ «Запретить перенаправление» (по умолчанию)
«Политика управления перенаправлением смарт-карт (RDP)»	Управление перенаправлением смарт-карт. Политика применяется только для протокола RDP. Возможные значения: ▪ «Разрешить перенаправление»; ▪ «Запретить перенаправление» (по умолчанию)
«Политика управления сглаживанием шрифтов (RDP)»	Управление сглаживанием шрифтов, отображаемых экраном ВРМ. Политика применяется только для протокола RDP. Возможные значения: ▪ «Разрешить сглаживание» (по умолчанию); ▪ «Запретить сглаживание»
«Политика управления сжатием (RDP)»	Управление использованием сжатия данных при взаимодействии с ВРМ по протоколу RDP. Если политика имеет значение «Не задано», то она не будет применяться на ВРМ, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «Включено» (по умолчанию); ▪ «Выключено»; ▪ «Не задано»
«Политика управления типом сети (RDP)»	Управление типом сетевого подключения, которое будет использоваться при подключении к ВРМ по протоколу RDP. Возможные значения: ▪ «Модем»; ▪ «Низкоскоростное широкополосное подключение»; ▪ «Широкополосное подключение»; ▪ «Высокоскоростное широкополосное подключение»; ▪ «Глобальная сеть»; ▪ «Локальная сеть»; ▪ «Авто» (по умолчанию)

Название политики	Описание
«Политика управления уровнем сжатия (RDP)»	Управление уровнем сжатия данных, при взаимодействии с BPM по протоколу RDP. Если политика имеет значение «Не задано», то она не будет применяться на BPM, таким образом администратор сохраняет возможность управления параметрами подключения средствами контроллера домена. Возможные значения: ▪ «0»; ▪ «1» (по умолчанию); ▪ «2»; ▪ «Не задано»
«Полноэкранный режим (для SPICE)»	Политика ограничения работы в полноэкранном режиме. Возможные значения: ▪ «Включен» (по умолчанию); ▪ «Выключен»
«Разрешение видеокамеры в протоколе доставки "SPICE (vdi-viewer, эксперим.)"»	Допустимые разрешения видеокамеры в протоколах доставки. Политика применяется только для протокола SPICE (vdi-viewer, эксперим.). Значение по умолчанию: «320-2560x240-1440»
«Удаление рабочего места после»	Политика определяет событие, после которого будет произведено удаление BPM. Возможные значения: ▪ «После события выхода пользователя из ОС» (по умолчанию); ▪ «После события завершения синхронизации профиля»
«Указать путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)»	По умолчанию службы удаленных рабочих столов хранят все профили пользователей локально на сервере узла сеанса удаленных рабочих столов. Политика используется для указания общего сетевого ресурса, в котором профили пользователей могут храниться централизованно, позволяя пользователю получать доступ к одному и тому же профилю для сеансов на всех серверах узла сеансов удаленных рабочих столов, настроенных на использование общего сетевого ресурса для профилей пользователей. При задании значения для политики, службы удаленных рабочих столов будут использовать указанный путь в качестве корневого каталога для всех профилей пользователей. Непосредственно профили будут содержаться во вложенных каталогах, названных по имени учетной записи каждого пользователя %USERNAME%, которые появятся на сетевом ресурсе автоматически после подключения пользователя. При изменении политики требуется перезагрузка BPM или терминальных серверов. Зависит от политики «Использовать обязательные профили на сервере узла сеанса удаленных рабочих столов (RDP)». Формат указания сетевого ресурса (пример): \\имя_компьютера\имя_общего_ресурса\. Значение «null» означает, что путь не задан. Значение по умолчанию: «null»

Название политики	Описание
«Установить домашний каталог пользователя служб RDS (RDP)»	Политика указывает, будут ли службы удаленных рабочих столов использовать указанный сетевой ресурс или путь к локальному каталогу в качестве корневого каталога домашнего каталога пользователя для сеанса служб удаленных рабочих столов. Формат указания сетевого ресурса (пример): \\имя_компьютера\имя_общего_ресурса\. При изменении политики требуется перезагрузка BPM или терминальных серверов. Значение «null» означает, что путь не задан. Значение по умолчанию: «null»

8.4 . Объединение фондов в группы BPM

Группы BPM отображаются как самостоятельные разделы в интерфейсе пользователя. Группы BPM являются логическим признаком, по которому можно объединять отображение фондов BPM для пользователей.

Для добавления группы администратору Termidesk следует перейти «Настройки - Группы рабочих мест» и нажать экранную кнопку **[Создать]**, затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 33).

Таблица 33 – Данные для объединения фондов BPM в группы

Параметр	Описание
«Название»	Текстовое наименование группы BPM
«Комментарий»	Информационное сообщение, используемое для описания назначения группы BPM
«Приоритет»	Преимущество использования группы BPM в «Портале пользователя»

Для редактирования группы рабочих мест в Termidesk нужно пометить необходимую группу и нажать экранную кнопку **[Изменить]**.

Для удаления группы рабочих мест в Termidesk нужно пометить необходимую группу и нажать экранную кнопку **[Удалить]**.

8.5 . Управление BPM

8.5.1 . Управление терминальными сессиями в назначенном фонде BPM

В графическом интерфейсе управления Termidesk предусмотрена возможность просмотра информации и управления терминальными сессиями пользователей в назначенном фонде BPM.

Для просмотра основных сведений о сессиях пользователей в назначенном фонде BPM следует перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Рабочие места» (см. Рисунок 24).

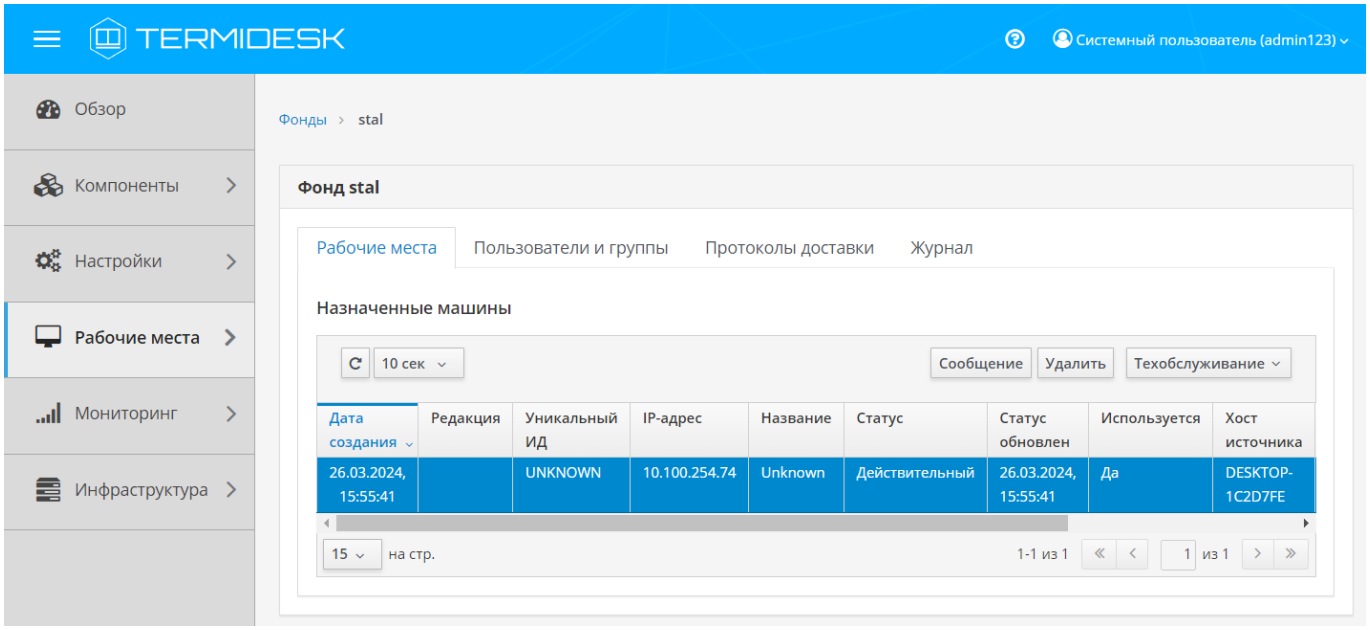

Рисунок 24 – Просмотр сведений о сессиях пользователей в назначенном фонде ВРМ

Для изменения состояния подключений предусмотрены элементы управления (см. Таблица 34).

Таблица 34 – Элементы управления состоянием терминального сервера

Элемент управления	Описание
«Сообщение»	Отправка сообщения пользователю терминального сервера. Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка». Назначенная машина при этом необязательно должна находиться в состоянии «Включена» (например, ВМ может быть в состоянии «Приостановлена»)
«Техобслуживание»	Перевод ВМ терминального сервера в режим техобслуживания (значение «Включить» в выпадающем списке) или вывод из него (значение «Выключить»). Режим техобслуживания - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в сессию на терминальном сервере. Если ВМ находится в режиме техобслуживания, то: ▪ пользователи могут подключаться к существующим сеансам, но не могут запускать новые сеансы; ▪ в существующем активном сеансе, который был создан до включения режима техобслуживания, пользователь может запускать новые приложения на этом терминальном сервере
«Удалить»	Инициирует процесс полного удаления ВМ, включая все связанные с ней данные и конфигурации

ⓘ Для отключения текущей сессии для терминальных подключений (например, STAL) следует выбрать сессию в статусе «Действительный» и нажать экранную кнопку **[Удалить]**. Отображение статуса «Удален» в столбце «Статус» свидетельствует об успешном удалении сессии.

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 35).

Таблица 35 – Основные параметры сессий в назначенном фонде BPM

Параметр	Описание
«Дата создания»	Временная метка создания сессии
«Редакция»	Порядковый номер версии сессии
«Уникальный ИД»	Уникальный идентификатор сессии
«IP-адрес»	IP-адрес терминального сервера, к которому установлено подключение сессии
«Название»	Номер сессии, выданной пользователю и ссылка на ее журнал
«Статус»	Флаг использования сессии
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения сессии
«Хост источника»	Наименование инициатора сессии
«IP источника»	IP-адрес инициатора сессии
«Владелец»	Субъект, инициировавший выдачу сессии
«Версия агента»	Версия компонента «Агент», установленного на терминальном сервере

⚠ После нажатия экранной кнопки **[Удалить]** принудительный штатный выход пользователя из ОС BPM произойдет в течение 30 секунд.

⚠ Сессия пользователя будет автоматически и принудительно завершена, если он был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален.

8.6 . Назначение пользователей доступа

Фонду BPM можно назначать пользователей, которым этот фонд будет доступен.

Для добавления нового пользователя к фонду BPM следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда BPM. На открывшейся странице в разделе «Пользователи и группы» нажать на экранную кнопку **[Создать]** в области «Пользователи».

⚠ Добавление пользователя домена будет доступно только в том случае, если пользователь хотя бы один раз осуществил вход в «Портал пользователя» под своей учетной записью.

8.7 . Назначение групп доступа фонду BPM

Фонду BPM можно назначать группы пользователей домена аутентификации, которым этот фонд будет доступен.

Для добавления новой группы к фонду BPM следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда BPM.

На открывшейся странице в разделе «Пользователи и группы» нужно нажать экранную кнопку **[Создать]** в области «Группы». В окне добавления объекта из выпадающего списка выбрать необходимый домен аутентификации, а затем требуемую для него группу.
Для удаления группы из фонда используется экранная кнопка **[Удалить]**.

⚠ Добавление группы пользователей домена будет возможно только в том случае, если указанная группа существует в службе каталога и добавлена в домен аутентификации в Termidesk.

8.8 . Назначение протоколов фонду BPM

Фонду BPM можно назначать доступные для него протоколы доставки как на этапе настройки при помощи «Мастера публикации фонда», так и после.

Для добавления нового протокола доставки фонду BPM следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда BPM.
На открывшейся странице в разделе «Протоколы доставки» нужно нажать экранную кнопку **[Создать]**. В окне добавления объекта из выпадающего списка выбрать необходимый протокол доставки.

⚠ Добавление протокола доставки в фонд BPM будет доступно только в том случае, если настроен хотя бы один протокол доставки в «Компоненты - Протоколы доставки».

8.9 . Управление сессиями подключенных к фонду BPM пользователей

8.9.1 . Управление активными сессиями пользователей

В графическом интерфейсе управления Termidesk реализована возможность просмотра информации и управления текущими активными сессиями пользователей в фондах BPM.

Доступны следующие возможности по управлению сессией:

- отключение сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Отключить]**. После нажатия экранной кнопки **[Отключить]** принудительный штатный выход пользователя из ОС BPM произойдет в течение 30 секунд. Также сессия пользователя будет автоматически и принудительно завершена, если он был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален;
- сброс сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Сбросить]**;

- подключение к сессии пользователя. Следует перейти «Рабочие места - Сессии», пометить сессию пользователя и нажать экранную кнопку **[Помощник]**. Для работы подключения необходимо, чтобы:
  - в гостевой ОС BPM был установлен компонент «Удаленный помощник» (клиентская часть);
  - в сетевой инфраструктуре предприятия существовал узел с установленным компонентом «Удаленный помощник» (серверная часть) и он был доступен для взаимодействия с «Универсальным диспетчером».

⚠ Функционал управления сессиями пользователя из страницы «Рабочие места - Сессии» недоступен для терминальных сессий. Возможности по управлению такими сессиями приведены в подразделе **Управление терминальными сессиями в назначенном фонде BPM**.

⚠ Не рекомендуется устанавливать компонент «Удаленный помощник» (серверная часть) на узел с установленным компонентом «Универсальный диспетчер», поскольку оба компонента вносят изменения в конфигурацию веб-сервера apache.

Для просмотра основных сведений об активных сессиях пользователей в фондах BPM следует перейти «Рабочие места - Сессии», после чего откроется сводная таблица (см. Рисунок 25).

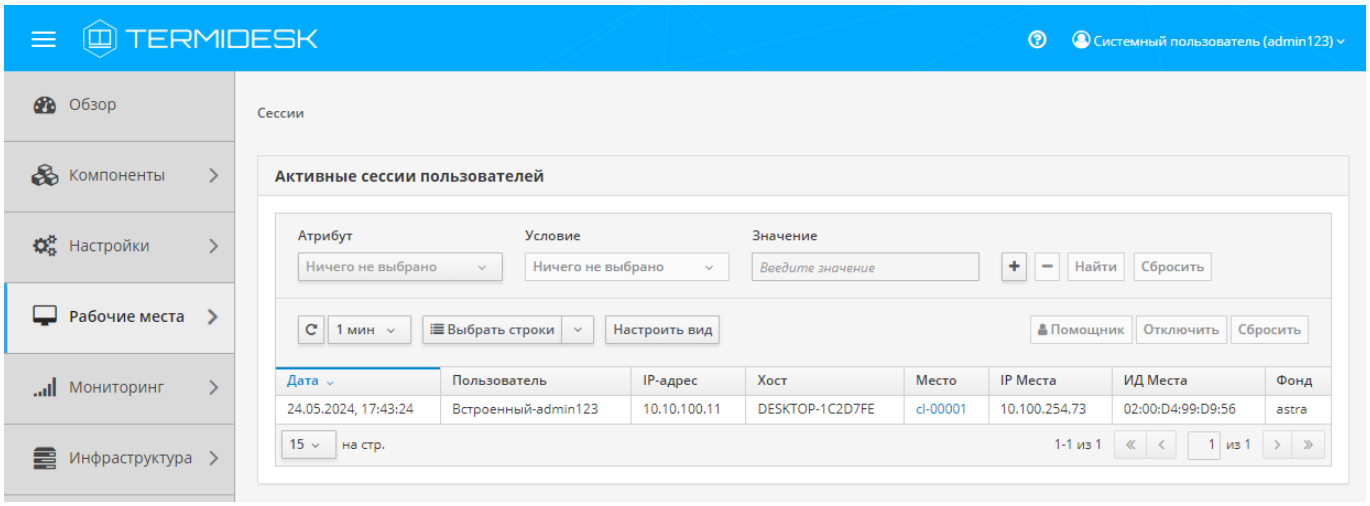

Рисунок 25 – Просмотр сведений об активных сессиях пользователей в фондах BPM

Записи в списке поддерживают функцию множественного выбора и выполнения операций над несколькими объектами одновременно. Выполнить операцию над несколькими объектами можно только тогда, когда она допустима для всех выбранных объектов.

Существуют варианты выбора записей таблицы, доступные через выпадающий список экранной кнопки **[Выбрать строки]**, а именно:

- выделить все строки таблицы, активировав «Выбрать все»;
- выделить все строки на текущей странице таблицы, активировав «Выбрать все на стр.»;

- сбросить выделение строк, активировав «Сбросить».

Для множественного выделения записей можно зажать и удерживать клавиши **<CTRL>** или **< SHIFT>**. Для сброса множественного выделения нужно активировать функцию «Сбросить» экранной кнопки **[Выбрать строки]** или нажать на произвольную строку таблицы.

В случае изменения ширины столбцов или их порядка произойдет сброс ранее выполненного выделения.

Для обновления значений таблицы используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список (см. Рисунок 26) со значениями интервала в минутах, расположенный рядом с указанным элементом.

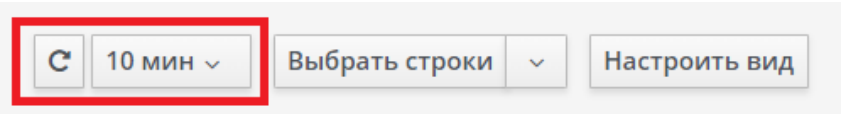

Рисунок 26 – Обновление значений таблицы

Внешний вид таблицы списка активных сессий можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться экранной кнопкой **[Настроить вид]** и отметить наименования столбцов (см. Рисунок 27), которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для применения изменений нужно нажать экранную кнопку **[Сохранить]**. При попытке убрать выбор со всех пунктов и нажатия экранной кнопки **[Сохранить]** отобразится сообщение «Нельзя скрыть все колонки таблицы» и изменение не применится. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить вид]**;

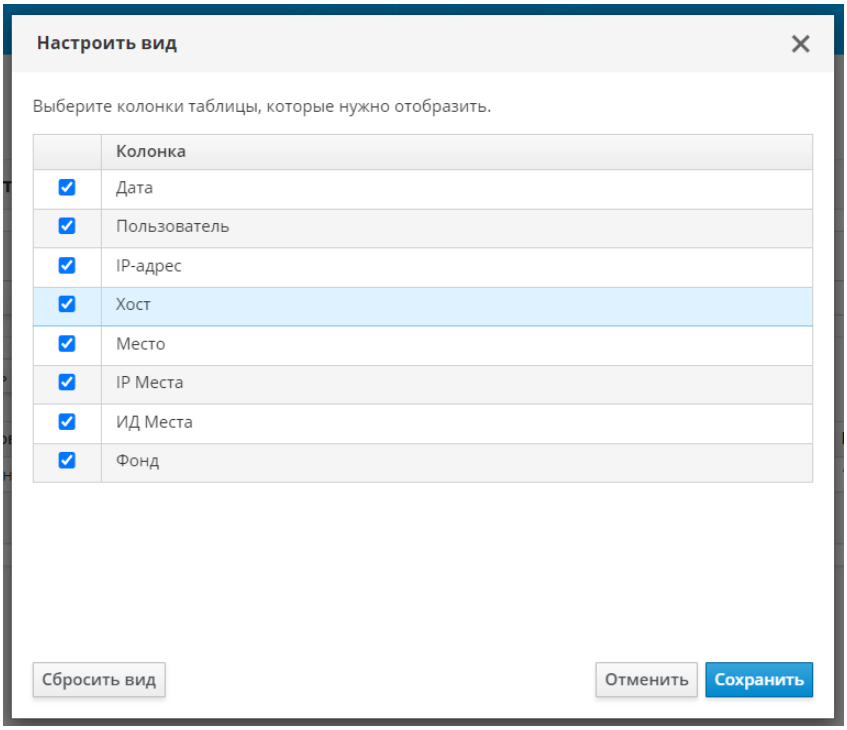

Рисунок 27 – Выбор столбцов для отображения

- порядок следования столбцов. Для изменения порядка следования нужно захватить левой кнопкой мыши заголовок столбца, и, не отпуская кнопку мыши, перенести его в нужное расположение (см. Рисунок 28). Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок колонок]**, которая становится доступна только после изменения порядка следования столбцов и будет скрыта после сброса;

Рисунок 28 – Изменение порядка следования столбцов

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца (см. Рисунок 29).

Рисунок 29 – Изменение ширины столбцов

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. Таблица 36).

Таблица 36 – Основные параметры сессий пользователей

Параметр	Описание
«Дата»	Дата и время входа пользователя на BPM
«Пользователь»	Имя пользователя, которому было выдано BPM
«IP-адрес»	IP-адрес инициатора сессии

Параметр	Описание
«Хост»	Наименование инициатора сессии
«Место»	Наименование BPM, выданного пользователю
«IP Места»	IP-адрес BPM, выданного пользователю
«ИД Места»	Идентификатор BPM, выданного пользователю
«Фонд»	Название фонда, в составе которого находится выданное BPM

Записи в списке поддерживают функцию множественного выбора и выполнения операций над несколькими объектами одновременно. Выполнить операцию над несколькими объектами можно только тогда, когда она допустима для всех выбранных объектов. Для выбора нескольких записей нужно зажать и удерживать клавиши **<CTRL>** или **<SHIFT>**.

8.9.2 . Фильтрация списка активных сессий

На странице со списком активных сессий доступна механика фильтрации (см. Рисунок 25). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Найти]**. Для сброса всех установленных параметров нужно нажать экранную кнопку **[Сбросить]**.

Подробное описание механики фильтрации списка сессий приведено в таблице (см. Таблица 37).

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку, фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 37 – Параметры фильтрации списка BPM

Атрибут	Условия	Значение
«Дата»	Формирование списка сессий: ▪ «В пределах» - в указанном временном промежутке; ▪ «Не в пределах» - исключая указанный временной промежуток	▪ «Минута»; ▪ «5 минут»; ▪ «30 минут»; ▪ «1 час»; ▪ «12 часов»; ▪ «24 часа»; ▪ «Сегодня»; ▪ «Эта неделя»; ▪ «Этот месяц»

Атрибут	Условия	Значение
«Пользователь»	Формирование списка сессий: ▪ «Является» - по указанному имени пользователя; ▪ «Не является» - исключая указанное имя пользователя; ▪ «Начинается с» - по начальной части имени пользователя; ▪ «Оканчивается на» - по конечной части имени пользователя; ▪ «Содержит» - включая указанную часть имени пользователя	Ручной ввод
«IP-адрес»	Формирование списка сессий: ▪ «Является» - по указанному IP-адресу инициатора сессии; ▪ «Не является» - исключая указанный IP-адрес инициатора сессии; ▪ «Начинается с» - по начальной части IP-адреса инициатора сессии; ▪ «Оканчивается на» - по конечной части IP-адреса инициатора сессии; ▪ «Содержит» - включая указанную часть IP-адреса инициатора сессии	Ручной ввод
«Хост»	Формирование списка сессий: ▪ «Является» - по указанному наименованию инициатора сессии; ▪ «Не является» - исключая указанное наименование инициатора сессии; ▪ «Начинается с» - по начальной части наименования инициатора сессии; ▪ «Оканчивается на» - по конечной части наименования инициатора сессии; ▪ «Содержит» - включая указанную часть наименования инициатора сессии	Ручной ввод
«Место»	Формирование списка сессий: ▪ «Является» - по указанному наименованию BPM, выданного пользователю; ▪ «Не является» - исключая указанное наименование BPM, выданного пользователю; ▪ «Начинается с» - по начальной части наименования BPM, выданного пользователю; ▪ «Оканчивается на» - по конечной части наименования BPM, выданного пользователю; ▪ «Содержит» - включая указанную часть наименования BPM, выданного пользователю	Ручной ввод
«IP Места»	Формирование списка сессий: ▪ «Является» - по указанному IP-адресу BPM, выданного пользователю; ▪ «Не является» - исключая указанный IP-адрес BPM, выданного пользователю; ▪ «Начинается с» - по начальной части IP-адреса BPM, выданного пользователю; ▪ «Оканчивается на» - по конечной части IP-адреса BPM, выданного пользователю; ▪ «Содержит» - включая указанную часть IP-адреса BPM, выданного пользователю	Ручной ввод

Атрибут	Условия	Значение
«ИД Места»	Формирование списка сессий: ▪ «Является» - по указанному идентификатору BPM, выданного пользователю; ▪ «Не является» - исключая указанный идентификатор BPM, выданного пользователю; ▪ «Начинается с» - по начальной части идентификатора BPM, выданного пользователю; ▪ «Оканчивается на» - по конечной части идентификатора BPM, выданного пользователю; ▪ «Содержит» - включая указанную часть идентификатора BPM, выданного пользователю	Ручной ввод
«Фонд»	Формирование списка сессий: ▪ «Является» - по указанному наименованию фонда, в котором находится BPM; ▪ «Не является» - исключая указанное наименование фонда, в котором находится BPM; ▪ «Начинается с» - по начальной части наименования фонда, в котором находится BPM; ▪ «Оканчивается на» - по конечной части наименования фонда, в котором находится BPM; ▪ «Содержит» - включая указанную часть наименования фонда, в котором находится BPM	Ручной ввод

8.10 . Настройка автоматического подключения к фонду BPM

8.10.1 . Автоматическое подключение к фонду BPM

Автоматическое подключение к фонду BPM позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер» и реализовать автоматическое подключение к опубликованным фондам BPM.

Для автоматического подключения к фонду BPM после настройки автоматического поиска сервера подключений на узле с установленным Termidesk следует перейти «Настройки - Системные параметры - Общие», активировать параметр «Автозапуск рабочего места» и нажать экранную кнопку **[Сохранить]**.

⚠ Для автоматического подключения к фонду BPM нужно настроить группы доступа к фондам BPM так, чтобы пользователям из каждой группы был доступен только один фонд. Если пользователь является членом нескольких групп, и каждой из этих групп предоставлен доступ к отдельному фонду BPM, то пользователь получает доступ к нескольким фондам одновременно. В таком случае, автоматическое подключение невыполнимо. При этом возможность ручного подключения сохраняется.

⚠ Для корректной работы автоматического подключения к фонду BPM необходимо выполнить настройку службы DNS.

8.10.2 . Настройка автоматического поиска в сети сервера Termidesk

Автоматический поиск сервера подключений позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер».

Для этого на DNS-сервере должна быть внесена одна из записей:

- либо запись `daas` типа `TXT` с URL-адресом сервера Termidesk, например: `https://termidesk.domain.local`;
- либо запись `vdi` типа `TXT` с URL-адресом сервера Termidesk, например: `https://termidesk.domain.local`.

8.11 . Режим техобслуживания фонда рабочих мест

8.11.1 . Режим техобслуживания фонда терминального сервера

Режим техобслуживания фонда - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в существующую сессию фонда терминального сервера. Этот режим предназначен для проведения плановых регламентных или аварийных работ: например, когда нужно применить обновления или исправления для терминального сервера и требуется временно прекратить новые подключения к фонду.

ⓘ Режим техобслуживания может применяться и к отдельному терминальному серверу в выбранном фонде (см. подраздел **Управление терминальными сессиями в назначенном фонде BPM**).

Для перевода фонда в режим техобслуживания следует перейти «Компоненты - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. Рисунок 30). Затем подтвердить включение режима.

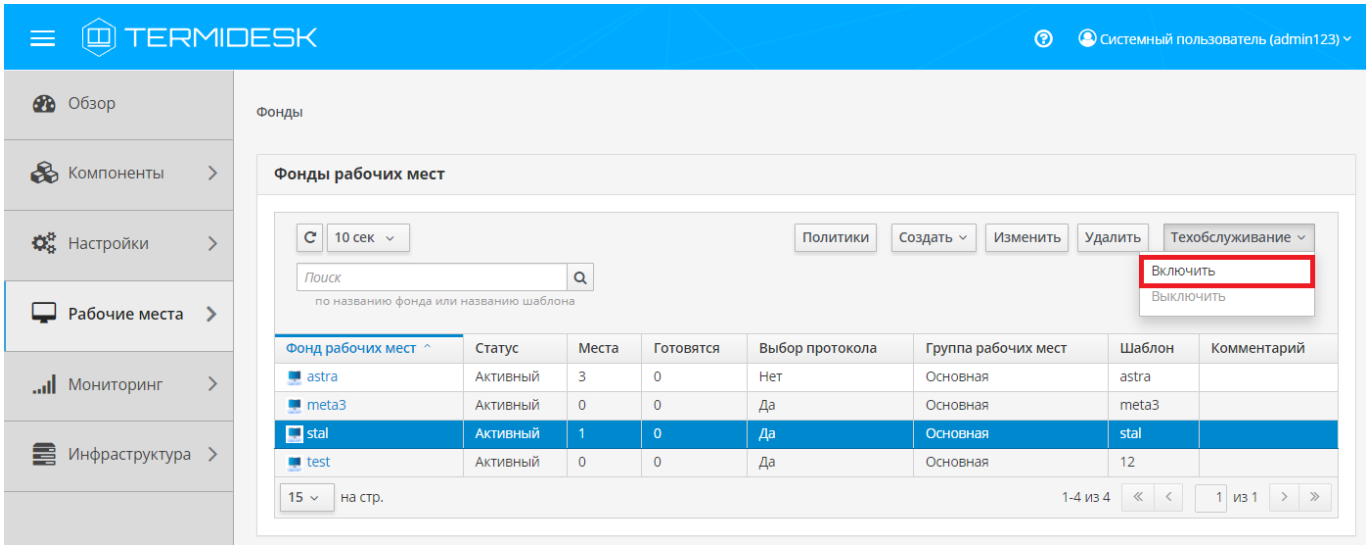

Рисунок 30 – Перевод фонда терминального сервера в режим техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Статус» списка фондов ВРМ.

Для отключения режима техобслуживания нужно выбрать фонд терминального сервера, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить». По завершении техобслуживания фонд может быть снова использован для размещения ВРМ (терминальных сессий).

9 . ПРОТОКОЛЫ ДОСТАВКИ

9.1 . Общие сведения о протоколах доставки

Протокол доставки – это поддерживаемый в Termidesk протокол удаленного доступа к ВРМ. Протоколы доставки обеспечивают передачу экрана ВРМ на пользовательскую рабочую станцию.
Доставка экрана ВРМ может быть выполнена как напрямую, так и через компонент «Шлюз».
Для добавления протокола доставки следует перейти «Компоненты - Протоколы доставки», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка поддерживаемый протокол и способ доставки.
Добавленные протоколы можно редактировать, для этого нужно пометить протокол и после нажать экранную кнопку **[Изменить]**.
Добавленные ранее протоколы можно удалить, для этого нужно пометить протокол и после нажать экранную кнопку **[Удалить]**.

⚠ Протокол доставки может быть удален только в том случае, если он не используется фондом ВРМ.

9.2 . Подключения по протоколу RDP для доступа к ресурсам серверов терминалов

9.2.1 . Подключение по протоколу RDP для доступа к ресурсам сервера терминалов

Для добавления подключения для доступа к MS RDS или STAL администратору Termidesk необходимо перейти «Компоненты - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «RDP (терминальный доступ)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 38).

Таблица 38 – Данные для добавления прямого подключения к серверам терминалов

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ
«URL шлюза»	Адрес «Шлюза» в формате `ws(s)://192.0.2.30:5099`, обеспечивающего формирование и поддержание соединения. Директива `ws` относится к использованию порта 80, директива `wss` означает использование 443 порта. Параметр `192.0.2.30` - доступный IP-адрес «Шлюза». Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре организации. Значение этого параметра не относится к значению `WSPROXY_BIND_ADDRESS` из конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`

Параметр	Описание
«Время ожидания соединения»	Время ожидания (в секундах) отклика «Шлюза». При прямом соединении (не через «Шлюз») можно оставить значение по умолчанию, т.к. параметр не будет оказывать влияния на подключение
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Разрешить смарт-карты»	Разрешить идентификацию субъектов на основе смарт-карт
«Разрешить принтеры»	Разрешить перенаправление устройств печати по протоколу RDP
«Разрешить диски»	Разрешить перенаправление устройств хранения по протоколу RDP
«Разрешить последовательные порты»	Разрешить перенаправление последовательных портов по протоколу RDP
«Показывать обои»	Отображать фоновое изображение, настроенное на рабочем столе
«Разрешить композицию рабочего стола»	Разрешить темы рабочего стола
«Сглаживание шрифтов»	Использовать технологию сглаживания шрифтов
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Использовать ALSA»	Использовать программный микшер для передачи звука
«Параметры смарт-карты»	Указать конфигурацию идентификации по смарт-картам
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«RemoteFX»	Использовать технологию RemoteFX
«Все RemoteFX устройства»	Использовать все RemoteFX устройства
«Динамическое разрешение»	Разрешить передачу динамического разрешения для экрана рабочего стола ⚠ Параметр должен быть отключен при реализации доступа к STAL с рабочей станции пользователя на ОС Microsoft Windows 11.
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Выбрать диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к BPM. Указанные диапазоны должны быть созданы в «Компоненты - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к BPM

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

9.2.2 . Подключение по протоколу RDP для доступа к ресурсам сервера терминалов через компонент «Шлюз»

Начиная с Termidesk версии 5.0 подключение к ресурсам сервера терминалов через «Шлюз» настраивается при выборе протокола «RDP (терминальный доступ)».

10 . СИСТЕМНЫЕ НАСТРОЙКИ

10.1 . Общие системные параметры Termidesk

Системные параметры позволяют задать основные значения, необходимые для успешного функционирования Termidesk.

Для конфигурации общих системных параметров следует перейти «Настройки - Системные параметры - Общие».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 38).

⚠ Изменение системных параметров вступают в силу только после перезагрузки Termidesk.

Таблица 39 – Общие системные параметры Termidesk

Параметр	Описание
«Генератор имен»	Варианты использования имен при развертывании BPM. Значение по умолчанию: «С переиспользованием имен»
«Тема оформления»	Выбор темы оформления графического интерфейса пользователя и управления
«Действие с учетной записью рабочего места»	Выбор действия, которое будет произведено над учетной записью BPM на сервере каталогов (в домене аутентификации) при удалении BPM из фонда. В текущей версии параметр применим только к домену аутентификации MS AD. Также требуется, чтобы на узле «Универсального диспетчера» в качестве DNS-сервера был указан сервер MS AD. Возможные значения: ▪ «Удалить при удалении фонда» (по умолчанию) - при удалении BPM из фонда учетная запись будет удалена из домена аутентификации; ▪ «Сбросить пароль при удалении фонда» - при удалении BPM из фонда у учетной записи будет сброшен пароль. В текущей версии этот вариант выбирать не следует, он приведен для справки; ▪ «Выключить при удалении фонда» - при удалении BPM из фонда учетная запись будет отключена в домене аутентификации; ▪ «Хранить при удалении фонда» - при удалении BPM из фонда учетная запись будет сохранена в домене аутентификации. Следует учесть, что при вводе гостевой ОС в домен MS AD: ▪ если учетная запись BPM находится не в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN); ▪ если учетная запись BPM находится в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «CN=Computers,DC=domain,DC=local», т.е. должен использоваться Common Name (CN)

Параметр	Описание
«Автозапуск рабочего места»	Параметр автоматического подключения к фонду BPM через компонент «Клиент» (см. подраздел **Настройка автоматического подключения к фонду BPM**). Значение по умолчанию: «Нет»
«Подключаться к BPM по»	Параметр определяет, какое значение в параметрах подключения к BPM «Универсальный диспетчер» должен передать компоненту «Клиент». Возможные значения: ▪ «Сетевому адресу (IP)» - в параметрах подключения будет передаваться IP-адрес BPM; ▪ «Полному доменному имени (FQDN)» - в параметрах подключения будет передаваться FQDN BPM. Действие параметра не распространяется на протокол подключения к терминальному серверу - при таком подключении всегда передается IP-адрес
«Интервал проверок кэша рабочих мест»	Период (в секундах) опроса ВМ в фонде BPM для определения статуса их готовности. Значение по умолчанию: «19»
«Интервал проверок неиспользуемых рабочих мест»	Период (в секундах) проверки наличия неактивных BPM для последующего их удаления. Для удаления неиспользуемых рабочих мест требуется задать значение «Удалять рабочее место» для политики «Действие при выходе пользователя из ОС». Значение по умолчанию: «631»
«Интервал очистки информационных объектов»	Период (в секундах) поиска информации о фондах BPM в статусе «Удален», «Отменен», «Ошибка» для ее дальнейшей очистки. Очистка производится после истечения времени, заданного в параметре «Время хранения информационных объектов». Значение по умолчанию: «3607»
«Количество потоков фоновых задач»	Количество одновременных задач, выполняемых «Менеджером рабочих мест» в фоновом процессе. Значение по умолчанию: «4»
«Не учитывать максимальные ограничения»	Не учитывать ограничения, заданные в полях «Подготавливать ВМ одновременно» и «Удалять ВМ одновременно» поставщика ресурсов при формировании фондов BPM. Если параметр активен, в фонде одновременно может создаваться и удаляться до 1000 ВМ. Значение по умолчанию: «Нет»
«Время хранения информационных объектов»	Время хранения (в секундах) информации о фондах BPM в статусе «Удален», «Отменен», «Ошибка». Значение по умолчанию: «14401»
«Время блокировки входа»	Время (в секундах) после истечения которого будет возможен повторный вход субъекта «Администратор», «Персонал» или «Пользователь» в случае превышения субъектом лимита неудачных попыток входа. Значение по умолчанию: «300»
«URL входа»	URL-адрес начальной страницы графического интерфейса управления ⚠ Значение параметра менять не следует. Значение по умолчанию: «/login»

Параметр	Описание
«Максимальное время инициализации рабочего места»	Максимальное время (в секундах) ожидания готовности ВРМ, после истечения которого ВМ будет удалена как зависшая. Значение по умолчанию: «3601»
«Максимум записей в журнале для объектов»	Максимальное количество системных событий, добавляемых в журнал объекта. Значение по умолчанию: «100»
«Интервал проверки для удаления объектов»	Период проверки (в секундах) ВРМ, помеченных для удаления. Значение по умолчанию: «31»
«Количество ошибок для ограничения фонда»	Пороговое значение количества ошибок, после которого фонд ВРМ будет переведен в статус «Ограниченный». Значение по умолчанию: «3»
«Интервал отслеживания ошибок в фонде»	Период появления ошибок (в секундах), связанных с функционированием фонда ВРМ. Значение по умолчанию: «600»
«Количество потоков планировщика задач»	Пороговое значение потоков задач, выполняемых «Менеджером рабочих мест», при обеспечении жизненного цикла фонда ВРМ. Значение по умолчанию: «3»
«Срок действия устаревшей публикации»	Время (в часах), по истечении которого ВМ будет удалена, если публикация фонда ВРМ объявлена устаревшей. При обновлении параметра его значение применяется к новым публикациям. Для публикаций, созданных до изменения параметра, будет действовать предыдущее значение параметра. При указании отрицательного значения ВМ будут удалены немедленно, если публикация фонда ВРМ объявлена устаревшей. Значение по умолчанию: «24»
«Срок хранения статистики»	Время (в днях) хранения файлов журналов, по истечению которого журналы будут перезаписаны. Значение по умолчанию: «365»
«Количество удаляемых рабочих мест за один проход»	Максимальное количество ВРМ, удаляемых единовременно из фонда ВРМ. Значение по умолчанию: «3»

Экранная кнопка **[Сохранить]** сохраняет общие системные параметры.

10.2 . Параметры безопасности Termidesk

Для конфигурации системных параметров безопасности следует перейти «Настройки - Системные параметры - Безопасность».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей Настройка параметров безопасности в Termidesk.

Таблица 40 – Параметры безопасности Termidesk

Параметр	Описание
«Мастер-ключ»	Идентификатор регистрации субъектов в Termidesk при доступе к фонду ВРМ
«Доверенные хосты»	Идентификатор узлов, имеющих право подключаться к Termidesk

Параметр	Описание
«Длительность сессии администратора»	Временной интервал сессии, инициированной на «Портале администратора»
«Доступ к веб-части системным пользователем»	Возможность администратора подключаться к «Порталу администратора»
«Использовать анонсируемый IP клиента»	Использовать IP-адрес клиента, передаваемый в процессе входа в Termidesk
«GID системной группы администратора»	Идентификатор группы, в которую входит учетная запись администратора
«Длительность сессии пользователя»	Временной интервал (в секундах) сессии пользователя. Параметр влияет на длительность сессии пользователя в «Портале пользователя». Начиная с Termidesk версии 5.0 параметр также определяет общее время подключения пользователя к «Универсальному диспетчеру» Termidesk. Вне зависимости от того, активен пользователь или нет, каждую секунду происходит уменьшение значения параметра на 1, при достижении значения 0 подключение пользователя завершится, при этом на пользовательской рабочей станции, в системном трее, отобразится уведомление от приложения «Клиент»: «Ваш сеанс завершился». В журнале «Клиента» отражаются события как получения параметра («userSessionLength»), так и завершения сессии по таймауту
«Максимум попыток входа Администраторов»	Пороговое положительное значение числа неудачных попыток входа администратора. Параметр может быть изменен только администратором (см. **Назначение служебных функций администраторам**). Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Персонала»	Пороговое положительное значение числа неудачных попыток входа субъектов, не относящихся к администратору. Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Пользователей»	Пороговое положительное значение числа неудачных попыток входа пользователей. Значение «0» эквивалентно «без ограничений»

10.3 . Утилиты интерфейса командной строки для настройки Termidesk

10.3.1 . Утилита termidesk-config

Утилита `termidesk-config` используется для переопределения настроек, заданных на этапе установки Termidesk.

Для вызова утилиты следует:

- в интерфейсе командной строки перейти в каталог `/opt/termidesk/sbin/`:

```
:~$ cd /opt/termidesk/sbin/
```

- выполнить запуск командой:

```
:~$ sudo ./termidesk-config
```

- откроется интерфейс утилиты (см. Рисунок 31).

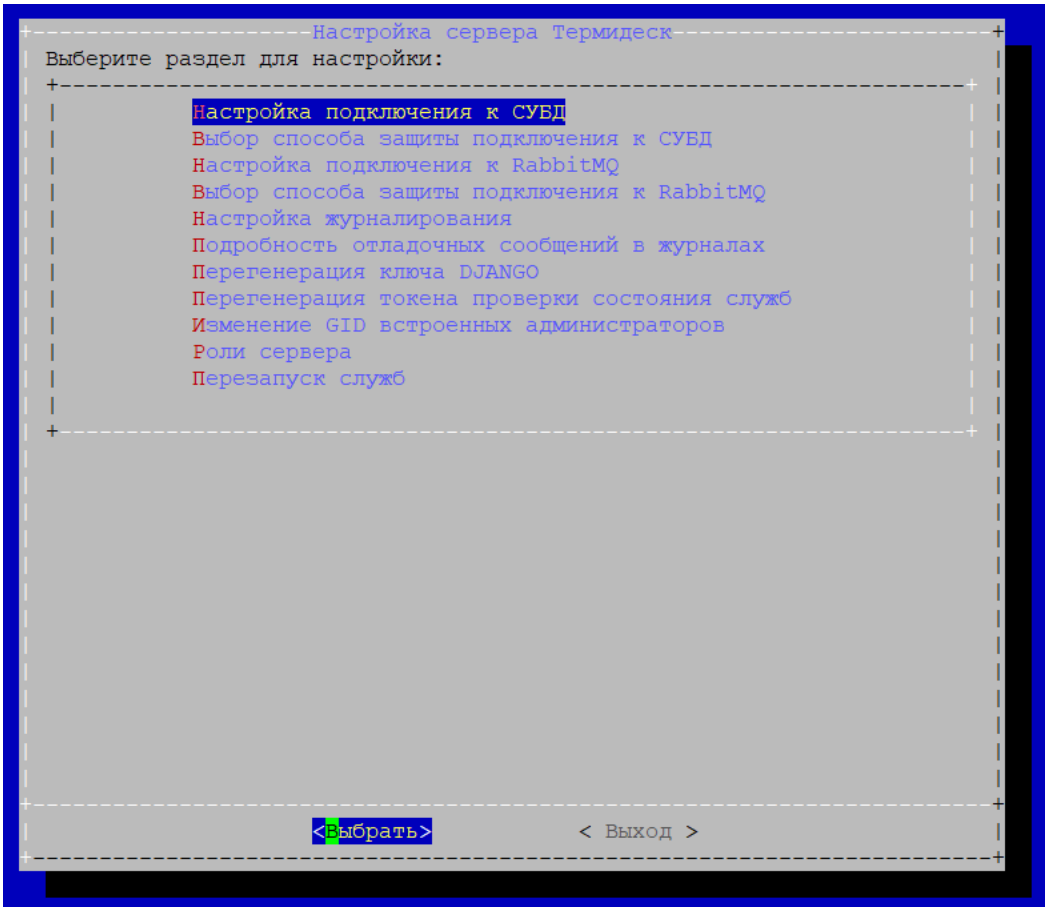

Рисунок 31 – Интерфейс утилиты termidesk-config

Доступны следующие функции утилиты:

- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД;
- «Выбор способа защиты подключения к СУБД»: позволяет выбрать защищенный протокол при подключении к СУБД;
- «Настройка подключения к RabbitMQ»: позволяет настроить параметры подключения к RabbitMQ;
- «Выбор способа защиты подключения к RabbitMQ»: позволяет выбрать защищенный протокол при подключении к RabbitMQ;
- «Настройка журналирования»: позволяет настроить параметры журналирования, такие как «Адрес логгера» (переменная окружения `LOG_ADDRESS`), «Поток (facility) журнала» (переменная окружения `LOG_FACILITY`);
- «Подробность отладочных сообщений в журналах»: позволяет выбрать уровень подробности отладочных сообщений (переменная окружения `LOG_LEVEL`);
- «Перегенерация ключа DJANGO»: позволяет переопределить значение ключа DJANDO (переменная окружения `DJANGO_SECRET_KEY`), который генерируется на этапе установки Termidesk. Переопределение ключа может понадобиться при его компрометации;

- «Перегенерация токена проверки состояния служб»: позволяет переопределить значение токена проверки состояния служб (переменная окружения `HEALTH_CHECK_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Изменение GID встроенных администраторов»: позволяет назначить идентификатор группы, использующегося для встроенного домена. Изменение идентификатора может понадобиться, если встроенная в ОС группа администраторов отличается от `astra-admin (1001)` или если нужно предоставить права администрирования Termidesk группе непривилегированных пользователей;
- «Роли сервера»: позволяет изменить роли, которые запускаются на узле. Доступные роли: «Портал администратора», «Портал пользователя», «Менеджер рабочих мест»;
- «Перезапуск служб»: позволяет выполнить перезапуск служб Termidesk.

После выполнения изменений в любом из разделов рекомендуется воспользоваться пунктом «Перезапуск служб» для применения изменений.

10.3.2 . Утилита termidesk-vdi-manage

Утилита `termidesk-vdi-manage` используется для настройки Termidesk из интерфейса командной строки.

Для вызова утилиты следует:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
:~$ sudo -u termidesk bash
```

- вывести список команд утилиты:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage help
```

Каждая подкоманда в приведенных ниже командах поддерживает вывод справки через ключ `-h`.
Для управления параметрами поставщиков ресурсов, доменов аутентификации, протоколов доставки и других компонентов, настраиваемых через «Портал администратора» Termidesk, следует обратиться к командам секции `[termidesk]`.

Большая часть команд из вывода `/opt/termidesk/sbin/termidesk-vdi-manage help` предназначена для работы с БД и фреймворком Django и не приведена здесь.

Команды секции `[termidesk]` приведены в таблице (см. Таблица 41).

Таблица 41 – Команды секции [termidesk]

Параметр	Описание
`drop_tables`	Удаляет таблицы из БД. Для просмотра списка ключей следует воспользоваться аргументом `-h`: `/opt/termidesk/sbin/termidesk-vdi-manage drop_tables -h` Поддерживаются аргументы: ▪ `--noinput`, `--no-input` - сообщает Django НЕ запрашивать у пользователя ввод; ▪ `-R <МАРШРУТИЗАТОР>`, `--router <МАРШРУТИЗАТОР>` - использование указанного маршрутизатора БД вместо того, который определен в настройках `settings.py`; ▪ `-S <СХЕМА>`, `--schema <СХЕМА>` - удаление указанной схемы вместо `public`; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
tdsk_auth	Создает домен аутентификации. Для просмотра списка ключей следует воспользоваться аргументом -h: /opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth -h Поддерживаются аргументы: ▪ --version - вывод версии программы; ▪ -v {0,1,2,3}, --verbosity {0,1,2,3} - уровень детализации сообщений; ▪ --settings <настройки> - путь к модулю настроек Python; ▪ --pythonpath <каталог Python> - каталог, который нужно добавить в путь Python, например /home/djangoprojects/myproject; ▪ --traceback - вызов исключений; ▪ --no-color - вывод команды без подсвечивания; ▪ --force-color - вывод команды с принудительным подсвечиванием; ▪ --skip-checks - пропуск проверки системы. Поддерживаются подкоманды: ▪ create - создание домена аутентификации; ▪ list - вывод списка доменов аутентификации; ▪ remove - удаление домена аутентификации; ▪ login - аутентификация в указанный домен; ▪ logout - завершение сессии. Подкоманда create принимает аргументы: ▪ --type - задание типа домена аутентификации. Доступны: ALDAuthenticatorPlugin («Astra Linux Directory»), IPAuth («IP аутентификация»), KerberosAuthenticatorPlugin («FreeIPA»), SAMLAuthenticator («SAML»), SimpleLdapAuthenticator («MS Active Directory (LDAP)»); ▪ --params - задание параметров домена аутентификации. Формат: имя1=значение1 имя2=значение2 и т.д. Доступные параметры для указанного типа домена аутентификации можно получить через команду --list , например: /opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth create --type KerberosAuthenticatorPlugin --name test --small_name test--list --test; ▪ --list - вывод параметров домена аутентификации; ▪ --test - проверка параметров без создания домена аутентификации; ▪ --quiet - вывод только сообщений об ошибках; ▪ --name <ИМЯ> - имя домена аутентификации; ▪ --small_name <короткое имя> - короткое имя домена аутентификации. Допустимые символы: a-z, A-Z, 0-9. Максимальная длина 32 символа; ▪ --priority <приоритет> - числовое значение приоритета домена аутентификации, по умолчанию «1»; ▪ --comments <комментарий> - комментарий к создаваемому домену. Подкоманда list принимает аргумент --output json для вывода списка в формате json. Подкоманда remove принимает аргументы: ▪ --output json - вывод параметров в формате json; ▪ --silent - «тихое» удаление для выполнения команды из исполняемого файла; ▪ --uuid <идентификатор> - идентификатор объекта для удаления. Подкоманда login принимает аргументы: ▪ --uuid <идентификатор> - идентификатор объекта для аутентификации; ▪ --small_name <короткое имя> - короткое имя домена аутентификации;

Параметр	Описание
	▪ `--output json` - вывод параметров в формате `json` Подкоманда `logout` принимает аргументы: ▪ `--token <токен>` - токен сессии пользователя; ▪ `--output json` - вывод параметров в формате `json`
`tdsk_clearsessions`	Порционная очистка сессий. Поддерживаются аргументы: ▪ `-chunk <количество>` - количество сессий для удаления, по умолчанию 1000; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы
`tdsk_config`	Работа с системными настройками. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `list` - вывод конфигурационных параметров и их значений; ▪ `set` - установка значения конфигурационному параметру. Подкоманда `set` принимает аргументы: ▪ `--section` - секция параметра из доступных: `Security`, `IPAUTH`, `Global`, `Monitoring`, `Experimental`, `Notifications`, `Audit`; ▪ `--key <ключ>` - ключ параметра; ▪ `--value <значение>` - значение параметра

Параметр	Описание
`tdsk_exp_2fa_add_statictoken`	Добавление токена пользователю. Поддерживаются аргументы: ▪ `username` - имя пользователя, с которым будет ассоциирован токен; ▪ `-t <токен>`, `--token <токен>` - токен, который нужно добавить. Если этот параметр пропущен, он будет сгенерирован случайным образом; ▪ `--auth_uuid <идентификатор>` - идентификатор домена аутентификации; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы
`tdsk_exp_2fa_clear_totpdevice`	Удаление TOTP-устройства пользователя. Поддерживаются аргументы: ▪ `username` - имя пользователя, которому нужно удалить TOTP-устройство; ▪ `--auth_uuid <идентификатор>` - идентификатор домена аутентификации; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
`tdsk_graph_models`	Создание файла GraphViz с описанием моделей БД для указанных имен приложений. Можно передать несколько имен приложений, и все они будут объединены в одну модель. Пример использования команды приведен в подразделе **Генерация отчета по моделям данных и структурам БД Termidesk**. Поддерживаются аргументы: ▪ `app_label` - наименование приложения; ▪ `--pygraphviz` - использование PyGraphViz для создания изображения; ▪ `--pydot` - использование PyDot(Plus) для создания изображения; ▪ `--disable-fields`, `-d` - не показывать поля; ▪ `--group-models`, `-g` - сгруппировать модели в соответствии с их применением; ▪ `--all-applications`, `-a` - включить все приложения для вывода модели; ▪ `--output <путь к файлу>`, `-o <путь к файлу>` - запись вывода в файл; ▪ `--layout <макет>`, `-l <макет>` - использование макета GraphViz для визуализации. Поддерживаются: `circo`, `dot`, `fdpneato`, `nop`, `nop1`, `nop2`, `twopi`; ▪ `--verbose-names`, `-n` - использование подробных имен для моделей и полей; ▪ `--language <локализация>`, `-L <локализация>` - указания языка, который будет использоваться для подробных имен; ▪ `--exclude-columns <столбцы>`, `-x <столбцы>` - исключение определенных столбцов; ▪ `--exclude-models <модели>`, `-X <модели>` - исключение определенных моделей; ▪ `--include-models <модели>`, `-I <модели>` - ограничение только указанными моделями; ▪ `--inheritance`, `-e` - включение наследования (используется по умолчанию); ▪ `--no-inheritance`, `-E` - выключение наследования; ▪ `--hide-relations-from-fields`, `-R` - ▪ `--disable-sort-fields`, `-S` - ▪ `--json` - вывод в формат `json`; ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы

Параметр	Описание
`tdsk_group`	Создание группы BPM. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманда `create` (создание группы рабочих мест) со следующими аргументами: ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - имя создаваемой группы; ▪ `--comments <комментарий>` - комментарий к создаваемой группе; ▪ `--priority <приоритет>` - числовое значение приоритета группы
`tdsk_license`	Управление лицензией Termidesk. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `install` - установить лицензию из файла, поддерживается относительный или абсолютный путь к файлу. Пример команды для установки лицензии: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license install <путь к файлу лицензии>`; ▪ `show` - вывести информацию об установленной лицензии. Для вывода в формате json следует использовать аргумент `--output`: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license show --output json`

Параметр	Описание
`tdsk_net`	Создание сети. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживается подкоманда `create` (создание сети) со следующими аргументами: ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - имя создаваемой сети; ▪ `--netRange <диапазон>` - диапазон IP-адресов. Допустимы различные форматы, например: A.B.C.*, A.B.C.D/N, A.B.C.D - E.F.G.D
`tdsk_osm`	Создание параметров гостевой ОС. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживается подкоманда `create` (создание параметров гостевой ОС) со следующими аргументами: ▪ `--params` - задание параметров гостевой ОС. Формат: `имя1=значение1 имя2=значение2` и т.д.; ▪ `--list` - вывод параметров гостевой ОС; ▪ `--test` - проверка параметров без создания объекта; ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <ИМЯ>` - наименование параметров гостевой ОС; ▪ `--comments <комментарий>` - комментарий к создаваемым параметрам

Параметр	Описание
`tdsk_pool`	Управление фондами ВРМ. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `create` - создание фонда ВРМ; ▪ `list` - вывод списка фондов ВРМ. Подкоманда `create` принимает аргументы: ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <ИМЯ>` - имя фонда ВРМ; ▪ `--comments <комментарий>` - комментарий к создаваемому фонду ВРМ; ▪ `--service_id <идентификатор>` - указание идентификатора шаблона ВРМ; ▪ `--osmanager_id <идентификатор>` - указание идентификатора параметров гостевой ОС ВРМ; ▪ `--image_id <идентификатор>` - указание идентификатора изображения гостевой ОС; ▪ `--servicesPoolGroup_id <идентификатор>` - указание идентификатора группы ВРМ; ▪ `--cache_l1_srvs <значение>` - количество ВРМ в кеше 1-го уровня; ▪ `--cache_l2_srvs <значение>` - количество ВРМ в кеше 2-го уровня; ▪ `--max_srvs <значение>` - максимальное количество ВРМ. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате `json`

Параметр	Описание
`tdsk_prov`	Управление поставщиками ресурсов. Поддерживаются аргументы: ▪ `--version` - вывод версии программы; ▪ `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений; ▪ `--settings <настройки>` - путь к модулю настроек Python; ▪ `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`; ▪ `--traceback` - вызов исключений; ▪ `--no-color` - вывод команды без подсвечивания; ▪ `--force-color` - вывод команды с принудительным подсвечиванием; ▪ `--skip-checks` - пропуск проверки системы. Поддерживаются подкоманды: ▪ `create` - создание поставщика ресурсов; ▪ `list` - вывод списка поставщиков ресурсов. Подкоманда `create` принимает аргументы: ▪ `--type` - задание типа поставщика ресурсов. Доступны: `RedVirtPlatform` («Платформа RED Virtualization»), `SessionsPlatform` («Сервер Терминалов [экспериментальный]»), `VMmanagerPlatform` («Платформа VMmanager»), `oVirtPlatform` («Платформа oVirt/RHEV»), `pksvbrestPlatform` («ПК СВ Брест»), `vmwarePlatform` («Платформа VMware»), `zVirtPlatform` («Платформа zVirt»); ▪ `--params` - задание параметров поставщика ресурсов. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа поставщика ресурсов можно получить через команду `--list` , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_prov create --type RedVirtPlatform --name test --list --test` ; ▪ `--list` - вывод параметров поставщика ресурсов; ▪ `--test` - проверка параметров без создания поставщика ресурсов; ▪ `--quiet` - вывод только сообщений об ошибках; ▪ `--name <имя>` - наименование поставщика ресурсов; ▪ `--comments <комментарий>` - комментарий к создаваемому поставщику ресурсов. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате `json`

Параметр	Описание
tdsk_trans	Управление протоколами доставки. Поддерживаются аргументы: ▪ --version - вывод версии программы; ▪ -v {0,1,2,3}, --verbosity {0,1,2,3} - уровень детализации сообщений; ▪ --settings <настройки> - путь к модулю настроек Python; ▪ --pythonpath <каталог Python> - каталог, который нужно добавить в путь Python, например /home/djangoprojects/myproject; ▪ --traceback - вызов исключений; ▪ --no-color - вывод команды без подсвечивания; ▪ --force-color - вывод команды с принудительным подсвечиванием; ▪ --skip-checks - пропуск проверки системы. Поддерживаются подкоманды: ▪ create - добавление протокола доставки; ▪ list - вывод списка протоколов доставки; ▪ remove - удалить протокол доставки; ▪ convert - конвертировать протокол доставки (RDSTransport, RDSWSTRDPTransport, STALTransport, STALWSTRDPTransport) в новый протокол TerminalTransport. Подкоманда create принимает аргументы: ▪ --type - задание типа протокола. Доступны: HTML5Transport («SPICE (HTML5, через локальный прокси)»), HTML5VNCTransport («VNC (HTML5, через локальный прокси)»), LoudplayDirectTransport («Loudplay (напрямую, эксперим.)»), LoudplayTunneledTransport («Loudplay (через вебсокет шлюз, эксперим.)»), RDPTransport («RDP (напрямую)»), RDSTransport («Доступ к MS RDS по RDP (напрямую) [экспериментальный]»), RDSWSTRDPTransport («Доступ к MS RDS по RDP (через шлюз) [экспериментальный]»), STALTransport («Доступ к STAL по RDP (напрямую) [экспериментальный]»), STALWSTRDPTransport («Доступ к STAL по RDP (через шлюз) [экспериментальный]»), TDSKSPICETransport («SPICE (vdi-viewer, эксперим.)»), WSTRDPTransport («RDP (через вебсокет шлюз)»), TERATransport («TERA [экспериментальный]»), TerminalTransport («RDP (терминальный доступ)»); ▪ --params - задание параметров протокола доставки. Формат: имя1=значение1 имя2=значение2 и т.д. Доступные параметры для указанного типа протокола доставки можно получить через команду --list, например: /opt/termidesk/sbin/termidesk-vdi-manage tdsk_trans create --type RDPTransport --name test --list; ▪ --list - вывод параметров протокола доставки; ▪ --test - проверка параметров без создания протокола доставки; ▪ --quiet - вывод только сообщений об ошибках; ▪ --name <имя> - наименование протокола доставки; ▪ --comments <комментарий> - комментарий к создаваемому протоколу доставки; ▪ --priority <приоритет> - числовое значение приоритета протокола доставки; ▪ --allowed_oss <перечень ОС> - перечень разрешенных ОС из списка: Android, CrOS, FreeBSD, iPad, iPhone, Linux, Mac, Windows, Windows Phone. Формат: имя1,имя2,имя3; ▪ --nets_positive <yes/no> - указание, что протокол должен быть доступен только из сетей, указанных в параметре --networks. Может принимать значения не только yes или no, подходит в целом любое непустое значение;

Параметр	Описание
	▪ `--networks <наименования сетей>` - перечень сетей, доступ из которых разрешен для создаваемого протокола доставки. Формат: `имя1,имя2,имя3`. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате `json`. Подкоманда `create` принимает аргументы: ▪ `--output json` - вывод списка в формате `json`; ▪ `--silent` - выполнение в «тихом» режиме; ▪ `--uuid <идентификатор>` - идентификатор объекта для удаления. Подкоманда `convert` принимает аргументы: ▪ `--uuid <идентификатор>` - идентификатор протокола доставки, который необходимо конвертировать (`RDSTransport`, `RDSWSTRDPTransport`, `STALTransport`, `STALWSTRDPTransport`); ▪ `--all` - ковернтировать все протоколы доставки RDS и STAL.
`tdsk_version`	Получение версии Termidesk

10.4 . Назначение служебных функций администраторам

В Termidesk для администраторов реализовано разделение доступных служебных функций.

Для назначения доступных служебных функций следует перейти «Настройки - Управление ролями» и нажать экранную кнопку [Создать] (см. Рисунок 32).

При добавлении функции необходимо ввести текстовое наименование создаваемого класса администратора, а также выбрать список назначаемых разрешений.

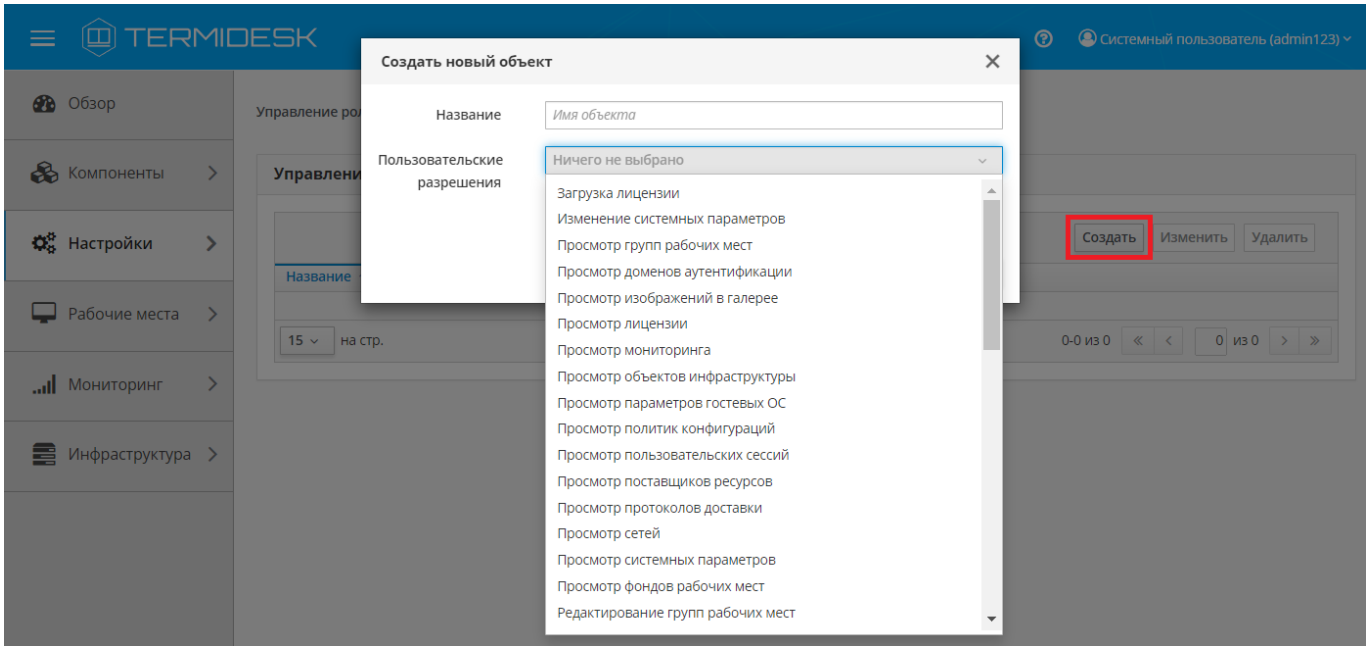

Рисунок 32 – Окно назначения пользовательских разрешений

Список разрешений для назначения служебных функций администраторам перечислен в столбце «Разрешение» следующей таблицы (см. Таблица 42).

⚠ Перед назначением разрешения на редактирование, создание, удаление или управление необходимо предоставить соответствующее разрешение на просмотр страницы.

Таблица 42 – Список доступных для выбора разрешений

Разрешение	Описание
«Загрузка лицензии»	Разрешение позволяет загружать лицензии на странице «Настройки - Лицензия» на вкладке «Загрузка»
«Изменение системных параметров»	Разрешение позволяет управлять системными параметрами на странице «Настройки - Системные параметры»
«Просмотр групп рабочих мест»	Предоставляет доступ на чтение страницы «Настройки - Группы рабочих мест» для просмотра списка созданных групп BPM
«Просмотр доменов аутентификации»	Предоставляет доступ на чтение страницы «Компоненты - Домены аутентификации». Разрешение позволяет выполнять просмотр: ▪ пользователей домена, назначенных им групп, BPM, BM и журнал; ▪ списка групп домена и пользователей, входящих в каждую группу; ▪ журнала
«Просмотр изображений в галерее»	Предоставляет доступ на чтение страницы «Настройки - Галерея» для просмотра списка загруженных изображений
«Просмотр лицензии»	Предоставляет доступ на чтение страницы «Настройки - Лицензия» для просмотра информации о лицензии и системе
«Просмотр мониторинга»	Предоставляет доступ на чтение страницы «Мониторинг». Разрешение позволяет выполнять просмотр: ▪ раздела «Журналы», экспорт записей в формате `.CSV`; ▪ раздела «Аудит», экспорт записей в формате `.CSV`; ▪ раздела «Отчёты», создание, редактирование, удаление отчетов, экспорт записей в формате `.CSV`
«Просмотр объектов инфраструктуры»	Предоставляет доступ на чтение страниц раздела «Инфраструктура» для просмотра информации о статусе компонентов Termidesk
«Просмотр параметров гостевых ОС»	Предоставляет доступ на чтение страницы «Компоненты - Параметры гостевых ОС» для просмотра списка созданных параметров гостевых ОС
«Просмотр политик конфигураций»	Предоставляет доступ на чтение страницы «Настройки - Глобальные политики» для просмотра значений параметров политик
«Просмотр пользовательских сессий»	Предоставляет доступ на чтение страницы «Рабочие места - Сессии» для просмотра списка активных сессий пользователей
«Просмотр поставщиков ресурсов»	Предоставляет доступ на чтение страницы «Компоненты - Поставщики ресурсов». Разрешение позволяет выполнять просмотр: ▪ списка созданных поставщиков ресурсов; ▪ списка созданных шаблонов BPM
«Просмотр протоколов доставки»	Предоставляет доступ на чтение страницы «Компоненты - Протоколы доставки» для просмотра списка созданных протоколов доставки

Разрешение	Описание
«Просмотр сетей»	Предоставляет доступ на чтение страницы «Компоненты - Сети» для просмотра списка созданных сетей
«Просмотр системных параметров»	Предоставляет доступ на чтение страницы «Настройки - Системные параметры» для просмотра заданных системных параметров
«Просмотр фондов рабочих мест»	Предоставляет доступ на чтение страницы «Рабочие места - Фонды». Разрешение позволяет выполнять: ▪ просмотр раздела «Фонды» и выполнять действия в разделе: • просматривать список опубликованных фондов BPM; • просматривать вкладки «Рабочие места», «Пользователи и группы», «Протоколы доставки», «Журнал» при выборе опубликованного фонда BPM; ▪ просмотр раздела «Индивидуальные рабочие места» для просмотра информации о назначенных ВМ
«Редактирование групп рабочих мест»	Разрешение позволяет редактировать параметры созданных групп BPM
«Редактирование доменов аутентификации»	Разрешение позволяет редактировать параметры созданных доменов аутентификации
«Редактирование изображений в галерее»	Разрешение позволяет редактировать параметры загруженных изображений в галерее
«Редактирование параметров гостевых ОС»	Разрешение позволяет редактировать созданные параметры гостевых ОС
«Редактирование политик конфигураций»	Разрешение позволяет выполнять: ▪ редактирование политик; ▪ сброс значения политики
«Редактирование поставщика ресурсов»	Разрешение позволяет редактировать параметры созданных поставщиков ресурсов
«Редактирование протоколов доставки»	Разрешение позволяет редактировать параметры созданных протоколов доставки
«Редактирование сетей»	Разрешение позволяет редактировать параметры созданных сетей
«Редактирование фондов рабочих мест»	Разрешение позволяет редактировать параметры: ▪ созданных фондов BPM; ▪ индивидуальных рабочих мест
«Создание групп рабочих мест»	Разрешение позволяет создавать группы BPM
«Создание доменов аутентификации»	Разрешение позволяет добавлять домены аутентификации
«Создание изображений в галерее»	Разрешение позволяет загружать изображения в галерею
«Создание параметров гостевых ОС»	Разрешение позволяет создавать параметры гостевых ОС
«Создание поставщика ресурсов»	Разрешение позволяет добавлять поставщиков ресурсов
«Создание протоколов доставки»	Разрешение позволяет добавлять протоколы доставки
«Создание сетей»	Разрешение позволяет добавлять сети

Разрешение	Описание
«Создание фондов рабочих мест»	Разрешение позволяет создавать фонды BPM
«Удаление групп рабочих мест»	Разрешение позволяет удалять группы BPM
«Удаление доменов аутентификации»	Разрешение позволяет удалять домены аутентификации
«Удаление изображений из галереи»	Разрешение позволяет удалять изображения из галереи
«Удаление объектов инфраструктуры»	Разрешение позволяет удалять компоненты Termidesk из таблиц раздела «Инфраструктура»
«Удаление параметров гостевых ОС»	Разрешение позволяет удалять параметры гостевых ОС
«Удаление поставщика ресурсов»	Разрешение позволяет удалять поставщиков ресурсов
«Удаление протоколов доставки»	Разрешение позволяет удалять протоколы доставки
«Удаление сетей»	Разрешение позволяет удалять сети
«Удаление фондов рабочих мест»	Разрешение позволяет удалять фонды BPM
«Управление группами домена аутентификации»	Разрешение позволяет выполнять действия: ▪ добавление группы домена аутентификации; ▪ редактирование группы домена аутентификации; ▪ удаление группы домена аутентификации
«Управление пользовательскими сессиями»	Разрешение позволяет выполнять действия с активными сессиями пользователей: ▪ отключение сессии; ▪ сброс сессии
«Управление пользователями домена аутентификации»	Разрешение позволяет выполнять действия: ▪ добавление пользователя домена аутентификации; ▪ редактирование пользователя домена аутентификации; ▪ удаление пользователя домена аутентификации
«Управление ролями»	Разрешение позволяет выполнять: ▪ просмотр раздела «Управление ролями» и выполнять действия в разделе: • создавать роли; • редактировать роли; • удалять роли; ▪ просмотр раздела «Управление ACL» и выполнять действия в разделе: • создавать разрешения для объектов; • редактировать разрешения для объектов; • удалять разрешения для объектов
«Управление шаблонами рабочих мест»	Разрешение позволяет выполнять действия: ▪ создание шаблона BPM; ▪ редактирование шаблона BPM; ▪ удаление шаблона BPM

Для редактирования класса администратора нужно выбрать его, а затем нажать экранную кнопку **[Изменить]**.

Для удаления нужно выбрать созданный объект, а затем нажать экранную кнопку **[Удалить]**.

⚠ Класс администратора может быть удален только в том случае, если он не назначен пользователю.

Класс администратора может быть назначен определенному пользователю. Для назначения созданного класса следует перейти «Компоненты - Домены аутентификации» и затем в столбце «Название» сводной таблицы выбрать домен аутентификации, в который входит пользователь.

На открывшейся странице в таблице «Пользователи» нужно выбрать пользователя и нажать экранную кнопку **[Изменить]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. Рисунок 33).

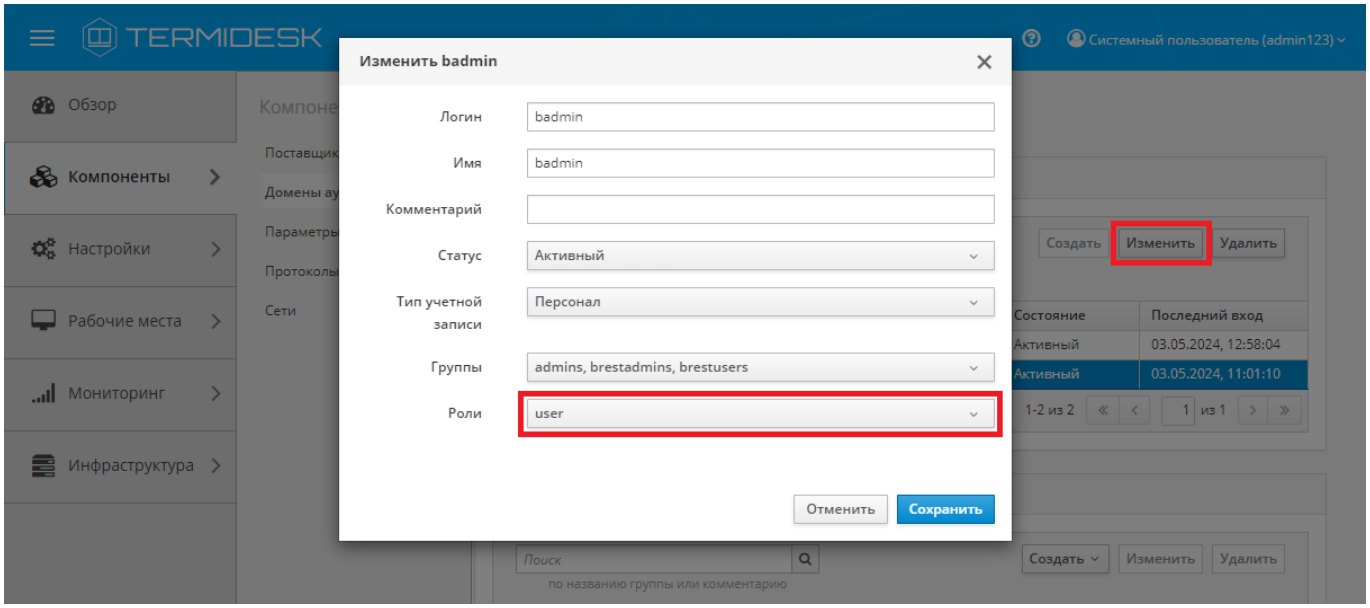

Рисунок 33 – Окно назначения пользовательских ролей

> ⚠ Параметр «Персонал» указывает, что пользователь является оператором Termidesk (класс администратора с ограниченными полномочиями в графическом интерфейсе Termidesk).

Созданным классам администраторов можно делегировать управление отдельными фондами BPM. Для добавления нового разрешения объекту следует перейти «Настройки - Управление ACL», нажать экранную кнопку **[Создать]** и выбрать объект «Фонд рабочих мест».

В режиме добавления нового разрешения для объекта администратору Termidesk необходимо заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 43).

Таблица 43 – Доступные параметры при добавлении пользовательских разрешений для фондов BPM

Параметр	Описание
«Роль»	Наименование заранее созданного и назначенного пользователю класса администратора

Параметр	Описание
«Пользовательское разрешение»	Выбор пользовательских разрешений, касающихся фондов BPM. Список всех доступных разрешений: ▪ просмотр фондов BPM; ▪ редактирование фондов BPM; ▪ удаление фондов BPM; ▪ управление кешем фондов BPM; ▪ управление пользовательскими группами фондов BPM; ▪ управление пользователями фондов BPM; ▪ управление протоколами доставки фондов BPM; ▪ управление публикациями фондов BPM
«Объект»	Ранее созданный фонд BPM

10.5 . Перенаправление на HTTPS

Для того, чтобы веб-интерфейс Termidesk работал по безопасному протоколу HTTPS, используются настройки веб-сервера apache для перенаправления запроса с протокола HTTP на HTTPS.

Настройки перенаправления задаются в конфигурационном файле `/etc/apache2/sites-available/termidesk.conf`. После внесения любых изменений в этот файл необходимо перезапустить службу веб-сервера apache:

```
:~$ sudo systemctl restart apache2
```

⚠ Перенаправление на HTPS настроено по умолчанию после установки Termidesk. При необходимости использования незащищенного протокола HTTP администратор должен изменить файл `/etc/apache2/sites-available/termidesk.conf`, раскомментировав настройки VirtualHost и закомментировав настройки HTTPS.

Пример исходного конфигурационного файла:

```
#<VirtualHost *:80>
#    ServerName #HOSTNAME#
#    DocumentRoot /opt/termidesk/share/termidesk-vdi/src
#
#    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
#    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/
#
#    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
#        Order deny,allow
#        Allow from all
#        Require all granted
#    </Directory>
#
#    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
#        Order deny,allow
#        Allow from all
#        Require all granted
#    </Directory>
```

```
#
#    RewriteEngine on
#    ProxyTimeout 70
#    ProxyPreserveHost On
#    ProxyRequests Off
#
#    ProxyPassMatch ^/media/ !
#    ProxyPassMatch ^/static/ !
#
#    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
#    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800
#
#    ProxyPass / http://127.0.0.1:8000/
#    ProxyPassReverse / http://127.0.0.1:8000/
#
#    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
#
#    ErrorLog ${APACHE_LOG_DIR}/error.log
#    CustomLog ${APACHE_LOG_DIR}/access.log combined
#</VirtualHost>

# Сайт для принудительного перенаправления на протокол HTTPS.
<VirtualHost *:80>
        ServerName #HOSTNAME#
        ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
        ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800
        RewriteEngine On
        RewriteCond "%{REQUEST_URI}" !^/websockify.*
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=308,L]
        RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerName #HOSTNAME#
    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

```

```
    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPassMatch ^/media/ !
    ProxyPassMatch ^/static/ !

    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800

    ProxyPass / http://127.0.0.1:8000/
    ProxyPassReverse / http://127.0.0.1:8000/

    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    # Для корректной работы Termidesk с MTLS необходимо настроить директивы ниже
    # в соответствии с условиями и требованиями окружения инсталляции
    # SSLCACertificateFile
    # SSLVerifyClient
    # SSLVerifyDepth

    # Проброс параметров клиентского сертификата в Termidesk
    # через набор собственных заголовков
    RequestHeader set X-TDSK-SSL_CLIENT_FORMAT 'apache'
    RequestHeader set X-TDSK-SSL_CLIENT_S_DN expr=%{SSL_CLIENT_S_DN}
    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_START expr=%
{SSL_CLIENT_V_START}
    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_END expr=%{SSL_CLIENT_V_END}
    RequestHeader set X-TDSK-SSL_CLIENT_VERIFY expr=%{SSL_CLIENT_VERIFY}
    RequestHeader set X-TDSK-SSL_CLIENT_CERT expr=%{SSL_CLIENT_CERT}
</VirtualHost>
</IfModule>
```

Пример конфигурационного файла для работы по незащищенному протоколу HTTP:

```
<VirtualHost *:80>
    ServerName #HOSTNAME#
    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
        Order deny,allow
        Allow from all
        Require all granted
```

```
    </Directory>

    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPassMatch ^/media/ !
    ProxyPassMatch ^/static/ !

    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800

    ProxyPass / http://127.0.0.1:8000/
    ProxyPassReverse / http://127.0.0.1:8000/

    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

# Сайт для принудительного перенаправления на протокол  HTTPS.
# <VirtualHost *:80>
#         ServerName #HOSTNAME#
#         ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
#         ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800
#         RewriteEngine On
#         RewriteCond "%{REQUEST_URI}" !^/websockify.*
#         RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=308,L]
#         RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
#     ErrorLog ${APACHE_LOG_DIR}/error.log
#     CustomLog ${APACHE_LOG_DIR}/access.log combined
#</VirtualHost>

# <IfModule mod_ssl.c>
# <VirtualHost _default_:443>
#     ServerName #HOSTNAME#
#     DocumentRoot /opt/termidesk/share/termidesk-vdi/src

#     Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
#     Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

#     <Directory /opt/termidesk/share/termidesk-vdi/src/static>
#         Order deny,allow
#         Allow from all
#         Require all granted
#     </Directory>
```

```
#    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
#        Order deny,allow
#        Allow from all
#        Require all granted
#    </Directory>

#    RewriteEngine on
#    ProxyTimeout 70
#    ProxyPreserveHost On
#    ProxyRequests Off

#    ProxyPassMatch ^/media/ !
#    ProxyPassMatch ^/static/ !

#    ProxyPass /websockify  ws://127.0.0.1:5099/ timeout=10800
#    ProxyPassReverse /websockify ws://127.0.0.1:5099/ timeout=10800

#    ProxyPass / http://127.0.0.1:8000/
#    ProxyPassReverse / http://127.0.0.1:8000/

#    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

#    ErrorLog ${APACHE_LOG_DIR}/error.log
 #   CustomLog ${APACHE_LOG_DIR}/access.log combined

#    SSLEngine on
#    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
#    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    # Для корректной работы Termidesk с MTLS необходимо настроить директивы ниже
    # в соответствии с условиями и требованиями окружения инсталляции
    # SSLCACertificateFile
    # SSLVerifyClient
    # SSLVerifyDepth

    # Проброс параметров клиентского сертификата в Termidesk
    # через набор собственных заголовков
#    RequestHeader set X-TDSK-SSL_CLIENT_FORMAT 'apache'
#    RequestHeader set X-TDSK-SSL_CLIENT_S_DN expr=%{SSL_CLIENT_S_DN}
#    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_START expr=%
{SSL_CLIENT_V_START}
#    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_END expr=%{SSL_CLIENT_V_END}
#    RequestHeader set X-TDSK-SSL_CLIENT_VERIFY expr=%{SSL_CLIENT_VERIFY}
#   RequestHeader set X-TDSK-SSL_CLIENT_CERT expr=%{SSL_CLIENT_CERT}
# </VirtualHost>
#</IfModule>
```

10.6 . Замена SSL-сертификата веб-сервера

Для доступа к веб-интерфейсу Termidesk по протоколу HTTPS на этапе установки веб-сервера автоматически генерируется самоподписанный сертификат и закрытый ключ к нему. В некоторых случаях может понадобиться заменить эти сертификаты на другие.

Ключ - последовательность псевдослучайных чисел, сгенерированная особым образом. Сертификат - артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу.

Для замены SSL-сертификатов необходимо:

- получить новый сертификат и ключ к нему;
- поместить новый сертификат формата `.pem` в каталог `/etc/ssl/certs/`:

```
:~$ sudo cp <путь_к_сертификату> /etc/ssl/certs/
```

- поместить новый ключ формата `.key` в каталог `/etc/ssl/private/`:

```
:~$ sudo cp <путь_к_ключу> /etc/ssl/certs/
```

Если сертификат и ключ находятся в PKCS12-контейнере (файл формата `.pfx`), необходимо сначала сконвертировать их в нужный формат:

```
:~$ openssl pkcs12 -in <путь_к_pfx-контейнеру> -out <путь_к_создаваемому_файлу.pem> -nodes
:~$ openssl pkcs12 -in <путь_к_pfx-контейнеру> -nocerts -nodes -out <путь_к_создаваемому_файлу.key>
```

- отредактировать файл `/etc/apache2/sites-available/termidesk.conf`, заменив путь к сертификату и ключу для параметров `SSLCertificateFile` и `SSLCertificateKeyFile` на новые:

```
SSLEngine on
SSLCertificateFile      /etc/ssl/certs/new_cert.pem
SSLCertificateKeyFile /etc/ssl/private/new_key.key
</VirtualHost>
```

- перезапустить веб-сервер:

```
:~$ sudo systemctl restart apache2
```

10.7 . Установка корневого сертификата центра сертификации

Установка корневого сертификата центра сертификации (ЦС) может быть необходима при настройке доступа между компонентами по протоколу SSL. Предполагается, что инфраструктура открытых ключей (PKI) уже развернута в организации, ЦС установлен.

Для того чтобы установить корневой сертификат ЦС (например, `CA.crt`) на «Универсальный диспетчер» Termidesk, нужно:

- скопировать файл `CA.crt` на сервер Termidesk;

- затем скопировать `CA.crt` в каталог `/usr/share/ca-certificates`:

```
:~$ sudo cp <путь_к_сертификату> /usr/share/ca-certificates/
```

- выполнить команду добавления корневого сертификата ЦС:

```
:~$ sudo dpkg-reconfigure ca-certificates
```

- на запрос «Доверять новым сертификатам удостоверяющих центров» ответить «Да»;
- убедиться, что сертификат `CA.crt` отмечен для активации;
- нажать экранную кнопку **[Ok]** и дождаться окончания операции.

Для настройки Termidesk на работу с сертификатами нужно:

- добавить переменную окружения `REQUESTS_CA_BUNDLE` в файле `/etc/opt/termidesk-vdi/termidesk.conf`. В переменной окружения нужно указать путь к файлу с доверенным корневым сертификатом. Пример:

```
REQUESTS_CA_BUNDLE=/etc/ssl/certs/ca.crt
```

- выполнить перезапуск службы `termidesk-vdi`:

```
:~$ sudo systemctl restart termidesk-vdi
```

10.8 . Работа веб-интерфейса Termidesk с протоколом TLS

Веб-интерфейс Termidesk по умолчанию поддерживает работу на всех протоколах, кроме SSLv3. Для того чтобы включить поддержку только протоколов TLS1.2 и TLS 1.3 в веб-сервере `apache`, нужно скорректировать файл конфигурации `/etc/apache2/mods-available/ssl.conf`.
Для этого:

- выполнить резервное копирование текущего файла конфигурации:

```
:~$ sudo cp /etc/apache2/mods-available/ssl.conf /etc/apache2/mods-available/ssl.conf_bkp
```

- включить поддержку только протоколов TLS1.2 и TLS 1.3, внеся изменения в файл конфигурации `/etc/apache2/mods-available/ssl.conf`:

```
1 :~$ sudo sed -i 's/SSLProtocol all -SSLv3/SSLProtocol -all +TLSv1.2 +TLSv1.3/g' /etc/apache2/mods-available/ssl.conf
2 :~$ sudo sed -i 's/SSLCipherSuite HIGH:!aNULL/SSLCipherSuite HIGH:!aNULL:!MD5:!3DES/g' /etc/apache2/mods-available/ssl.conf
3 :~$ sudo sed -i 's/#SSLHonorCipherOrder on/SSLHonorCipherOrder on/g' /etc/apache2/mods-available/ssl.conf
```

- выполнить обновление файлов конфигурации веб-сервера `apache`:

```
:~$ sudo systemctl reload apache2
```

10.9 . Управление авторизацией пользователя в компоненте «Клиент»

В Termidesk предусмотрена возможность управления авторизацией пользователя в компоненте «Клиент».

Для изменения параметров авторизации следует перейти «Настройки - Системные параметры - Аутентификация», и настроить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 44).

Для сохранения параметров авторизации нужно нажать экранную кнопку **[Сохранить]**.

Таблица 44 – Доступные параметры при настройке сохранения паролей в компоненте «Клиент»

Параметр	Описание
«Разрешить сохранение имени пользователя в клиенте»	Управление параметром сохранения имени пользователя в компоненте «Клиент» при подключении к «Универсальному диспетчеру». Значение по умолчанию: «Да»
«Разрешить сохранение пароля в клиенте»	Управление параметром сохранения пароля в компоненте «Клиент» при подключении к «Универсальному диспетчеру». Значение по умолчанию: «Да»
«Доп. информация при ошибке входа»	Информационное сообщение, отображаемое при ошибке входа

11 . РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

11.1 . Общие сведения

Поскольку каждая установка компонентов Termidesk может отличаться от других, подробные шаги по резервному копированию и восстановлению и используемые инструменты будут приведены не для всех компонентов. Резервное копирование и восстановление может выполняться как средствами и службами ОС, так и специализированными системами. Порядок выполнения и периодичность резервного копирования определяются эксплуатирующим предприятием.

Резервному копированию подлежат:

- БД Termidesk;
- конфигурационные файлы компонента «Универсальный диспетчер» и административного и/или пользовательского порталов;
- конфигурационные файлы компонента «Шлюз»;
- конфигурационные файлы компонента «Менеджер рабочих мест»;
- конфигурационные файлы компонента «Сервер терминалов Astra Linux»;
- конфигурационные файлы компонента «Сессионный агент»;
- конфигурационные файлы балансировщика нагрузки;
- конфигурационные файлы, использующиеся для режима высокой доступности.

В качестве альтернативного варианта могут резервироваться целиком узлы компонентов, если они установлены на ВМ. Такой подход применяется, например, для резервирования компонента «Виртуальный модуль Termidesk».

Как правило, файлы компонентов «Удаленный помощник», «Клиент» не подлежат резервному копированию, т.к. повторная установка в большинстве случаев будет быстрее.

11.2 . Действия с БД Termidesk

11.2.1 . Резервное копирование БД

Резервное копирование БД, созданной СУБД Postgres-11 можно выполнить утилитой `pg_dump`:

```
:$ pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t > <имя_файла_для_сохранения_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`--format=t` - ключ для экспорта БД в формате `tar`;

`<имя_файла_для_сохранения_БД.tar>` - имя и формат файла (`tar`) для сохранения БД.

11.2.2 . Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
:$ pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь>
-W -f <файл_копии_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если используется локальная БД, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`-f <файл_копии_БД.tar>` - путь к файлу резервной копии БД.

11.3 . Действия с брокером сообщений RabbitMQ

11.3.1 . Резервное копирование данных брокера сообщений RabbitMQ-server

Для RabbitMQ-server следует:

- остановить службу `rabbitmq-server`:

```
:~$ sudo systemctl stop rabbitmq-server
```

- выполнить резервное копирование каталога `/etc/rabbitmq/` вместе с его содержимым;
- выполнить резервное копирование каталога данных `/var/lib/rabbitmq/mnesia/`;
- запустить службу `rabbitmq-server`:

```
:~$ sudo systemctl start rabbitmq-server
```

11.3.2 . Восстановление брокера сообщений RabbitMQ-server из резервной копии

> Современные версии RabbitMQ (3.8.0+) поддерживают восстановление из резервной копии тогда, когда они восстанавливаются на узел RabbitMQ с точно таким же именем узла, с которого была создана резервная копия данных.

Для восстановления конфигурации RabbitMQ-server следует:

- остановить службу `rabbitmq-server`:

```
:~$ sudo systemctl stop rabbitmq-server
```

- восстановить резервные копии каталогов `/etc/rabbitmq/` и `/var/lib/rabbitmq/mnesia/`;
- запустить RabbitMQ-server:

```
:~$ sudo systemctl start rabbitmq-server
```

11.4 . Действия с компонентом «Универсальный диспетчер»

11.4.1 . Резервное копирование данных «Универсального диспетчера»

Для компонента «Универсальный диспетчер» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-vdi/` вместе с его содержимым;
- конфигурационного файла `/etc/apache2/sites-available/termidesk.conf`;
- ключей `/etc/ssl/certs/ssl-cert-snakeoil.pem` и `/etc/ssl/private/ssl-cert-snakeoil.key`, использующихся для защищенного подключения к порталу администратора и/или пользователя.

11.4.2 . Восстановление «Универсального диспетчера» из резервной копии

Для восстановления конфигурации «Универсального диспетчера» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-vdi/`;
- восстановить резервные копии конфигурационного файла `/etc/apache2/sites-available/termidesk.conf` и ключей `/etc/ssl/certs/ssl-cert-snakeoil.pem`, `/etc/ssl/private/ssl-cert-snakeoil.key`;
- перезапустить службу `termidesk-vdi`:

```
:~$ sudo systemctl restart termidesk-vdi
```

- перезапустить веб-сервер:

```
:~$ sudo systemctl restart apache2
```

11.5 . Действия с компонентом «Шлюз»

11.5.1 . Резервное копирование данных «Шлюза»

Для компонента «Шлюз» следует выполнить резервное копирование:

- конфигурационного файла `/etc/termidesk/termidesk-gateway.conf`;
- ключей, использующихся для защищенного соединения, указанных в файле `/etc/termidesk/termidesk-gateway.conf`.

11.5.2 . Восстановление «Шлюза» из резервной копии

Для восстановления конфигурации «Шлюза» следует:

- восстановить резервную копию файла `/etc/termidesk/termidesk-gateway.conf` и ключей указанных в этом файле;
- перезапустить службу `termidesk-gateway`:

```
:~$ sudo systemctl restart termidesk-gateway
```

11.6 . Действия с компонентом «Менеджер рабочих мест»

11.6.1 . Резервное копирование данных «Менеджера рабочих мест»

Для компонента «Менеджер рабочих мест» следует выполнить резервное копирование каталога `/etc/opt/termidesk-vdi/` вместе с его содержимым.

11.6.2 . Восстановление «Менеджера рабочих мест» из резервной копии

Для восстановления конфигурации «Менеджера рабочих мест» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-vdi/`;
- перезапустить службы:

```
:~$ sudo systemctl restart termidesk-taskman termidesk-celery-beat termidesk-celery-worker
```

⚠ Если компонент «Менеджер рабочих мест» был установлен в распределенном варианте установки Termidesk, необходимо учесть, что одновременно служба `termidesk-taskman` должна быть запущена только на одном из узлов, работающих в режиме балансировки.

11.7 . Действия с компонентом «Сервер терминалов Astra Linux»

11.7.1 . Резервное копирование данных «Сервера терминалов Astra Linux»

Для компонента «Сервер терминалов Astra Linux» следует выполнить резервное копирование каталога `/etc/stal/` и компонента «Сессионный агент» (см. подраздел **Резервное копирование данных «Сессионного агента»**).

11.7.2 . Восстановление «Сервера терминалов Astra Linux» из резервной копии

Для восстановления конфигурации «Сервера терминалов Astra Linux» следует:

- восстановить резервную копию каталога `/etc/stal/`;
- восстановить компонент «Сессионный агент» (см. подраздел **Восстановление «Сессионного агента» из резервной копии**);
- перезапустить службы:

```
:~$ sudo systemctl restart termidesk-stal stal-proxy stal-rdpepc
```

11.8 . Действия с компонентом «Сессионный агент»

11.8.1 . Резервное копирование данных «Сессионного агента»

Для компонента «Сессионный агент» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server));
- каталога `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server).

11.8.2 . Восстановление «Сессионного агента» из резервной копии

Для восстановления конфигурации «Сессионного агента» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server)) или `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server);
- перезапустить службу «TermideskSessionAgentService» через оснастку «Службы» в ОС Microsoft Windows Server или командой в ОС Astra Linux Special Edition (Server):

```
:~$ sudo systemctl restart termidesk-session-agent
```

11.9 . Действия с балансировщиком нагрузки

11.9.1 . Резервное копирование данных балансировщика нагрузки

> ⓘ Пример приведен для балансировщика nginx, поскольку его настройка описана в качестве примера в подразделе **Настройка балансировщика для работы с самоподписанными сертификатами**.

Для балансировщика нагрузки `nginx` следует выполнить резервное копирование:

- каталога `/etc/nginx/snippets`;
- каталога с ключами и сертификатами `/etc/ssl/`;
- каталога `/etc/nginx/sites-available/`;
- каталога `/etc/nginx/conf.d/`.

11.9.2 . Восстановление балансировщика нагрузки из резервной копии

Для восстановления конфигурации балансировщика нагрузки `nginx` следует:

- восстановить резервные копии каталогов `/etc/nginx/snippets`, `/etc/ssl/`, `/etc/nginx/sites-available/`, `/etc/nginx/conf.d/`;
- перезапустить веб-сервер:

```
:~$ sudo systemctl restart nginx
```

11.10 . Действия для режима высокой доступности

11.10.1 . Резервное копирование конфигурации режима высокой доступности

Для режима высокой доступности, который обычно настраивается для отказоустойчивой или распределенной установки Termidesk, следует выполнить резервное копирование каталога `/etc/keepalived/`.

11.10.2 . Восстановление конфигурации режима высокой доступности из резервной копии

Для восстановления конфигурации режима высокой доступности следует:

- восстановить из резервной копии каталог `/etc/keepalived/`;
- перезапустить сервис `keeaplived`:

```
:~$ sudo systemctl restart keepalived
```

12 . ГЕНЕРАЦИЯ ОТЧЕТА ПО МОДЕЛЯМ ДАННЫХ И СТРУКТУРАМ БД TERMIDESK

12.1 . Генерация отчета по моделям данных и структурам БД Termidesk

В Termidesk реализована возможность генерации отчета по моделям данных и структурам БД с описанием полей таблиц, их значений и межтабличных связей.

Для генерации отчета следует перейти в интерфейс командной строки и выполнить команду:

- если требуется сгенерировать отчет по модели данных и структуре БД приложения:

```
:~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models termidesk >
<имя_файла_для_сохранения.html>
```

где:

`termidesk` - название приложения;

`<имя_файла_для_сохранения.html>` - имя и формат файла (`html`) для сохранения отчета.

> ⚠ Для генерации отчета по модели данных и структуре БД нескольких приложений их названия указываются через пробел.

- если требуется сгенерировать отчет по всей модели данных и структуре БД Termidesk:

```
:~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models -a -g >
<имя_файла_для_сохранения.html>
```

где:

`-a` - ключ для генерации отчета, описывающего все доступные модели данных и структуры БД;

`-g` - ключ группировки таблиц в соответствии с их приложениями;

`<имя_файла_для_сохранения.html>` - имя и формат файла (`html`) для сохранения отчета.

Структура файла отчета приведена в таблице (см. Таблица 45).

Таблица 45 – Структура файла отчёта

Параметр	Описание
`App`	Название приложения, для которого представлена структура модели данных
`Model`	Идентификатор модели с представлением структуры данных
`Abstract Model`	Идентификатор модели, для которой представлена структура данных
<Информационная строка>	Строка содержит модель отчета с перечислением полей, либо дополнительную информацию о модели данных
`NAME`	Столбец содержит имена параметров

Параметр	Описание
VALUE	Столбец содержит тип данных параметров
HELP TEXT	Столбец содержит описание параметров

13 . МОНИТОРИНГ И УВЕДОМЛЕНИЯ

13.1 . Системные параметры мониторинга

Системные параметры мониторинга позволяют настроить вывод событий в syslog-сервер.

Для конфигурации системных параметров мониторинга следует перейти «Настройки - Системные параметры - Мониторинг».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 46).

Таблица 46 – Параметры мониторинга Termidesk

Параметр	Описание
«Логирование Syslog»	Перенаправление потока событий мониторинга на отдельный syslog-сервер
«Хост 1» — «Хост 3»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на узел с «Универсальным диспетчером» Termidesk корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**. Значение по умолчанию: «UDP»
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал мониторинга
«Уровень логирования»	Выбор уровня логирования событий (`INFO`, `WARNING`, `ERROR`, `CRITICAL`, `DEBUG`)

13.2 . Настройка отправки уведомлений о системных событиях

Для настройки отправки уведомлений о системных событиях следует перейти «Настройки - Системные параметры - Уведомления».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 47).

Таблица 47 – Параметры отправки уведомлений о событиях

Параметр	Описание
«Вкл/выкл почтовых уведомлений»	Включение или отключение возможности отправки уведомлений о системных событиях по электронной почте
«Хост»	IP-адрес или имя узла, на котором развернута служба сервера электронной почты
«Порт»	Номер порта, на котором ведется прослушивание службой сервера электронной почты
«Email отправителя»	Почтовый адрес отправителя сообщений на сервере электронной почты. Формат: `mailto:user@mail.domain`

Параметр	Описание
«Пользователь»	Идентификатор пользователя сервиса электронной почты
«Пароль»	Последовательность символов для подтверждения полномочий пользователя сервиса электронной почты
«Поддержка TLS»	Включение поддержки протокола TLS при взаимодействии с сервером электронной почты
«Поддержка SSL»	Включение поддержки протокола SSL при взаимодействии с сервером электронной почты
«Таймаут»	Время ожидания (в секундах) ответа от сервера электронной почты
«Email получателей (через запятую)»	Перечень адресов электронной почты получателей уведомлений. Формат: `mailto:user@mail.domain`
«Префикс для темы письма»	Текстовое поле, содержащее информацию для подстановки в тему электронного письма
«Уведомление о смене режима техобслуживания в поставщике ресурсов»	Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в поставщике ресурсов»
«Уведомление о смене режима техобслуживания в фонде рабочих мест»	Включение возможности отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в фонде рабочих мест»
«Уведомление о возникновении ошибок с рабочими местами»	Включение возможности отправки уведомления по электронной почте о системном событии «Возникновение ошибок внутри фонда рабочих мест»
«Уведомление о превышении лицензированного количества подключений»	Включение возможности отправки уведомления по электронной почте о системном событии «Запрос подключения сверх лимита, установленного лицензией»
«Уведомление о превышении лицензированного количества пользователей»	Включение возможности отправки уведомления по электронной почте о системном событии «Запрос входа пользователя сверх лимита, установленного лицензией»

13.3 . Шаблон для мониторинга Zabbix

Termidesk поддерживает мониторинг состояния компонентов через `Zabbix`.

Шаблон для мониторинга распространяется через `iso`-образ Termidesk.

В шаблоне находятся метрики для мониторинга компонентов Termidesk: «Универсального диспетчера», «Шлюза», «Менеджера виртуального рабочего места».

Реализованы как простые проверки (подключение к портам), так и опрос состояния служб `health checking`.

13.4 . Отчеты

Для формирования отчетов о событиях в графическом интерфейсе управления следует перейти «Мониторинг - Отчеты».

Можно сформировать следующие отчеты:

- отчет по последнему пользовательскому входу в систему;

- отчет по пользовательским сеансам;
- отчет по пользовательским подключениям.

Для формирования отчета по последнему пользовательскому входу в систему надо нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по последнему пользовательскому входу в систему» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 48).

Таблица 48 – Параметры для формирования отчета по последнему пользовательскому входу в Termidesk

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала»	Дата и время начала события, от которых будет сформирован отчет. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора

⚠ Если сформированные отчеты не содержат никакой информации (пустые), необходимо проверить, что системный параметр аудита «Сохранение в БД» установлен в значение «Да» (см. подраздел **Системные параметры аудита**).

Для формирования отчета по пользовательским сеансам надо нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским сеансам» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 49).

Таблица 49 – Параметры для формирования отчета по пользовательским сеансам

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала сеанса»	Дата и время начала события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора
«Дата и время завершения сеанса»	Дата и время завершения события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора
«Домен аутентификации»	Наименование домена аутентификации, по которому будет осуществлен поиск события
«Пользователь»	Логин пользователя, по которому будет осуществлен поиск события

Для формирования отчета по пользовательским подключениям надо нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским подключениям» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 50).

Таблица 50 – Параметры для формирования отчета по пользовательским подключениям

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала подключения»	Дата и время начала события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора
«Дата и время завершения подключения»	Дата и время завершения события. Для выбора даты и времени надо нажать левой кнопкой мыши в поле ввода, затем выбрать нужное значение и нажать клавишу **<Enter>** для подтверждения выбора

Для просмотра сформированного отчета следует перейти «Мониторинг – Отчеты» и выбрать название отчета.

При помощи экранной кнопки **[CSV]** можно выгрузить в `csv`-файл весь представленный отчет (см. Рисунок 34).

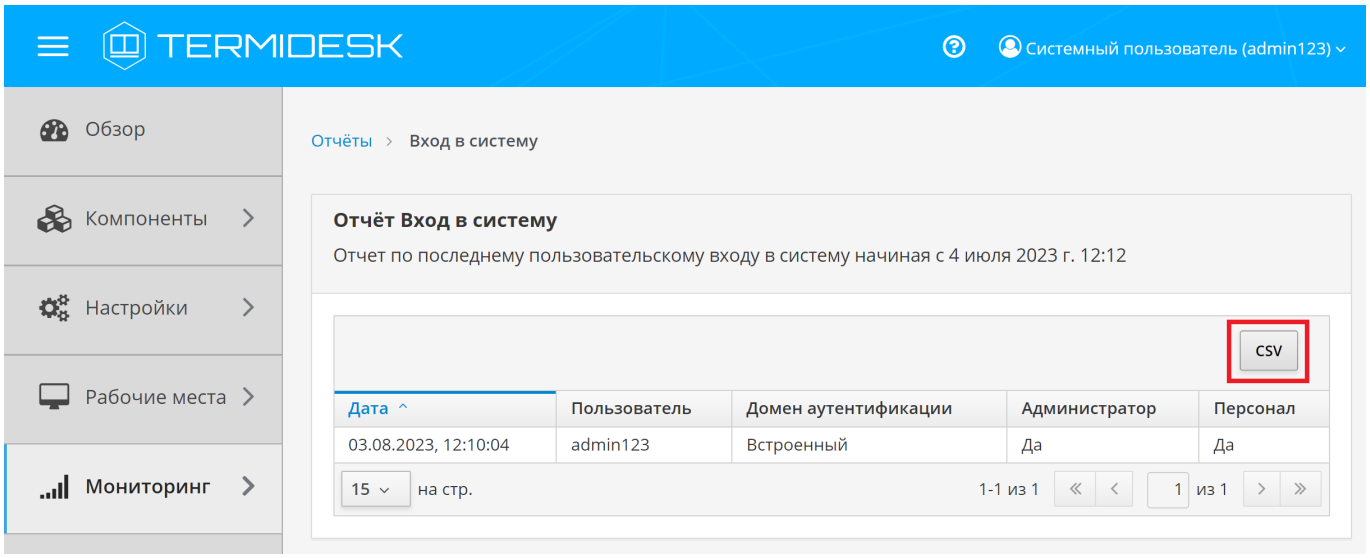

Рисунок 34 – Окно сформированного отчета по последнему пользовательскому входу

14 . СИСТЕМА АУДИТА

14.1 . Системные параметры аудита

Для конфигурации системных параметров аудита следует перейти «Настройки - Системные параметры - Аудит».

Доступные для редактирования администратору Termidesk параметры перечислены в столбце «Параметр» следующей таблицы (см. Таблица 50).

Таблица 51 – Системные параметры аудита

Параметр	Описание
«Использовать "строгий" режим аудита»	Включение режима максимально полного сохранения информации о событиях аудита
«Сохранение в БД»	Выбор сохранения событий аудита в БД
«Время хранения записи в БД (дней)»	Время хранения (в днях) записи события аудита в БД
«Максимум удаляемых событий»	Максимальное количество удаляемых событий в журнале аудита
«Сохранение в файл»	Выбор сохранения событий аудита в отдельный файл журнала
«Файл хранения событий»	Указание полного пути к файлу хранения журнала событий аудита при выбранной опции «Сохранение в файл»
«Количество архивных файлов»	Максимальное количество архивных файлов журнала событий аудита, по достижении которого начинается перезапись
«Отправка в Syslog»	Направление логирования на отдельный syslog-сервер
«Хост»	IP-адрес или имя узла, на котором развёрнута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на «Универсальный диспетчер» Termidesk корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**. Значение по умолчанию: «UDP»
«Порт»	Порт, на котором находится служба syslog-сервера
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал аудита

События аудита, регистрируемые Termidesk:

- события, связанные с интерфейсом командной строки:
  - изменение системных параметров «Универсального диспетчера» через командную строку;
  - операции пользователей с объектами;
  - вход пользователя в систему через интерфейс командной строки;
  - выход пользователя из системы через интерфейс командной строки;

- события, связанные с политиками фонов BPM:
  - изменение глобальных политик;
  - изменение политик BPM;
  - сброс политики BPM;
  - сброс глобальных политик;
- события, связанные с пользователем:
  - подключение пользователя к BPM;
  - отключение пользователя от BPM;
  - вход пользователя в ОС BPM;
  - выход пользователя из ОС BPM;
  - блокировка гостевой ОС BPM;
  - разблокировка гостевой ОС BPM;
  - неактивность пользователя;
  - активность пользователя;
  - подключение пользователя к BPM и начало работы;
  - прекращение сессии пользователя по команде с «Универсального диспетчера»;
  - назначение пользователя на BPM;
- события, связанные с веб-интерфейсом Termidesk:
  - вход пользователя в систему через веб-интерфейс;
  - выход пользователя из веб-интерфейса;
  - изменение системных параметров Termidesk;
  - операции пользователей с объектами через REST API;
  - загрузка файла лицензии через REST API;
  - прекращение сессии пользователя по команде с «Универсального диспетчера»;
  - сброс сессии пользователя по команде с «Универсального диспетчера»;
- события, связанные с API:
  - вход пользователя в систему через API;
  - выход пользователя из системы через API.

14.2 . Журналы

Журналы Termidesk хранятся в каталоге `/var/log/termidesk`.

Установлены следующие журналы Termidesk, разделенные по типам событий, которые в них записываются:

- `auth.log` - записываются события об авторизации субъектов в Ternidesk;
- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;

- `celery-worker.log` - записываются события обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `other.log` - записываются события, не относящиеся к другим модулям;
- `database.log` - записываются отладочные события БД;
- `termidesk.log` - записываются события работы «Универсального диспетчера» Termidesk;
- `use.log` - записываются события пользователей ВРМ;
- `workers.log` - записываются события обработчика фоновых задач.

Настройки ротации журналов определены в конфигурационном файле `/etc/logrotate.d/termidesk.local`.

14.3 . Настройка журналирования

Уровень журналирования задается параметром `LOG_LEVEL` в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`.

Для изменения уровня журналирования необходимо:

- изменить параметр `LOG_LEVEL`;
- перезапустить службы Termidesk:

```
:~$ sudo systemctl restart termidesk-vdi.service termidesk-taskman.service termidesk-wsproxy.service termidesk-celery-beat.service termidesk-celery-worker.service
```

14.4 . Просмотр журналов

Для просмотра общего журнала событий, связанного с функционированием Termidesk и действиями субъектов доступа, следует перейти «Мониторинг – Журнал», где визуализируются системные события с указанием уровня важности (`CRITICAL`, `ERROR`, `WARNING`, `INFO`, `DEBUG`) и источника возникновения события.

При помощи экранной кнопки `[CSV]` можно выгрузить в `csv`-файл весь представленный журнал событий.

Количество событий, отображаемых в графическом интерфейсе или экспортируемых в csv-файл, можно менять при помощи выпадающего списка «Количество записей для загрузки». Таким образом можно задать 100, 500, 1000 записей или ввести свое значение в доступном поле.

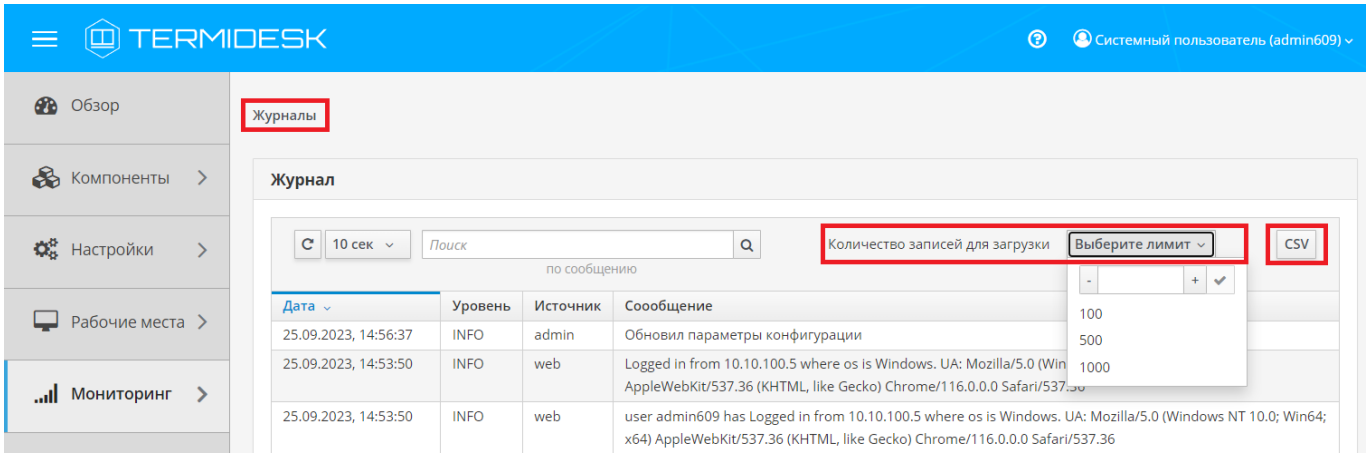

Рисунок 35 – Отображение общего журнала в графическом интерфейсе управления Termidesk

Для просмотра журнала событий, связанного с действиями субъектов доступа, следует перейти «Мониторинг – Аудит».

При помощи экранной кнопки [CSV] (см. Рисунок 36) можно выгрузить в csv-файл весь представленный журнал событий, либо строки событий.

Количество событий, отображаемых в графическом интерфейсе или экспортируемых в csv-файл, можно менять при помощи выпадающего списка «Количество записей для выгрузки». Таким образом можно задать 100, 500, 1000 записей или ввести свое значение в доступном поле.

При помощи экранной кнопки **[Копировать]** строки событий можно скопировать в буфер обмена.

> ⚠ Если события аудита не отображаются во вкладке «Мониторинг – Аудит», необходимо убедиться, что в «Настройки - Системные параметры - Аудит» параметр «Сохранение в БД» имеет значение «Да».

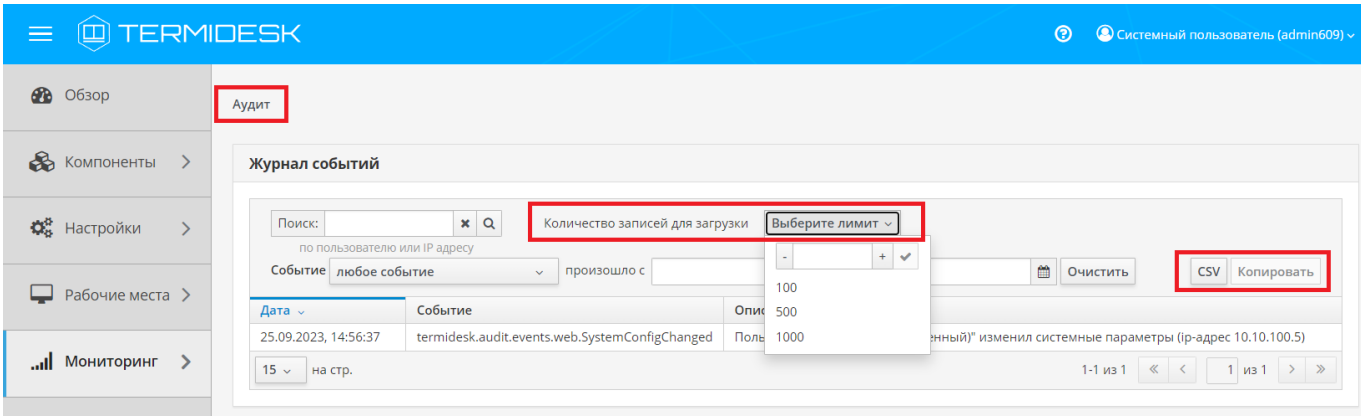

Рисунок 36 – Отображение журнала аудита в графическом интерфейсе управления Termidesk

14.5 . Описание шаблонов событий аудита

14.5.1 . Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных (см. Таблица 52) регистрируемой информации, состав которых может отличаться для разных событий.

Таблица 52 – Типы данных регистрируемой информации

Тип данных	Описание
Дата/время	Дата и время указываются в формате: `DD.MM.YYYY, hh:mm:ss`, где: `DD.MM.YYYY` обозначает «день» - «месяц» - «год»; `hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»; «.» и «:» используются как разделители в обозначениях даты и времени дня соответственно
Имя/логин	Идентификационные данные субъекта, совершающего доступ к объекту
Наименование параметра/секции/политики	Указывает объект, над которым производится действие
Значение	Указывается значение, которое принимал или принял объект после выполнения над ним операции
Тип объекта/сущности	Указывает тип объекта, над которым производится действие
Действие	Название операции, которую совершил субъект над объектом
Уровень важности	Показатель критичности события
Идентификатор	Указывают уникальную (для соответствующего объекта) последовательность чисел для его однозначной идентификации
IP-адрес	32-битовое число. Формой записи IP-адреса является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.0.2.1)

14.5.2 . Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий и шаблоны к ним приведены в таблице (см. Таблица 53).

Таблица 53 – Список типов и шаблонов регистрируемых событий аудита

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
События, связанные с командной строкой		
Изменение системных параметров «Универсального диспетчера» через командную строку `cli.SystemConfigChanged`	Регистрируется: ▪ логин пользователя (`username`); ▪ название секции (`section_name`); ▪ название изменяемого параметра; (`parameter_key`); ▪ новое значение параметра (`parameter_value`)	«Пользователь `"[username]"` изменил системный параметр `[section_name].[parameter_key]=[parameter_value]`»
CRUD операции с объектами через командную строку `cli.EntityAction`	Регистрируется: ▪ имя системного пользователя, запустившего команду (`username`); ▪ тип сущности (`entity`); ▪ уникальный идентификатор (`uuid`); ▪ тип объекта (`subtype`); ▪ название объекта (`name`); ▪ действие над объектом (`action`)	«Пользователь `"[username]"` выполнил операцию `[action]` для объекта `[entity] ([uuid]) [subtype] "[name]"`»

Вход пользователя в систему через командную строку `cli.UserLogin`	Регистрируется: ▪ наименование домена аутентификации (`authenticator`); ▪ логин пользователя (`username`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь `"[username] ([authenticator])"` вошел в систему через `[portal] ([portal_uuid])`»
Выход пользователя из системы через командную строку `cli.UserLogout`	Регистрируется: ▪ наименование домена аутентификации (`authenticator`); ▪ логин пользователя (`username`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь `"[username] ([authenticator])"` вышел из системы через `[portal] ([portal_uuid])`»
События, связанные с политиками		
Изменение глобальных политик `policies.GlobalPolicyChanged`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ новое значение в дружественном к пользователю описании (`value`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ новое значение, в оригинальном формате (`value_raw`)	«Пользователь `"[username] ([authenticator_name])"` изменил значение глобальной политики `"[policy_name]"` на `"[value]"`»
Изменение политик BPM `policies.DeployedServicePolicyChanged`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ название фонда BPM (`deployed_service_name`); ▪ новое значение в дружественном к пользователю описании (`value`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ идентификатор фонда BPM (`deployed_service_uuid`); ▪ новое значение, в оригинальном формате (`value_raw`)	«Пользователь `"[username] ([authenticator_name])"` изменил значение политики `"[policy_name]"` для фонда `"[deployed_service_name]"` на `"[value]"`»

Сброс политики BPM `policies.DeployedServicePolicyDeleted`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ название фонда BPM (`deployed_service_name`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ идентификатор фонда BPM (`deployed_service_uuid`)	«Пользователь "`[username] ([authenticator_name])`" сбросил значение политики "`[policy_name]`" для фонда "`[deployed_service_name]`"»
Сброс глобальных политик `policies.GlobalPolicyDeleted`	Регистрируется: ▪ имя пользователя (`username`); ▪ название домена аутентификации пользователя (`authenticator_name`); ▪ название политики (`policy_name`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`)	«Пользователь "`[username] ([authenticator_name])`" сбросил значение глобальной политики "`[policy_name]`"»
События, связанные с пользователем		
Подключение пользователя к BPM `workplace.UserConnected`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`); ▪ протокол доставки (`transport`)	«К рабочему месту `[vm_name]([vm_ip])` фонда `[workplace]` пользователя "`[username]([authenticator])`" произведено подключение с помощью протокола `[transport]`»
Отключение пользователя от BPM `workplace.UserDisconnected`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`); ▪ протокол доставки (`transport`)	«Подключение к рабочему месту `[vm_name]([vm_ip])` фонда `[workplace]` пользователя "`[username]([authenticator])`" по протоколу `[transport]` разорвано»
Вход пользователя в ОС BPM `workplace.UserLogin`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ Логин пользователя (`username`); ▪ Имя пользователя совершающего вход в гостевую ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда BPM (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" вошел в гостевую ОС ВМ `[vm_name]` (`[vm_ip]`) фонда `[workplace]` как пользователь `[guest_os_username]` с ip-адреса `[ip]`»

Выход пользователя из ОС ВМ `workplace.UserLogout`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего вход в гостевую ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" вышел из гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]` с ip-адреса `[ip]`»
Блокировка ВРМ `workplace.UserLock`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" заблокировал гостевую ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»
Разблокировка ВРМ `workplace.UserUnlock`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" разблокировал гостевую ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»
Пользователь неактивен `workplace.UserIdle`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" неактивен в гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»

Пользователь активен `workplace.UserActive`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ имя пользователя совершающего выход из гостевой ОС ВМ (`guest_os_username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ IP-адрес выданной ВМ (`vm_ip`)	«Пользователь "`[username] ([authenticator])`" вновь активен в гостевой ОС ВМ `[vm_name] ([vm_ip])` фонда `[workplace]` как пользователь `[guest_os_username]`»
Подключение пользователя к ВРМ и начало работы `user.WorkplaceConnectionRequest`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ название фонда ВРМ (`workplace`); ▪ имя выданной ВМ (`vm_name`); ▪ название протокола доставки (`transport`)	«Пользователь "`[username] ([authenticator])`" подключился к ВМ `[vm_name]` фонда `[workplace]` по протоколу `[transport]` с ip-адреса `[ip]`»
Прекращение сессии пользователя по команде с «Универсального диспетчера» `user.WorkplaceMessageSent`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ идентификатор домена аутентификации пользователя (`authenticator_uuid`); ▪ имя пользователя (`username`); ▪ название фонда ВРМ (`deployed_service_name`); ▪ идентификатор фонда ВРМ (`deployed_service_uuid`); ▪ название ВРМ (`user_service_name`); ▪ идентификатор ВРМ (`user_service_uuid`); ▪ тип сообщения (`msg_level`); ▪ текст сообщения (`msg_text`)	«Пользователь `[username] ([authenticator])` отправил сообщение "`[msg_text]`" уровня `[msg_level]` на рабочее место `[user_service_name]` фонда `[deployed_service_name]` »
Назначение пользователя на ВРМ `workplace.UserAssigned`	Регистрируется: ▪ логин пользователя (`username`); ▪ назначенный пользователь (`assigned_to`); ▪ кем назначен пользователь (`assigned_by`); ▪ время назначения (`assignment_time`)	«Пользователь "`[username]`" назначен на рабочее место "`[assigned_to]`" пользователем "`[assigned_by]`"»
События, связанные с веб-интерфейсом		

Вход пользователя в систему через веб-интерфейс `web.UserLogin`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь "`[username] ([authenticator])`" вошел в систему с ip-адреса `[ip]`через `[portal] ([portal_uuid])`»
Выход пользователя из веб-интерфейса `web.UserLogout`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь "`[username] ([authenticator])`" вышел из системы (ip-адрес `[ip]`) через `[portal] ([portal_uuid])`»
Изменение системных параметров «Универсального диспетчера» `web.SystemConfigChanged`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь "`[username] ([authenticator])`" изменил системные параметры (ip-адрес `[ip]`)»
CRUD операции с объектами через REST API `web.EntityAction`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип сущности (`entity`); ▪ идентификатор (`uuid`); ▪ тип объекта (`subtype`); ▪ название объекта (`name`); ▪ действие над объектом (`action`)	«Пользователь "`[username] ([authenticator])`" выполнил операцию `[action]` для объекта `[entity] ([uuid]) [subtype] "[name]"` (ip-адрес `[ip]`)»
Загрузка файла лицензии через REST API `web.LicenseUpdated`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ имя файла лицензии (`license_file_name`)	«Пользователь "`[username] ([authenticator])`" загрузил новый файл лицензии `[license_file_name]` с ip-адреса `[ip]`»
Прекращение сессии пользователя по команде с «Универсального диспетчера» `web.LogoffUserservice`	Регистрируется: ▪ логин пользователя (`user`); ▪ данные гостевой ВМ, сессию которой прекратили (`userservice`)	«Пользователь "`[user]`" отправил запрос на прекращение сессии `[userservice]`»
Сброс сессии пользователя по команде с «Универсального диспетчера» `web.DisconnectUserservice`	Регистрируется: ▪ логин пользователя (`user`); ▪ данные гостевой ВМ, сессию которой прекратили (`userservice`)	«Пользователь "`[user]`" отправил запрос на сброс сессии `[userservice]`»

События, связанные с разными API		
Вход пользователя в систему через API `api.UserLogin`	Регистрируется: ▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь "`[username]` (`[authenticator]`)" вошел в систему с ip-адреса `[ip]`через `[portal]` (`[portal_uuid]`)»
Выход пользователя из системы через API `api.UserLogout`	▪ название домена аутентификации пользователя (`authenticator`); ▪ логин пользователя (`username`); ▪ IP-адрес, с которого был сделан запрос (`ip`); ▪ тип портала (`portal`); ▪ идентификатор портала (`portal_uuid`)	«Пользователь "`[username]` (`[authenticator]`)" вышел из системы с ip-адреса `[ip]` через `[portal]` (`[portal_uuid]`)»

14.5.3 . Форматы регистрируемых событий аудита и их примеры

Каждая запись аудита регистрируются в формате: `[Дата][termidesk.audit.events.`Наименование события`]` `[Текст события согласно шаблону]`.

Пример регистрации события аудита «Изменение системных параметров «Универсального диспетчера»:

Дата	Событие	Текст события
28.08.2023, 16:55:35	termidesk.audit.events.web.SystemConfigChanged	«Пользователь "admin123(Встроенный)" изменил системные параметры (ip-адрес 192.0.2.1)»

Пример регистрации события аудита «CRUD операции с объектами через REST API»:

Дата	Событие	Текст события
28.08.2023, 17:02:59	termidesk.audit.events.web.EntityAction	«Пользователь "u(Встроенный)" выполнил операцию read для объекта Provider (c1305fb0-e2ab-5fae-905b-b441c816f1f9) SessionsPlatform "RDS Provider (ip)" (ip-адрес 192.0.2.1)»

Пример регистрации события аудита «Пользователь неактивен»:

Дата	Событие	Текст события
28.08.2023, 17:04:00	termidesk.audit.events.workplace.UserIdle	«Пользователь "user1(FreeIPA)" неактивен в гостевой ОС ВМ a17olf-a17s-120(192.0.2.1) фонда a17olf-a17s-2 как пользователь u»

14.6 . Отслеживание жизненного цикла сессий и ресурсов пользователей

Начиная с Termidesk версии 5.0 поддерживается возможность отследить действия пользователя по идентификаторам, которыми маркируются все события, относящихся к работе пользователя с Termidesk с момента его авторизации и до завершения работы с Termidesk:

- глобальный уникальный сессионный идентификатор (Global Unique Session ID, GUSID) - позволяет однозначно сопоставить пользователя и производимые им действия.

Присваивается в момент аутентификации пользователя в компоненте «Клиент» или на портале пользователя;

- уникальный идентификатор запуска ресурса (Unique Resource Start ID, URSI) - позволяет однозначно сопоставить пользователя и конкретный ресурс, который он получает - BPM и/или приложение. Присваивается в момент запуска пользователем ресурса.

Последовательность присвоения и отправки идентификаторов представлена на рисунке.

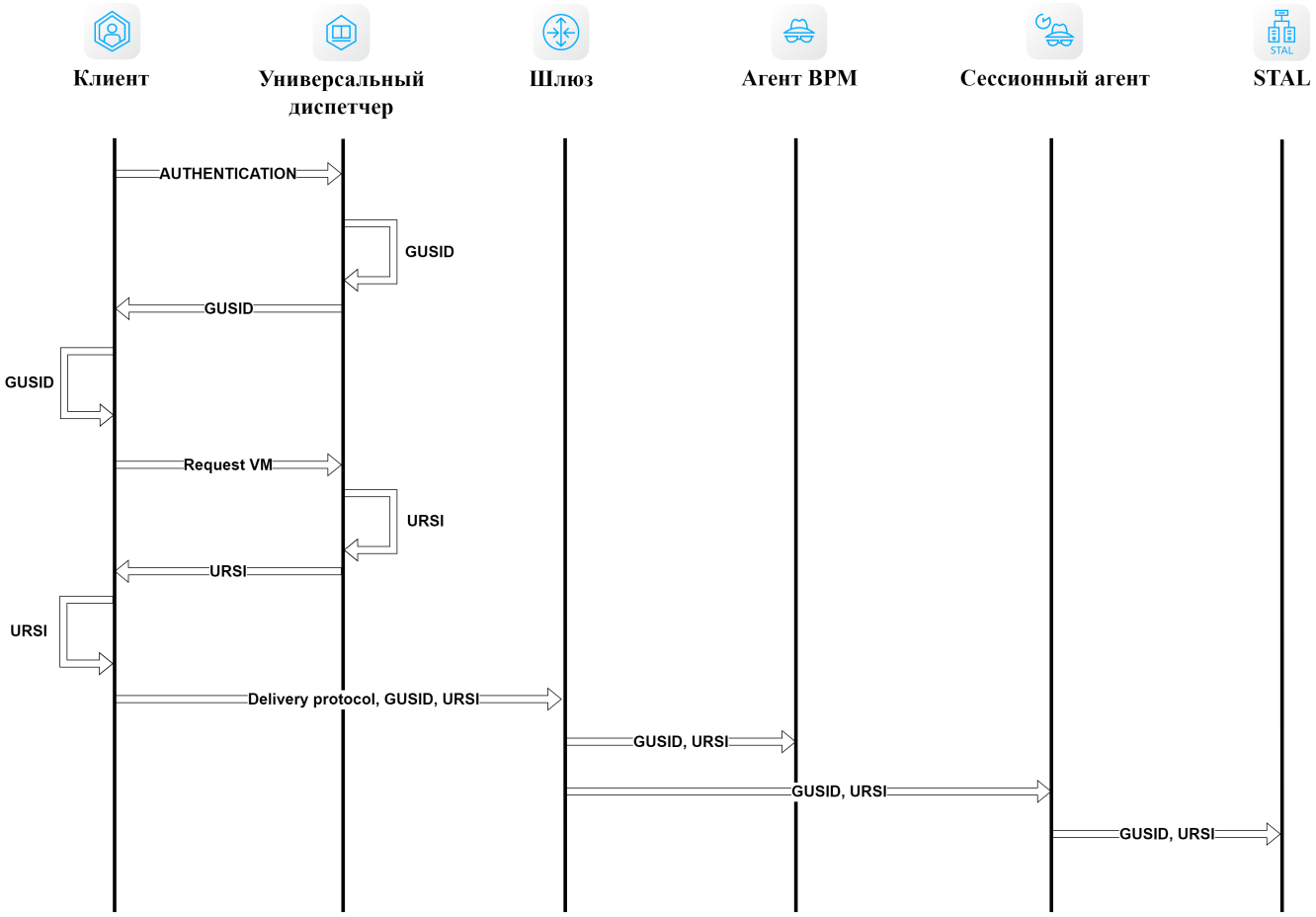

Рисунок 37 – Последовательность присвоения и отправки GUSID и URSI

Аннулирование GUSID происходит при:

- завершении сессии пользователя по истечении времени, заданного параметром «Длительность сессии пользователя» (см. подраздел **Параметры безопасности Termidesk**);
- отключении пользователя от «Универсального диспетчера»;
- закрытии компонента «Клиент» пользователем;
- запуске нового экземпляра компонента «Клиент» на той же пользовательской рабочей станции;

- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении пользователя к «Универсальному диспетчеру» будут назначены новые идентификаторы.

Аннулирование URSI происходит при:

- закрытии пользователем окна опубликованного приложения или выходе из сеанса BPM (`logoff`);
- отключении от сеанса BPM (`disconnect`);
- закрытии компонента «Клиент» и окна программы доставки BPM (`termidesk-viewer`);
- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении пользователя к «Универсальному диспетчеру» будут назначены новые идентификаторы

GUSID и URSI регистрируются в журналах:

- компонента «Сессионный агент»;
- компонента «Агент виртуального рабочего места».

События, связанные с GUSID и URSI, хранятся в БД. Они доступны для просмотра в журнале на портале Termidesk (см. подраздел **Просмотр журналов**). Пример сообщения от источника «agent»: «preConnect. User: u, Protocol: spice, GUSID: 93418bcd-5c95-5f46-ae1b-980a8519ae8f, URSI: 73fe89e3-5fe4-5b02-81a8-06b8e3bac2d1».

15 . УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ TERMIDESK

15.1 . Обзор и управление инфраструктурой Termidesk

Раздел «Инфраструктура» предназначен для использования в качестве единого центра управления при распределенной установке Termidesk. Он позволяет централизованно управлять компонентами и просматривать их статус на сервере.

Просмотр компонентов и их состояния также доступен в разделе «Обзор» (см. Рисунок 38), наименования элементов в котором служат активной ссылкой на соответствующий подраздел веб-интерфейса.

Состояние компонента визуализируется пиктограммой:

-  - количество узлов, находящихся в статусе «ok», который вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «maintance» (техобслуживание), который вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «error» (ошибка), который вернул запрос `healthcheck`;
-  - количество узлов, находящихся в статусе «unknown» (неизвестно). Статус появляется, если после регистрации компонента еще не было ни одной попытки запроса состояния `healthcheck`.

По умолчанию запрос состояния компонентов производится с интервалом 60 секунд.

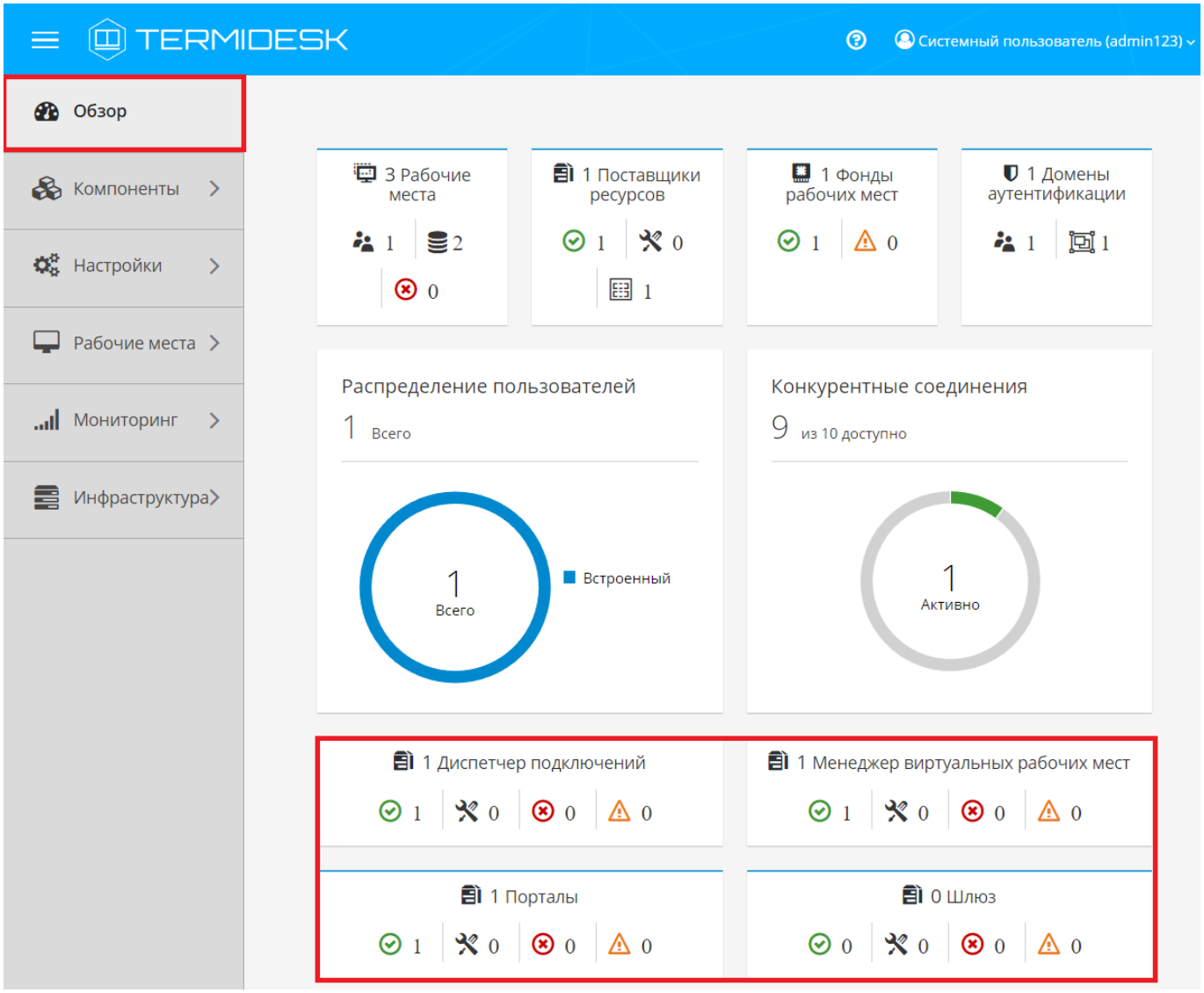

Рисунок 38 – Отображение компонентов в разделе «Обзор»

Регистрация компонента в системе происходит через подключение к серверу RabbitMQ, который хранит информацию об узле компонента и передает ее компоненту «Менеджер рабочих мест» (`termidesk-taskman`) для обработки и добавления в таблицу раздела «Инфраструктура». Регистрация компонентов происходит при их запуске.

Для получения списка компонентов Termidesk нужно перейти в раздел «Инфраструктура» (см. Рисунок 39) и выбрать интересующий элемент:

- «Диспетчеры подключений»;
- «Менеджеры BPM»;
- «Порталы»;
- «Шлюзы» (`termidesk-gateway`).

По умолчанию записи в представленной таблице будут упорядочены согласно столбцу «Имя». Для удаления узла компонента из таблицы следует выбрать нужный компонент и нажать экранную кнопку **[Удалить]**.

Удаление компонента из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова.

Отображение таблиц будет доступно администратору, если у него есть разрешение «Просмотр объектов инфраструктуры».
Удаление узла компонента из таблицы будет доступно администратору, если у него есть разрешение «Удаление объектов инфраструктуры».

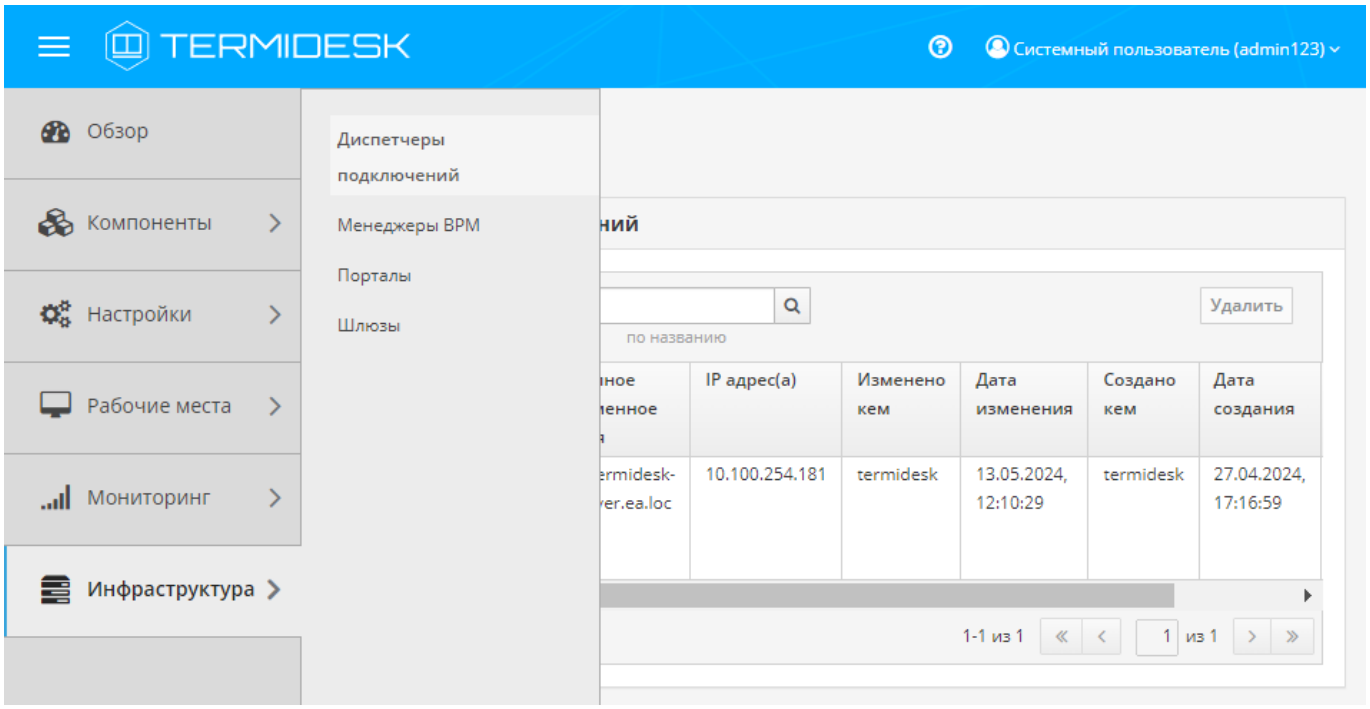

Рисунок 39 – Пример отображения списка элементов инфраструктуры

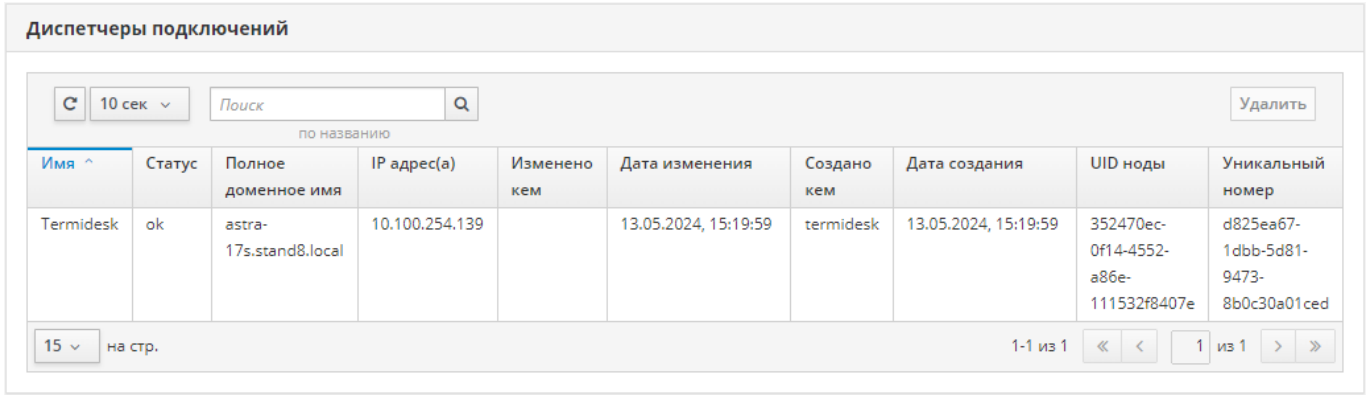

Рисунок 40 – Пример отображения записей мониторинга

Основные регистрируемые параметры приведены в таблице (см. Таблица 54).

Таблица 54 – Основные параметры списка элементов инфраструктуры

Параметр	Описание
«Имя»	Наименование компонента
«Роль»	Параметр доступен только для элемента «Портал», т.к определяет тип портала, с которым установлен компонент «Универсальный диспетчер». Может быть: «admin» (административный), «user» (пользовательский), «universal» (универсальный, если установлены «admin» и «user»)
«Статус»	Текущее состояние компонента, может принимать значения: ▪ «ok» - компонент нормально функционирует; ▪ «failed» - компонент функционирует с ошибками; ▪ «unknown» - состояние неизвестно или не поддерживается
«Полное доменное имя»	Полное доменное имя узла, на котором запущен компонент
«IP адрес(а)»	Список IP-адресов на узле, на котором запущен компонент
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который запустил компонент
«Дата создания»	Дата создания записи в таблице о компоненте
«UID ноды»	Системный UUID (Universally Unique Identifier, уникальный идентификатор) узла, на котором установлен компонент
«Уникальный номер»	Уникальный идентификатор компонента

16 . РЕЖИМ ВЫСОКОЙ ДОСТУПНОСТИ И РАБОТА С СЕРТИФИКАТАМИ

16.1 . Настройка «Менеджера рабочего места» в режиме высокой доступности

Настройка выполняется после установки программного комплекса в распределенной конфигурации.

Последовательность настройки узлов с компонентом «Менеджер рабочих мест» следующая:

- на узле, выбранном в качестве `master`, помимо уже запущенных служб, запустить только службу `termidesk-taskman`, не добавляя ее в раздел автоматической загрузки:

```
:~$ sudo systemctl start termidesk-taskman
```

- на узлах `master` и `slave` установить пакеты программ для организации высокой доступности:

```
:~$ sudo apt install -y keepalived ipset
```

где:

`-y` - ключ для пропуска подтверждения установки;

- на узлах `master` и `slave` создать каталог `/etc/keepalived/` (если каталог ранее не был создан):

```
:~$ sudo mkdir -p /etc/keepalived
```

где:

`-p` - ключ для создания подкаталогов в указанном пути, если их не существует;

- на узлах `master` и `slave` в каталоге `/etc/keepalived/` создать пустые файлы `keepalived.conf` (файл настроек режима высокой доступности) и `notify.sh` (управление переключениями режимов высокой доступности):

```
:~$ sudo touch /etc/keepalived/keepalived.conf
:~$ sudo touch /etc/keepalived/notify.sh
```

- отредактировать созданный файл `/etc/keepalived/keepalived.conf`, приведя его к следующему виду (по очереди на каждом из узлов):

> ⚠ Значения параметров в файле `keepalived.conf` приведены в качестве примера. Значения должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре предприятия.

```
global_defs {

```

```
    router_id NAME_OF_ROUTER_ID # НУЖНО УКАЗАТЬ: hostname хоста
    script_user user # НУЖНО УКАЗАТЬ: вместо user -> пользователь, от имени которого запускается keepalived
    enable_script_security
}

vrrp_script check_httpd {
    script "/usr/bin/pgrep apache" # path of the script to execute
    interval 1  # seconds between script invocations, default 1 second
    timeout 3   # seconds after which script is considered to have failed
    #weight <INTEGER:-254..254>  # adjust priority by this weight, default 0
    rise 1              # required number of successes for OK transition
    fall 2              # required number of successes for KO transition
    #user USERNAME [GROUPNAME]   # user/group names to run script under
    init_fail                   # assume script initially is in failed state
}

# Для каждого виртуального IPv4-адреса создается свой экземпляр vrrp_instance
vrrp_instance termidesk-taskman {
    notify /etc/keepalived/notify.sh

    # Initial state, MASTER|BACKUP
    # As soon as the other machine(s) come up,
    # an election will be held and the machine
    # with the highest priority will become MASTER.
    # So the entry here doesn't matter a whole lot.
    state BACKUP

    # interface for inside_network, bound by vrrp
    # НУЖНО УКАЗАТЬ: eth0 -> интерфейс, смотрящий в Интернет
    interface eth0

    # arbitrary unique number from 0 to 255
    # used to differentiate multiple instances of vrrpd
    # running on the same NIC (and hence same socket).
    # НУЖНО УКАЗАТЬ: вместо 106 -> номер экземпляра vrrp_instance
    virtual_router_id 106

    # for electing MASTER, highest priority wins.
    # to be MASTER, make this 50 more than on other machines.
    # НУЖНО УКАЗАТЬ: вместо 128 -> приоритет экземпляра vrrp_instance
    priority 128

    preempt_delay 5 # Seconds

    # VRRP Advert interval in seconds (e.g. 0.92) (use default)
    advert_int 1

    # НУЖНО УКАЗАТЬ: вместо IP_ADDRESS_OF_THIS_HOST -> IPv4-адрес интерфейса, смотрящего в Интернет
    unicast_src_ip IP_ADDRESS_OF_THIS_HOST

    authentication {
        auth_type PASS
```

```
        # НУЖНО УКАЗАТЬ: ksedimret -> заменить на безопасный пароль
        auth_pass ksedimret
    }

    virtual_ipaddress {
        # НУЖНО УКАЗАТЬ: вместо VIRTUAL_IP_ADDREESS/MASK -> виртуальный IPv4-адрес и сетевой префикс с интерфейса, смотрящего в Интернет
        # НУЖНО УКАЗАТЬ: вместо eth0 -> интерфейс, смотрящий в Интернет
        # НУЖНО УКАЗАТЬ: вместо eth0:<значение> -> интерфейс, смотрящий в Интернет:4-й октет виртуального IPv4-адреса
        VIRTUAL_IP_ADDREESS/MASK dev eth0 label eth0:<значение>
    }

    track_script {
        check_httpd
    }
}
```

где:

`script_user` - значение этого параметра соответствует наименованию пользователя, от имени которого запускается служба `keepalived` (обычно - `root`);

`NAME_OF_ROUTER_ID` - имя зоны маршрутизации VRRP (общее для узлов `master` и `slave`);

`IP_ADDREESS_OF_THIS_HOST` - текущий статический IP-адрес узла, на котором запускается служба `keepalived`;

`VIRTUAL_IP_ADDRESS/MASK` - виртуальный статический IP-адрес и маска (общие для узлов `master` и `slave`);

`eth0:<значение>` - значение четвертого октета виртуального IPv4-адреса. Например, если используется виртуальный статический IP-адрес 192.0.2.30, то данный параметр примет значение `eth0:30`;

> ⚠ В рамках одной распределенной установки значение `NAME_OF_ROUTER_ID` параметра `router_id` должно быть идентичным. Если в сети или в одном VLAN присутствуют несколько распределенных установок Termidesk, то значение `NAME_OF_ROUTER_ID` параметра `router_id` должно быть уникальным для каждого экземпляра установки.

- по очереди на каждом из узлов `master` и `slave` отредактировать созданный файл `/etc/keepalived/notify.sh`, приведя его к следующему виду:

```
#!/bin/sh -e

SELF_BIN=$(realpath ${0})
SELF_DIR=$(dirname ${SELF_BIN})
TYPE=${1}
NAME=${2}
STATE=${3}
PRIORITY=${4}
TASKMAN_SYSTEMCTL_NAME="termidesk-taskman"
```

```
TASKMAN_SYSTEMCTL_DESCRIPTION="Termidesk-VDI Taskman daemon"
TASKMAN_SYSTEMCTL_PIDFILE="/run/termidesk-taskman/pid"
msg2log () {
    logger -i "Termidesk: ${1}"
}
taskman_stop () {
    msg2log "Stopping ${TASKMAN_SYSTEMCTL_NAME} service"
    systemctl is-active -q ${TASKMAN_SYSTEMCTL_NAME} && systemctl stop -q ${TASKMAN_SYSTEMCTL_NAME}
}
taskman_start () {
    msg2log "Starting ${TASKMAN_SYSTEMCTL_NAME} service"
    systemctl is-active -q ${TASKMAN_SYSTEMCTL_NAME} || systemctl start -q ${TASKMAN_SYSTEMCTL_NAME}
}
# VRRP event type: INSTANCE, name: lsb_40, state: BACKUP, priority: 64
msg2log "VRRP event type: ${TYPE}, name: ${NAME}, state: ${STATE}, priority: ${PRIORITY}"
case ${STATE} in
    BACKUP)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_stop
    ;;
    FAULT)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_stop
    ;;
    MASTER)
        [ "${NAME}" = "${TASKMAN_SYSTEMCTL_NAME}" ] && taskman_start
    ;;
    *)
        msg2log "Error: unknown state ${STATE}"
        exit 1
    ;;
esac
exit 0
```

- на узлах `master` и `slave` сделать файл `notify.sh` исполняемым:

```
:~$ sudo chmod +x /etc/keepalived/notify.sh
```

- на узлах `master` и `slave` добавить в автоматическую загрузку и запустить сервис `keeaplived`:

```
:~$ sudo systemctl enable keepalived
:~$ sudo systemctl start keepalived
```

16.2 . Настройка балансировщика для работы с самоподписанными сертификатами

16.2.1 . Создание самоподписанного SSL-сертификата

Для создания самоподписанного SSL-сертификата и ключа к нему нужно:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;

- выполнить генерацию SSL-сертификата (`/etc/ssl/certs/nginx-selfsigned.crt`) и ключа к нему (`/etc/ssl/private/nginx-selfsigned.key`):

```
:~$ sudo openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```

Используемые ключи команды:

- `openssl` - базовый инструмент командной строки для создания и управления сертификатами, ключами и другими файлами OpenSSL;
- `req` - эта опция указывает, что на данном этапе нужно использовать запрос на подпись сертификата X.509 (CSR). X.509 – это стандарт инфраструктуры открытого ключа, которого придерживаются SSL и TLS при управлении ключами и сертификатами. Данная команда позволяет создать новый сертификат X.509;
- `new` - эта опция указывает, что будет создаваться новый запрос;
- `x509` - эта опция вносит поправку в предыдущую команду, сообщая утилите о том, что вместо запроса на подписание сертификата необходимо создать самоподписанный сертификат;
- `nodes` - ключ для пропуска опции защиты сертификата парольной фразой. Нужно, чтобы при запуске балансировщик нагрузки (nginx) имел возможность читать файл без вмешательства пользователя. Установив пароль, придется вводить его после каждой перезагрузки;
- `days 365` - эта опция устанавливает срок действия сертификата (в данном случае сертификат действителен в течение года);
- `newkey rsa:2048` - эта опция позволяет одновременно создать новый сертификат и новый ключ. Поскольку ключ, необходимый для подписания сертификата, не был создан ранее, нужно создать его вместе с сертификатом. Данная опция создаст RSA-ключ размером 2048 бит;
- `keyout` - эта опция сообщает OpenSSL, куда поместить сгенерированный файл ключа;
- `out` - эта опция сообщает OpenSSL, куда поместить созданный сертификат.

После исполнения команды надо последовательно ввести ряд параметров, запросы на которые отобразятся в командной строке:

- `Country Name` (2 letter code) [AU];
- `State or Province Name` (full name) [Some-State];
- `Locality Name` (eg, city) [];
- `Organization Name` (eg, company) [Internet Widgits Pty Ltd];
- `Organizational Unit Name` (eg, section) [];
- `Common Name` (e.g. server FQDN or YOUR name) [];

- `Email Address` [].

Наиболее важным параметром является `Common Name` (необходимо ввести FQDN-имя балансировщика). Как правило, в эту строку вносят доменное имя, с которым нужно связать сервер. В случае если доменного имени нет, нужно внести в эту строку IP-адрес сервера.

Файлы ключа и сертификата будут размещены в каталоге, указанном при вызове команды `openssl` в параметрах `keyout` и `out`.

При использовании OpenSSL необходимо также создать ключи Диффи-Хеллмана, для этого:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;
- сгенерировать ключи Диффи-Хеллмана длиной 4096 бит и сохранить их в файл `/etc/nginx/dhparam.pem`:

```
:~$ sudo openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

16.2.2 . Настройка nginx для поддержки SSL

Для настройки nginx нужно:

- создать новый пустой сниппет nginx в каталоге `/etc/nginx/snippets` для указания размещения сертификата и ключа:

```
:~$ sudo touch /etc/nginx/snippets/self-signed.conf
```

- отредактировать созданный файл, приведя его к виду:

```
1 ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
2 ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

- создать еще один пустой сниппет, предназначенный для настроек SSL (это позволит серверу nginx использовать надежный механизм преобразования и включит некоторые дополнительные функции безопасности):

```
:~$ sudo touch /etc/nginx/snippets/ssl-params.conf
```

- отредактировать созданный файл `ssl-params.conf`, приведя его к виду:

```
1 ssl_protocols TLSv1.3;
2 ssl_prefer_server_ciphers on;
3 ssl_dhparam /etc/nginx/dhparam.pem;
4 ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-
  AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
5 ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
6 ssl_session_timeout  10m;
7 ssl_session_cache shared:SSL:10m;
```

```
ssl_session_tickets off; # Requires nginx >= 1.5.9
ssl_stapling on; # Requires nginx >= 1.3.7
ssl_stapling_verify on; # Requires nginx => 1.3.7
resolver 77.88.8.8 77.88.8.1 valid=300s;
resolver_timeout 5s;
# Disable strict transport security for now. You can uncomment the following
# line if you understand the implications.
# add_header Strict-Transport-Security "max-age=63072000; includeSubDomains;
preload";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
add_header X-XSS-Protection "1; mode=block";
```

⚠ Поскольку сертификат является самоподписанным, `SSL stapling` не будет использоваться. Сервер nginx выдаст предупреждение, отключит `stapling` для данного сертификата и продолжит работу.

16.2.3 . Конфигурирование веб-сервера

Для конфигурирования веб-сервера нужно:

- создать пустой конфигурационный файл:

```
:~$ sudo touch /etc/nginx/sites-available/sampledomain.ru.conf
```

- отредактировать созданный файл, приведя его к виду:

⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре предприятия.

```
upstream daas-upstream-ws {
 least_conn;
    # PROXY TERMIDESK

     server 192.0.2.41:5099;
     server 192.0.2.42:5099;
     server 192.0.2.43:5099;
     server 192.0.2.44:5099;

}

upstream daas-upstream-nodes {
 least_conn;
     # DISPATCHER TERMIDESK

     server 192.0.2.30:443;
     server 192.0.2.31:443;
     server 192.0.2.32:443;
```

```
 }

server {
 listen 0.0.0.0:80;
 listen 0.0.0.0:443 ssl;

  include snippets/self-signed.conf;
  include snippets/ssl-params.conf;

 location /websockify {
         # limit_req zone=fast nodelay;
        proxy_http_version 1.1;
        proxy_pass http://daas-upstream-ws/;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

        # Connection timeout
        proxy_connect_timeout 1000;
        proxy_send_timeout 1000;
        proxy_read_timeout 1000;
        send_timeout 1000;

        # Disable cache
        proxy_buffering off;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }

 location / {
        proxy_pass https://daas-upstream-nodes/;

        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-Proto $scheme;

 }

}
```

⚠ IP-адреса, перечисленные в директиве `daas-upstream-ws`, являются адресами «Шлюзов» Termidesk, а IP-адреса, перечисленные в директиве `daas-upstream-nodes`, являются адресами «Универсальных диспетчеров» Termidesk.

- создать символическую ссылку на данный виртуальный хост из директории `/etc/nginx/sites-available` в директорию `/etc/nginx/sites-enabled`, чтобы nginx его обслуживал:

```
:~$ sudo ln -s /etc/nginx/sites-available/sampledomain.ru.conf /etc/nginx/sites-enabled/
```

- проверить корректность настроек:

```
:~$ sudo nginx -t
```

```
1  nginx: [warn] "ssl_stapling" ignored, issuer certificate not found
2  nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
3  nginx: configuration file /etc/nginx/nginx.conf test is successful
```

⚠ Веб-сервер возвращает предупреждение в случае использования самоподписанного сертификата, однако это не влияет на работу.

- если в синтаксисе обнаружены ошибки, необходимо исправить их, затем перезапустить веб-сервер:

```
:~$ sudo systemctl restart nginx
```

17 . ЭКСПЕРИМЕНТАЛЬНЫЕ ФУНКЦИИ

17.1 . Перечень переменных окружения «Универсального диспетчера»

В Termidesk используются переменные для указания параметров настройки компонентов программного комплекса.

Перечень переменных и параметров, используемых компонентом «Универсальный диспетчер», приведены в таблице (см. Таблица 55).
Перечень переменных, используемых в других компонентах программного комплекса, приведен в соответствующих им документах.

Таблица 55 – Переменные окружения Termidesk

Переменная окружения	Значение по умолчанию	Описание
«Универсальный диспетчер»		
`TDSK_AUTOFS_IMAGES_ID`	Не задано	Используется для настройки шаблонов переносимых профилей. В качестве значения используются идентификаторы дисков. Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]`. Значение переменной задается в файле `/etc/opt/termidesk-vdi/termidesk.conf`
`DBHOST`	Не задано	IP-адрес или FQDN СУБД PostgreSQL. Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBPORT`	`5432`	Порт, который используется для соединения с сервером БД. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBSSL`	Не задано	Протокол, использующийся при подключении к БД. Возможные значения: `Disable`, `TLSv1.2`, `TLSv1.3`. Начальное значение задается на этапе установки Termidesk. Изменить значение можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBNAME`	Не задано	Имя БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`
`DBUSER`	Не задано	Имя пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk. Изменить значение переменной можно через файл `/etc/opt/termidesk-vdi/termidesk.conf`

DBPASS	Не задано	Пароль пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде. ⚠ В стандартных установках значения менять не следует. Изменить значение переменной можно через файл /etc/opt/termidesk-vdi/termidesk.conf. Для получения преобразованного значения пароля следует воспользоваться утилитой scramble: :~$ sudo /opt/termidesk/bin/scramble -v <пароль> Утилита scramble использует в качестве вектора преобразования значение из файла /etc/opt/termidesk-vdi/termidesk.cookie. Значение генерируется автоматически на этапе установки Termidesk
DBCERT	Не задано	Путь к сертификату mTLS для защищенного подключения к БД. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf ⚠ mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов.
DBKEY	Не задано	Путь к ключу mTLS для защищенного подключения к БД. Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: :~$ openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key Изменить значение переменной DBKEY можно через файл /etc/opt/termidesk-vdi/termidesk.conf
DBCHAIN	Не задано	Путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к БД. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
DJANGO_SECRET_KEY	Не задано	Параметр, используемый для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределенной установке. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf

RABBITMQ_URL	Не задано	Параметры для подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов. Начальное значение задается на этапе установки Termidesk. Значение этого параметра записывается в файл /etc/opt/termidesk-vdi/termidtermidesk-vdi/termidesk.conf. Пароль, указанный для подключения к серверу RabbitMQ хранится в преобразованном виде. Этот функционал реализован, начиная с версии Termidesk 4.3.1, и применяется только для новых установок. При обновлении с более старой версии сохраняется значение этой переменной. При необходимости изменить пароль подключения следует получить преобразованное значение утилитой scramble и выполнить перезапуск служб Termidesk
RABBITMQ_SSL	Не задано	Протокол, использующийся при подключении к RabbitMQ. Возможные значения: Disable, TLSv1.2. Начальное значение задается на этапе установки Termidesk. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
NODE_ROLES	Не задано	Параметр, задающий тип роли, с которой будет установлен Termidesk. Возможные значения: ADMIN, USER, TASKMAN. Начальное значение задается на этапе установки Termidesk. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. Настройки будут применены после перезапуска службы termidesk-vdi. При переустановке Termidesk значение параметра в конфигурационном файле будет перезаписано
LOG_LEVEL	INFO	Уровень журналирования сообщений. Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
LOG_ADDRESS	/dev/log	Адрес для отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf
LOG_FACILITY	local3	Параметр, определяющий категорию сообщений syslog. Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf
HEALTH_CHECK_ACCESS_KEY	Не задано	Параметр для доступа к проверке состояния API сервера. Начальное значение генерируется на этапе установки Termidesk. Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. При задании значения параметра следует руководствоваться правилом, что: ▪ размер должен составлять от 0 до 64 символа; ▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
TASKMAN_HEALTH_CHECK_PORT	8100	Порт, на котором работает веб-сервер для обслуживания запросов проверки состояния API компонента «Менеджер рабочих мест». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)

TASKMAN_HEALTH_CHECK_CERT	/etc/opt/termidesk-vdi/taskman-healthcheck.pem	Путь к сертификату SSL/TLS для защищенного подключения к проверке состояния API компонента «Менеджер рабочих мест». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
TASKMAN_HEALTH_CHECK_KEY	/etc/opt/termidesk-vdi/taskman-healthcheck.key	Путь к ключу SSL/TLS для защищенного подключения к проверке состояния API компонента «Менеджер рабочих мест». Изменить значение можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
REQUESTS_CA_BUNDLE	Не задано	Путь к файлу с доверенным корневым сертификатом. Переменная используется для настройки работы с сертификатами собственных ЦС. Добавить переменную можно через файл /etc/opt/termidesk-vdi/termidesk.conf. По умолчанию переменная не используется (закомментирована)
EULA_ACCEPTED	Не задано	Параметр, определяющий принятие лицензионного соглашения при установке. Задается через файл /etc/opt/termidesk-vdi/termidesk.conf
Установочный пакет termidesk-vdi		
TDSK_PKG_DEBUG	Не задано	Включение режима отладки при установке пакета. Пример: TDSK_PKG_DEBUG=1

17.2 . Управление экспериментальными параметрами Termidesk

Включение и отключение экспериментальных параметров сервера Termidesk производится из командной строки.

Перечень экспериментальных параметров приведен в таблице (см. Таблица 56).

Таблица 56 – Экспериментальные параметры Termidesk

Параметр	Описание	Значение по умолчанию
experimental.2fa.enabled	Параметр поддержки двухфакторной аутентификации	0
experimental.deviceauth.enabled	Параметр поддержки авторизации устройств доступа	0
experimental.radiusauth.enabled	Параметр поддержки домена аутентификации RADIUS	0

Для активации экспериментального параметра необходимо присвоить ему значение 1, выполнив команды:

- переключиться на пользователя termidesk:

```
:~$ sudo -u termidesk bash
```

- активировать параметр:

```
:~$ /opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --section Experimental --key
experimental.2fa.enabled --value 1
```

где:

`experimental.2fa.enabled` - наименование параметра;

`1` - значение параметра для его активации;

`0` - значение параметра для его деактивации.

17.3 . Установка плагинов расширений

Экспериментальный функционал, не вошедший в основной релиз Termidesk, можно добавить в программный комплекс через установку плагинов расширений (каталог `addons` в комплектации поставки Termidesk).

Для установки плагинов нужно выполнить следующее:

- распаковать содержимое `zip`-архива в целевой каталог (например, `/tmp`);
- переключиться на пользователя `Termidesk`:

```
:~$ sudo -u termidesk bash
```

- перейти в каталог `Termidesk`:

```
:~$ cd /opt/termidesk/share/termidesk-vdi/
```

- активировать виртуальное окружение `Termidesk`:

```
:~$ source venv/bin/activate
```

- установить необходимый плагин:

```
1  :~$ pip install --upgrade --no-index --find-links /tmp/termidesk_internaldbauth
    termidesk_internaldbauth
```

где:

`/tmp/termidesk_internaldbauth` - каталог с `whl`-файлами;

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
:~$ exit
```

- обновить структуру БД и статических файлов командами:

```
1  :~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage migrate
2  :~$ sudo /opt/termidesk/sbin/termidesk-vdi-manage collectstatic --no-input
```

- перезапустить службу Termidesk:

```
1  :~$ sudo systemctl restart termidesk-vdi.service
```

17.4 . Удаление плагинов расширений

⚠ Перед удалением плагина необходимо удалить фонды BPM, шаблоны ВМ и поставщика ресурсов, соответствующих данному плагину.
Удаление фонда BPM может занять продолжительное время.

Для удаления плагина расширений нужно выполнить следующее:

- переключиться на пользователя `Termidesk`:

```
:~$ sudo -u termidesk bash
```

- перейти в каталог `Termidesk`:

```
:~$ cd /opt/termidesk/share/termidesk-vdi/
```

- активировать виртуальное окружение `Termidesk`:

```
:~$ source venv/bin/activate
```

- удалить необходимый плагин:

```
:~$ pip uninstall -y termidesk_internaldbauth
```

где:

`termidesk_internaldbauth` - имя плагина (без версии, платформы и расширения файла);

- выйти из окружения пользователя `Termidesk`:

```
:~$ exit
```

- перезапустить службу Termidesk:

```
1 :~$ sudo systemctl restart termidesk-vdi.service
```

17.5 . Откат к предыдущей версии плагина

Откат к предыдущей версии файла выполняется в той же последовательности, что и установка, однако вместо команды установки плагина используется следующая:

```
1 :~$ pip install --no-index --find-links /tmp/termidesk_internaldbauth
  termidesk_internaldbauth==4.0.1
```

где:

`/tmp/termidesk_internaldbauth` - каталог с `whl`-файлами, `whl`-файл с версией плагина должен существовать в данном каталоге;
`termidesk_internaldbauth` - имя плагина с указанием версии.

18 . РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ОТСЛЕЖИВАНИЯ СОСТОЯНИЯ КОМПОНЕНТОВ TERMIDESK

18.1 . Общие сведения по проверке состояния компонентов

Для отслеживания состояния компонентов Termidesk и обращения к ним для выполнения проверок состояния (health check) используется API-запрос `/api/health`.

Начальная спецификация схемы HealthCheck API в формате OpenAPI соответствует описанию:

```
openapi: 3.0.3
info:
  title: Termidesk health check api schema
  version: 0.1
paths:
  /api/health:
    get:
      responses:
        '200':
          description: Successful Response
          content:
            application/json:
              schema:
                type: object
                properties:
                  status:
                    type: string
                    enum: [pass, warn, fail]
                    example: fail
                    description: "Состояние компонента"
                  version:
                    type: string
                    example: 3.3
                    description: "Версия компонента"
                  description:
                    type: string
                    example: termidesk-taskman
                    description: "Описание компонента"
                  output:
                    type: string
                    example: "django.db.utils.OperationalError: FATAL:  password authentication failed for user 'termidesk'"
                    description: "Описание ошибки (если есть)"
                required:
                  - status
        '401':
          description: Authorization information is missing or invalid
```

Базовый URL для API: `/api/health`.

Тип контента: `application/json`.

Для каждого компонента Termidesk механизм проверки состояния должен быть доступен на порте, заданном в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`. Порт можно переопределить в этом же файле.

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу контролируется отдельным токеном. Значение токена задается конфигурационным файлом `/etc/opt/termidesk-vdi/termidesk.conf` в переменной `HEALTH_CHECK_ACCESS_KEY`.

Пример:

```
HEALTH_CHECK_ACCESS_KEY = "9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b"
```

18.2 . Состояние компонента «Универсальный диспетчер»

При распределенной установке Termidesk экземпляры компонента «Универсальный диспетчер» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик трафика, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Компонент изначально задействован для работы по протоколу HTTP, поэтому механизм проверки состояния реализуется отдельными вызовами REST API.

Пример команды проверки состояния компонента через утилиту `curl`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:${HEALTH_PORT}/api/health" -H 'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%{http_code}"
```

18.3 . Состояние компонента «Шлюз»

При распределенной установке Termidesk экземпляры компонента «Шлюз» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик трафика, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Пример команды проверки состояния компонента через утилиту `curl` :

```
:~$ curl -I -X 'GET' -H "Accept: text/plain" http://<IP-адрес_шлюза>:5099/info
```

Пример ответа для работоспособного компонента:

```
HTTP/1.1 200 OK
Date: Tue, 28 Nov 2023 07:37:51 GMT
uWebSockets: 20
Content-Length: 314
```

Код 200 в ответе на API-запрос свидетельствует о работоспособности компонента «Шлюз». Отсутствие ответа говорит о том, что компонент не работает. Данное правило необходимо добавить на балансировщике трафика.

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу компонента «Шлюз» `termidesk-gateway` контролируется отдельным токеном. Значение токена задается при запуске службы «Шлюза» в параметре `--healthCheckAccessKey`.

Для использования механизма проверки состояния компонента необходимо выполнить запуск Шлюза `termidesk-gateway` с указанием путей расположения сертификата и ключа (`--sslKey` и `--sslCert`), используемых для защищенного подключения.

Пример команды запуска службы `termidesk-gateway`:

```
:~$ termidesk-gateway --wssServerIP=0.0.0.0 --wssServerPort=8443 --sslKey=<путь_к_ключу> --sslCert=<путь_к_сертифкату> --urlCheckToken=http://<FQDN_Узла>/api/wsproxy/v1/verify --wsIdleTimeout=30 --mgtServerIP=0.0.0.0 --mgtServerPort=8102 --healthCheckAccessKey=<HEALTH_CHECK_ACCESS_KEY> --debug
```

Пример команды проверки состояния компонента через утилиту `curl` для компонента «Шлюз» `termidesk-gateway`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:8102/api/health" -H 'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%{http_code}"
```

18.4 . Состояние компонента «Менеджер рабочих мест»

При распределенной установке Termidesk экземпляры компонента «Менеджер рабочих мест» могут быть установлены на нескольких узлах, но активен должен быть только один из них. Все остальные компоненты являются резервными и, по умолчанию, находятся в состоянии «Passive».

Для использования механизма проверки состояния компонента необходимо в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` раскомментировать строки параметров `TASKMAN_HEALTH_CHECK_PORT`, `TASKMAN_HEALTH_CHECK_CERT`, `TASKMAN_HEALTH_CHECK_KEY`. Для параметров `TASKMAN_HEALTH_CHECK_CERT`, `TASKMAN_HEALTH_CHECK_KEY` нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk.

Пример задания значений:

```
TASKMAN_HEALTH_CHECK_PORT=8100
TASKMAN_HEALTH_CHECK_CERT=/etc/opt/termidesk-vdi/taskman-healthcheck.pem
TASKMAN_HEALTH_CHECK_KEY=/etc/opt/termidesk-vdi/taskman-healthcheck-decrypted.key
```

Пример команды проверки состояния компонента через утилиту `curl`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:8100/api/health" -H 'accept: application/
json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%
{http_code}"
```

19 . НЕШТАТНЫЕ СИТУАЦИИ

19.1 . Нештатные ситуации и способы их устранения

Возможные неисправности при работе с Termidesk и способы их устранения приведены в таблице (см. Таблица 57).

Таблица 57 – Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «СБОЙ: оставшиеся слоты подключений зарезервированы для подключений суперпользователя (не для репликации)»	Ошибка возникает при попытке авторизации на сервере Termidesk	Изменить максимальное количество подключений в настройках БД: изменить значение `max_connections` в конфигурационном файле `/etc/postgresql/11/main/postgresql.conf` в бОльшую сторону
Ошибка: «SSL: WRONG_VERSION_NUMBER] wrong version number (_ssl.c:1056)»	Ошибка возникает, если сервер поставщика ресурсов не поддерживает SSL	Необходимо отредактировать поставщика ресурсов, выставив параметру «Использовать SSL» значение «Нет»
Ошибка: «kinit: Client 'HTTP/termidesk.local@LOCAL' not found in Kerberos database while getting initial credentials»	Ошибка возникает при добавлении или редактировании домена аутентификации FreeIPA	Необходимо создать указанную учетную запись на КД FreeIPA

Ошибка при установке пакета:
«Невозможно найти пакет» или «Неудовлетворенные зависимости»
	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:
		`:~$ sudo apt update`
		После этого нужно вновь выполнить команду установки пакета.
		Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:
		`:~$ sudo apt -f install`
		Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов.

Индикация	Описание	Возможное решение

Ошибка при установке пакета:
«Невозможно найти пакет» или «Неудовлетворенные зависимости»
	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:
		`:~$ sudo apt update`
		После этого нужно вновь выполнить команду установки пакета.
		Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:
		`:~$ sudo apt -f install`
		Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов

20 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»
Виртуальное рабочее место	Также: ВРМ. Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа
Гостевая ОС	ОС, функционирующая на ВМ
Группы рабочих мест	Также: группы ВРМ. Функциональное объединение множества фондов ВРМ по определенному признаку
Домен аутентификации	Способ проверки субъектов и их полномочий
Компонент «Менеджер рабочих мест»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-taskman.service`
Поставщик ресурсов	ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов ВРМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к ВРМ
Компонент «Сессионный агент»	Компонент Termidesk. Устанавливается на сервер терминалов (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям
Компонент «Универсальный диспетчер»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им ВРМ и контроля доставки ВРМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Фонд рабочих мест	Также: фонд ВРМ. Совокупность подготовленных ВРМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Шаблон рабочего места	Также: шаблон ВРМ. Параметры конфигурации базового ВРМ для использования в фонде ВРМ
Компонент «Шлюз»	Компонент Termidesk. Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. В более старой реализации устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-wsproxy.service`. В новой реализации устанавливается из пакета `termidesk-gateway`, поддержка старой реализации удалена, начиная с Termidesk версии 5.0. Наименование службы после установки: `termidesk-gateway.service`.
Компонент «Сервер терминалов Astra Linux»	Компонент Termidesk. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к ВРМ с ОС Astra Linux Special Edition через сеанс удаленного терминала
Портал администратора	Предоставляет веб-интерфейс для управления Termidesk и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API («auth», «discover», «health», «agent», «webui»).

Термин	Определение
Портал пользователя	Предоставляет пользовательский веб-интерфейс Termidesk (без доступа к функциям управления) и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API
Портал универсальный	Предоставляет функции обоих вариантов - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом swagger
Ключ	Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом
Сертификат	Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

21 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
ЭЦП	Электронная цифровая подпись
ALD	Astra Linux Directory (единое пространство пользователей)
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
FreeIPA	Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем)
GID	Group Identification Data (идентификатор группы)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IP	Internet Protocol (межсетевой протокол)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
OU	Organizational Unit (организационная единица)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
RDSH	Remote Desktop Session Host (хост сеансов удаленных рабочих столов)
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
STAL	Terminal Server Astra Linux (сервер терминалов ОС Astra Linux Special Edition (Server))
TCP	Transmission Control Protocol (протокол управления передачей)

Сокращение	Пояснение
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

UVEON
Unified Virtualization
Experience, Opportunities, Now

119571, г. Москва, Ленинский проспект,
д. 119А, помещ. 9Н
https://termidesk.ru/
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru