kaspersky

# Kaspersky Secure Remote Workspace:

- Kaspersky Thin Client
- Kaspersky Security Management Suite

# Оглавление

# О Решении

Kaspersky Secure Remote Workspace – решение (далее – «KSRW») для администрирования инфраструктуры тонких клиентов под управлением KasperskyOS, состоящее из трех компонентов:

- Kaspersky Thin Client (далее – «KTC») – программный продукт в виде операционной системы KasperskyOS с прикладным программным обеспечением для тонких клиентов, предназначенное для организации удаленного доступа к удаленным рабочим столам пользователей.
- Kaspersky Security Center (далее – «KSC») – программный продукт для централизованного мониторинга и управления KTC и некоторыми другими защитными решениями Лаборатории Касперского.
- Kaspersky Security Management Suite (далее – «KSMS») – программный продукт (веб-плагин) позволяет Kaspersky Security Center управлять Kaspersky Thin Client.

Версия компонентов программного обеспечения решения:

- Kaspersky Thin Client – 1.0.0.552
- Kaspersky Security Management Suite – 1.0.1.57
- Kaspersky Security Center – 12.0.0.7734

Основные функции системы:

- Подключение к физическим и виртуальным машинам под управлением операционной системы Microsoft Windows по протоколу RDP с авторизацией с помощью имени пользователя и пароля.
- Подключение к платформе виртуализации Скала-Р Виртуальное Рабочее Место (далее также Скала-Р ВРМ).
- Передача изображения экрана удаленной машины на монитор, подключенный к Kaspersky Thin Client.
- Передача событий от клавиатуры и мыши, подключенных к Kaspersky Thin Client, на удаленную машину.
- Передача USB-накопителей и смарт-карт, подключенных к Kaspersky Thin Client, на удаленную машину.

## Комплект поставки

Программное обеспечение Kaspersky Thin Client устанавливается и работает на аппаратной платформе тонкого клиента DEPO Sky 270.

В комплект поставки программно-аппаратного комплекса Kaspersky Secure Remote Workspace входит следующее:

- Программно-аппаратный комплекс DEPO Sky 270 с предустановленным программный продуктом Kaspersky Thin Client.
- Дистрибутив веб-плагина Kaspersky Security Management Suite: Web_Plugin_KOS_for_Thin_Client_1.0.1.57.zip.
- Текстовый файл с информацией о стороннем коде: LegalNotices.txt.
- Текстовый файл с описанием нового функционала и известных проблем: ReleaseNotes_KOS_for_Thin_Client_1.0_RU.txt.

## Принцип работы Kaspersky Thin Client

Типовая схема работы Kaspersky Thin Client (см. рис ниже) предполагает следующее:

- Kaspersky Thin Client, установленный на аппаратную платформу, получает параметры сети от DHCP-сервера, либо администратор настраивает параметры вручную.
- Администратор подключает настраивает взаимодействие между Kaspersky Thin Client и Kaspersky Security Center.
- Kaspersky Thin Client получает параметры подключения к удаленному рабочему столу, обновлений, доверенных сертификатов и перенаправления USB-устройств с политикой от Kaspersky Security Center, а параметры даты и времени администратор настраивает вручную.
- Пользователь подключается к удаленному рабочему столу по протоколу RDP, либо через платформу виртуализации Скала-Р.
- Kaspersky Thin Client отправляет журналы событий на сервер хранения журналов событий.
- Kaspersky Thin Client получает обновление программного обеспечения с сервера обновлений.


Типовая схема работы Kaspersky Thin Client

## Аппаратные и программные требования

Требования к мониторам, подключаемым к Kaspersky Thin Client
Поддерживаемые разрешения:

- 1920x1080.
- 1680x1050.
- 1024x768.

Поддерживаемые интерфейсы подключения:

- HDMI.
- VGA.
- Display Port.

### Требования к периферийным устройствам, подключаемым к Kaspersky Thin Client

Клавиатуры и мыши без мультимедийных функций, подключаемые по USB.

### Требования к удаленным рабочим столам

Вы можете подключаться к физическим компьютерам и виртуальным машинам. Поддерживаемые операционные системы:

- Windows 10.
- Windows Server 2012.

Поддерживаемые программы:

- Microsoft Office 2013:
  - Microsoft Word 2013.
  - Microsoft Excel 2013.
  - Microsoft Access 2013.
  - Microsoft Outlook 2013.
  - Microsoft PowerPoint 2013.
- Foxit Reader.
- WinRar.
- Google Chrome.
- Internet Explorer 11.
- Microsoft Teams (не поддерживаются аудио- и видео-конференции).

### Требования к сети

Скорость не менее 50 Мбит/с.

### Требования к серверу Kaspersky Security Center

О системных и программных требованиях к серверу Kaspersky Security Center см. в отдельном документе или онлайн-справке.
Kaspersky Thin Client поддерживает работу с Kaspersky Security Management Suite версии 12.1.

### Требования к серверам обновлений и серверам для отправки журналов событий

Серверы обновлений и серверы для отправки журналов событий разворачиваются специалистами "Лаборатории Касперского". Требования к серверам определяются специалистами "Лаборатории Касперского" в ходе указанных работ.

# Установка компонентов решения

## Установка веб-плагина управления Kaspersky Thin Client (Kaspersky Security Management Suite)

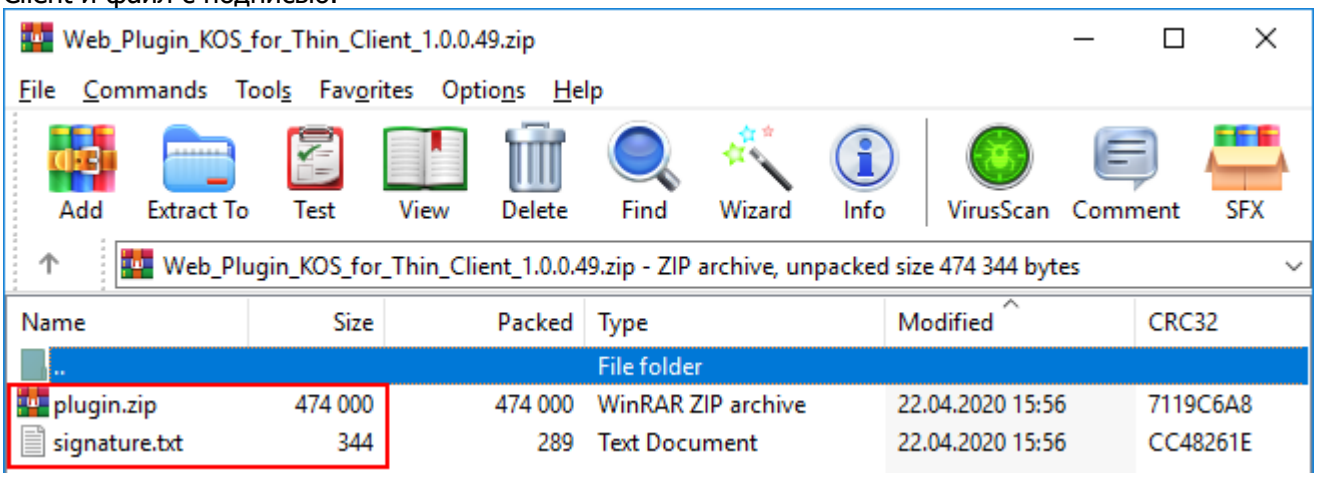
### О веб-плагине управления Kaspersky Thin Client (Kaspersky Security Managemet Suite)

Веб-плагин управления Kaspersky Thin Client (Kaspersky Security Managemet Suite, далее также KSMS) обеспечивает взаимодействие Kaspersky Thin Client с Kaspersky Security Center.
KSMS позволяет позволяет централизованно выполнять следующие действия:

- Управлять параметрами Kaspersky Thin Client в сети с помощью политик Kaspersky Security Center.
- Получать события из Kaspersky Thin Client.
- Устанавливать сертификаты безопасности на Kaspersky Thin Client.
- Осуществлять контроль лицензионных ключей на Kaspersky Thin Client.

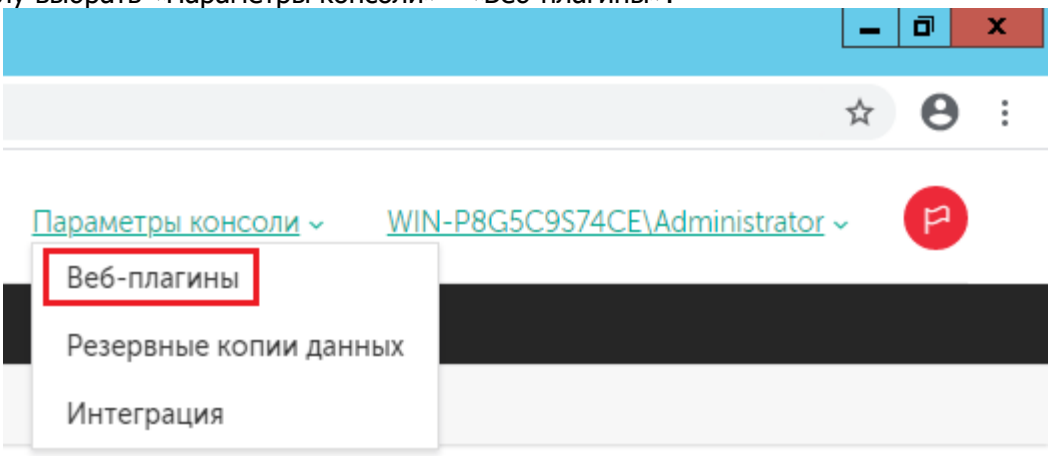
Веб-плагин по умолчанию не установлен в Kaspersky Security Management Suite. Веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Management Suite. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере.

KSMS поставляется в виде ZIP-архива, который содержит в себе архив с веб-плагином Kaspersky Thin Client и файл с подписью.

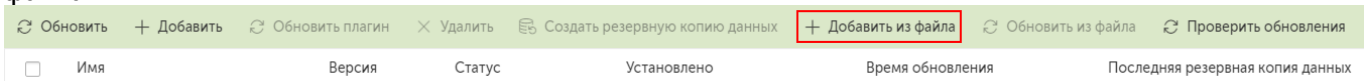



### Необходимые условия для установки Kaspersky Security Management Suite

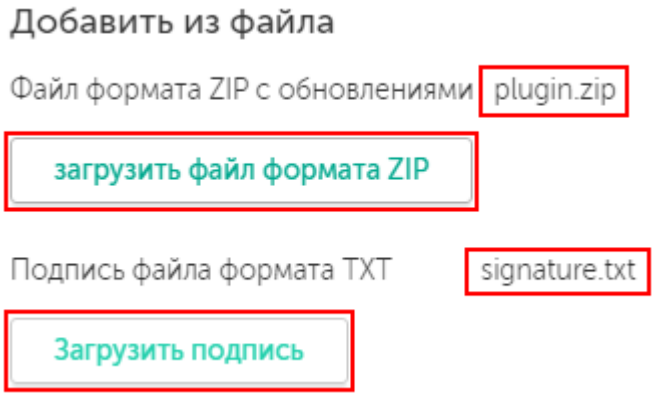
Перед установкой Kaspersky Security Management Suite необходимо установить Kaspersky Security Center, а также Kaspersky Security Management Suite.
На момент выпуска данного документа Kaspersky Thin Client поддерживает интеграцию только с KSC версии 12.0.0.7734 и новее.
Для установки Kaspersky Security Management Suite необходимо перейти в Web Console. В правом верхнем углу выбрать «Параметры консоли» - «Веб-плагины».



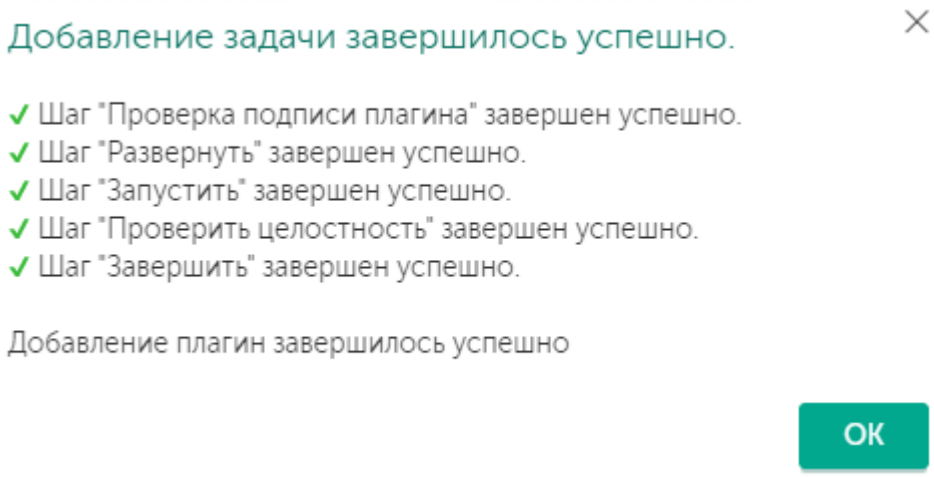

В открывшемся окне «Параметры консоли» на вкладке «Веб-плагины» выбрать пункт «Добавить из файла».



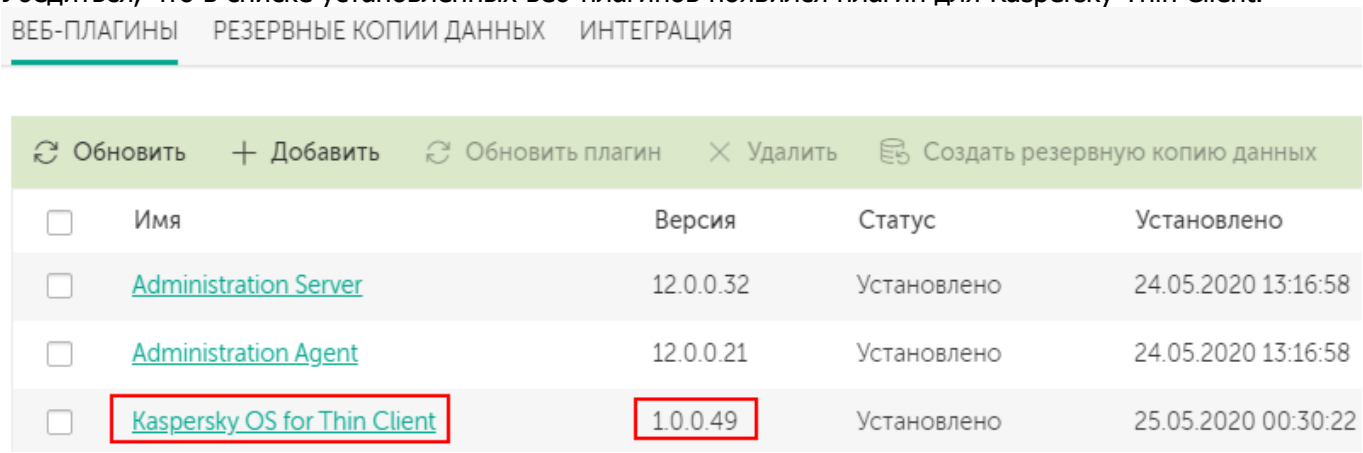
В открывшемся справа окне «Добавить из файла» выбрать архив с плагином (**plugin.zip**) и файл подписи (**signature.txt**).




Дождаться сообщения об успешном добавлении веб-плагина.




Убедиться, что в списке установленных веб-плагинов появился плагин для Kaspersky Thin Client.




# Прошивка тонкого клиента с помощь ПО Kaspersky Thin Client

## В каких случаях необходима прошивка тонкого клиента

В отдельных ситуациях может потребоваться выполнить перепрошивку тонкого клиента. Это может быть необходимо в следующих случаях:

- Подготовка нового устройства (DEPO Sky 270)
- Восстановление работы Kaspersky Thin Client после критических нарушений работоспособности
- Откат к релизной версии Kaspersky Thin Client после прохождения теста на обновление.

В последнем случае необходимость перепрошивки устройства обусловлена тем, что тонкий клиент поставляется с релизной версией Kaspersky Thin Client, в ходе теста он обновляется до промежуточной версии, а после завершения теста необходимо вернуть релизную версию Kaspersky Thin Client. Обновление на младшую версию в Kaspersky Thin Client не предусмотрено.

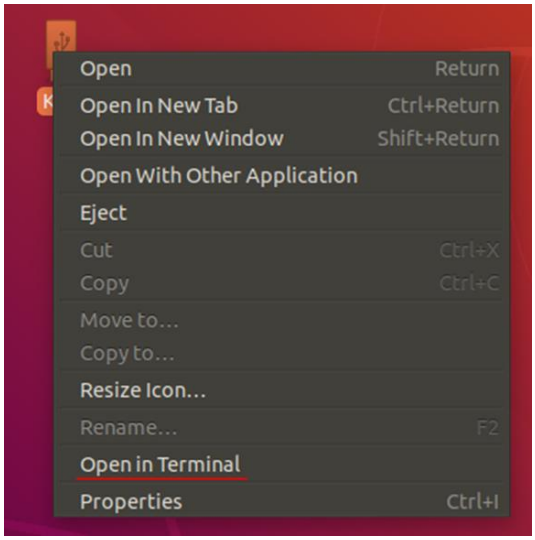
## Что необходимо для прошивки

Для перепрошивки тонкого клиента необходимо два USB-накопителя:
Live USB с Linux. Привязки к конкретной версии Linux нет. В данном руководстве используется Ubuntu 18.04 LTS.
С файлами Kaspersky Thin Client релизной версии.
Файлы необходимые для перепрошивки устройства необходимо запросить у инженера предпродажной поддержки «Лаборатории Касперского».

## Процедура прошивки

Необходимо загрузиться с Live USB. Параметры загрузки тонкого клиента можно отредактировать в настройках BIOS. После загрузки в рабочее пространство Ubuntu необходимо подключить устройство с файлами Kaspersky Thin Client релизной версии и перейти в директорию этого устройства с помощью командной строки.
Подключенное устройство располагается в **/media/ubuntu/<имя устройства>**. Перейти в директорию можно с помощью команды **cd**.

Также, можно нажать правой кнопкой мыши на иконку подключенного устройства на рабочем столе и выбрать пункт «**Open in Terminal**».




Далее необходимо перейти в директорию, содержащую файлы Kaspersky Thin Client релизной версии.

```
ubuntu@ubuntu:/media/ubuntu/KOS/1.0.0.552 (release)$ ll
total 29800
drwxr-xr-x 2 ubuntu ubuntu     8192 May 29 15:30 ./
drwxr-xr-x 5 ubuntu ubuntu     8192 Jan  1  1970 ../
-rw-r--r-- 1 ubuntu ubuntu   270218 May 29 14:40 KOS4TC-u-boot_1.0.0.552.tar.gz
-rw-r--r-- 1 ubuntu ubuntu 30203125 May 29 14:40 KOS_for_Thin_Client_1.0.0.552.tar.gz
-rw-r--r-- 1 ubuntu ubuntu    11074 May 28 10:26 ReleaseNotes_KOS_for_Thin_Client_1.0_RU.txt
-rw-r--r-- 1 ubuntu ubuntu     6192 May 29 14:40 kos4tc-1.0-uboot-install.sh
```

Для перепрошивки устройства необходимо запустить bash-скрипт с правами администратора:
**sudo bash kos4tc-1.0-uboot-install.sh -b KOS4TC-u-boot_1.0.0.552.tar.gz -u KOS_for_Thin_Client_1.0.0.552.tar.gz**

```
ubuntu@ubuntu:/media/ubuntu/KOS/1.0.0.552 (release)$ sudo bash kos4tc-1.0-uboot-install.sh -b
 KOS4TC-u-boot_1.0.0.552.tar.gz -u KOS_for_Thin_Client_1.0.0.552.tar.gz
```

После того как перепрошивка будет завершена в консоли отобразится соответствующее сообщение:

```
40+1 records in
40+1 records out
20704 bytes (21 kB, 20 KiB) copied, 0.00202936 s, 10.2 MB/s
/media/ubuntu/KOS/1.0.0.552 (release)
102400+0 records in
102400+0 records out
52428800 bytes (52 MB, 50 MiB) copied, 2.4588 s, 21.3 MB/s
/media/ubuntu/KOS/1.0.0.552 (release)
 Installed OK!
Remove USB drive and reboot.
ubuntu@ubuntu:/media/ubuntu/KOS/1.0.0.552 (release)$
```

Можно отключать USB-накопители и перезагружать тонкий клиент.

## Восстановление настроек BIOS после прошивки

После прошивки устройства рекомендуется скорректировать порядок загрузки в настройках BIOS таким образом, чтобы загрузка устройства производилась с встроенного в DEPO Sky 270 SSD-накопителя.

# Интерфейс Kaspersky Thin Client

Этот раздел содержит информацию об основных элементах интерфейса Kaspersky Thin Client.

## Обзор интерфейса Kaspersky Thin Client

Интерфейс содержит следующие элементы:

- Закладка Подключения.

  Позволяет подключиться к удаленным рабочим столам.

- Закладка Параметры.

  Позволяет настраивать параметры Kaspersky Thin Client.

- Закладка Инструменты.

  Позволяет просматривать информацию о работе Kaspersky Thin Client, обновлять Kaspersky Thin Client и работать с журналом событий.

- Панель состояния.

  Показывает статусную информацию о работе Kaspersky Thin Client.

- Панель подключения.

  Отображается в верхней части экрана в течение сессии подключения к удаленному рабочему столу. Показывает название удаленного рабочего стола и имя подключенного пользователя, а также позволяетзавершить сессию или послать сочетание клавиш **Alt+Ctrl+Del** на удаленный рабочий стол. Когда Kaspersky Thin Client скачивает обновление, на панели подключения появляется уведомление об этом.

## Закладка Подключения

В центре закладки Подключения отображаются две кнопки:

- Кнопка подключения к удаленному столу по протоколу RDP напрямую.
- Кнопка подключения к удаленным рабочим столам под управлением Скала-Р BPM.

## Окно подключения к удаленному рабочему столу

Окно подключения к удаленному рабочему столу содержит следующие элементы интерфейса:

- Поле Сервер.

  В этом поле указывается адрес RDP-сервера, к которому нужно подключиться.

  Kaspersky Thin Client сохраняет адрес последнего RDP-сервера, к которому было совершеноподключение, и вам не нужно вводить его при повторном подключении.

- Поле Имя пользователя.

  В этом поле указывается домен, если он требуется, и имя пользователя под которым осуществляетсяподключение к удаленному рабочему столу.

  Kaspersky Thin Client сохраняет имя пользователя, который последний раз подключался к RDP-серверу, и вам не нужно вводить его при повторном подключении.

- Поле Домен.

  Это поле заполняется автоматически, если заполнено поле Имя пользователя.

- Поле Пароль.

  В этом поле указывается пароль пользователя, под которым осуществляется подключение к удаленному рабочему столу.

  Пароль пользователя сбрасывается каждый раз, когда вы выходите из окна подключения к удаленному рабочему столу.

- Кнопка Подключиться.

  Эта кнопка инициирует подключение к удаленному рабочему столу.

- Кнопка Параметры.

  Эта кнопка открывает окно Параметры, которое содержит разделы Перенаправление USB-устройств и Внешний вид окон.

## Окно подключения к удаленным рабочим столам под управлениемСкала-Р BPM

Окно подключения к удаленному рабочему столу содержит следующие элементы интерфейса:

- Поле Сервер.

  В этом поле указывается адрес сервера, на котором запущен диспетчер подключений Скала-Р BPM.

  Kaspersky Thin Client сохраняет адрес последнего сервера, к которому было совершено подключение, и вам не нужно вводить его при повторном подключении.

- Поле Имя пользователя.

  В этом поле указывается домен, если он требуется, и имя пользователя.

  Kaspersky Thin Client сохраняет имя пользователя, который последний раз подключался к Скала-РBPM, и вам не нужно вводить его при повторном подключении.

- Поле Домен.

  Это поле заполняется автоматически, если заполнено поле Имя пользователя.

- Поле Пароль.

  В этом поле указывается пароль пользователя.

  Пароль пользователя сбрасывается каждый раз, когда вы выходите из окна подключения к рабочимстолам под управлением Скала-Р BPM.

- Кнопка Подключиться.

  Эта кнопка инициирует подключение к диспетчеру подключений Скала-Р BPM.

## Закладка Параметры

Закладка Параметры позволяет вам настраивать параметры Kaspersky Thin Client.

### Раздел Общие

Этот раздел содержит следующие элементы интерфейса:

- Поле Имя тонкого клиента.

  Имя, под которым тонкий клиент отображается в Kaspersky Security Center.

- Раскрывающийся список. Язык системы

  Язык интерфейса тонкого клиента.

- Область Настройка подключения к KSC.

  Параметры соединения с Kaspersky Security Center. Вы можете выбрать один из предложенных вариантов:

  - Автоматически (DHCP).

    Если выбран этот вариант, тонкий клиент получает параметры подключения к Kaspersky SecurityCenter по DHCP.

  - Вручную.

    Если выбран этот вариант, вы можете указать адрес Kaspersky Security Center вручную. Если вы выбрали этот вариант, станут доступны поле Сервер и Проверить:

    - Поле Сервер.

      Адрес сервера, на котором запущен Kaspersky Security Center.

    - Кнопка Проверить.

      Кнопка, позволяющая протестировать соединение с сервером, на котором запущен Kaspersky Security Center.

  - Не подключаться к KSC.

    Если выбран этот вариант, тонкие клиенты не синхронизируются с Kaspersky Security Center и выможете изменять настройки отдельных тонких клиентов локально.

### Раздел Сеть

Этот раздел содержит следующие элементы интерфейса:

- Область Настройка параметров сети.

  Параметры соединения с сетью. Вы можете выбрать один из предложенных вариантов:

  - Автоматически (DHCP).

    Если вы выбрали этот вариант, тонкий клиент получит параметры подключения к сети Интернет по DHCP.

- Вручную.

  Если вы выбрали этот вариант, вы можете настроить подключение к сети Интернету вручную. Вам станут доступны поля IP-адрес, Маска подсети, Основной шлюз и DNS-серверы:

  - Поле IP-адрес.

    Адрес компьютера, на котором запущен Kaspersky Thin Client.

  - Поле Маска подсети.

    Маска подсети.

  - Поле Основной шлюз.

    Адрес основного шлюза.

  - Поле DNS-серверы.

    Список IP-адресов DNS-серверов.

### Раздел Дата и время

Этот раздел содержит следующие элементы интерфейса:

- Раскрывающийся список Часовой пояс.

  Смещение относительно UTC.

- Поле Дата.

  Дата в формате ДД.ММ.ГГГГ.

- Поле Время.

  Время в формате ЧЧ:ММ.

## Закладка Инструменты

Закладка **Инструменты** позволяет просматривать информацию о работе Kaspersky Thin Client, обновлять Kaspersky Thin Client и работать с журналом событий.

### Раздел Информация о системе

Этот раздел содержит следующее:

- Номер версии Kaspersky Thin Client.
- Номер версии KasperskyOS.
- Кнопку Проверить обновления, которая позволяет запустить проверку обновлений вручную.

### Раздел Сеть

Этот раздел содержит информацию о состоянии соединения.

### Раздел Журнал событий

Этот раздел содержит следующее:

- Область событий системы.
  В этой области отображаются события, которые сохраняются в журнал событий.
- Поле Адрес для отправки.
  IP-адрес и порт или имя сервера, на который отправляется журнал событий.
- Кнопка Отправить.
  Позволяет отправить журнал событий на сервер, указанный в поле Адрес для отправки.

## Панель состояния

Панель состояния содержит следующие элементы интерфейса:

- Кнопка завершения работы.
  При нажатии на эту кнопку открывается меню завершения работы.
- Имя, под которым Kaspersky Thin Client отображается в Kaspersky Security Center.
- Оповещение об обновлении.
  Это оповещение отображается, только если Kaspersky Thin Client готов для установки обновлений.
- Значок состояния сети.
  Этот значок показывает состояние сети:
  - Нет сети.
    Kaspersky Thin Client не подключен к сети.
  - Не удалось получить IP-адрес.
    Kaspersky Thin Client подключен к сети, но не получил IP-адрес.
  - Отсутствует связь с KSC.
    Kaspersky Thin Client подключен к сети, но нет соединения с Kaspersky Security Center.
  - Подключено.
    Kaspersky Thin Client подключен к сети и Kaspersky Security Center.
- Кнопка переключения раскладки клавиатуры.
  При нажатии на эту кнопку переключается раскладка клавиатуры.
  Доступны следующие языки раскладки:
  - Русский.
  - Английский.
- Дата и время.

## Панель подключения

Панель подключения отображается в центре верхней части экрана в течение сессии подключения к удаленному рабочему столу. Когда вы подключаетесь к удаленному рабочем столу панель подключениясвернута и ее кнопки скрыты.

Панель подключения разворачивается при следующих действиях:

- Нажатии на панель подключения левой клавишей мыши.
- Нажатии комбинации клавиш **Ctrl+Alt+Home**.

На развернутой панели подключения находятся следующие кнопки:

- Кнопка Завершить сессию, которая завершает сессию подключения к удаленному рабочему столу.
- Кнопка **Alt+Ctrl+Del**, которая посылает комбинацию клавиш **Alt+Ctrl+Del** на удаленный рабочий стол.

# Лицензирование

Условия использования продукта изложены в Соглашении о сотрудничестве в области информационнойбезопасности или подобном документе, на основании которого используется продукт.

## О лицензии

*Лицензия* – это ограниченное по времени право на использование продукта, предоставляемое вам на основании Соглашения о сотрудничестве в области информационной безопасности или подобного документа, на основании которого используется продукт.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование продукта в соответствии с условиями Соглашения о сотрудничестве в области информационной безопасности или подобного документа, на основании которого используется продукт.
- Получение технической поддержки.

## О лицензионном сертификате

*Лицензионный сертификат* – это документ, который передается вам вместе с файлом ключа или кодомактивации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

## О лицензионном ключе

*Лицензионный ключ* (далее также *ключ*) – последовательность бит, с помощью которой вы можете использовать продукт в соответствии с условиями Соглашения о сотрудничестве в области информационной безопасности или подобного документа, на основании которого используется продукт.Лицензионный ключ создается специалистами "Лаборатории Касперского". Ключ обеспечивает использование продукта в соответствии с условиями, указанными в Лицензионном сертификате (типомлицензии, сроком действия лицензии, лицензионным ограничением).

Ключ можно добавить в Kaspersky Security Center с помощью кода активации или файла ключа и выбрать егов Kaspersky Security Management Suite через политику. Ввести ключ на самом Kaspersky Thin Client невозможно.

Вы можете добавлять, заменять или удалять ключи. Ключ может быть заблокирован "Лабораторией Касперского", если условия Соглашения о сотрудничестве в области информационной безопасности илиподобного документа, на основании которого используется продукт, нарушены.

Информация о введенном ключе показывается в разделе Лицензия в веб-плагине Kaspersky Security Center.

Параметры на закладке Лицензия

| Параметр | Описание |
|---|---|
| Лицензионный ключ | Серийный номер ключа. |
| Информация о ключе | Название ключа, введенного в Kaspersky Security Center. |
| Тип ключа | Тип выбранного ключа. |
| Действителен до | Дата окончания действия ключа. |
| Количество устройств | Количество Kaspersky Thin Client, на которое распространяется действие ключа. |

Если лицензионный ключ отсутствует, срок действия ключа истек, ключ занесен в список запрещенных или под действие лицензионного ключа попадает больше копий Kaspersky Thin Client, чем позволяет лицензионный сертификат, никакие функции Kaspersky Thin Client и веб-плагина Kaspersky Security Center не блокируются.

## О коде активации

*Код активации* – это уникальная последовательность из латинских букв и цифр. Вы вводите код активации,чтобы добавить лицензионный ключ на использование веб-плагина для централизованного управления Kaspersky Thin Client.

Для использования кода активации нужно чтобы Kaspersky Security Center имел доступ к сети Интернет.

## О файле ключа

*Файл ключа* – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файлключа предназначен для добавления лицензионного ключа на использование веб-плагина для централизованного управления Kaspersky Thin Client.

## Выбор лицензионного ключа

Чтобы выбрать лицензионный ключ, выполните следующие действия:

1. Добавьте лицензионный ключ в Kaspersky Security Center. Подробную информацию о добавлении лицензионного ключа см. в *онлайн-справке Kaspersky Security Center*.
2. В главном окне Kaspersky Security Management Suite выберите Устройства → Политики и профили политик.
3. Нажмите на название Kaspersky Thin Client.
4. Откроется окно, содержащее информацию о Kaspersky Thin Client.
5. Выберите закладку Параметры программы.
6. Выберите раздел Лицензия.
7. В раскрывающемся списке Лицензионный ключ выберите нужный лицензионный ключ.
8. Нажмите на кнопку Сохранить.

# Предоставление данных

Kaspersky Thin Client не передает никаких данных в "Лабораторию Касперского". Данные обрабатываются на компьютерах, на которых установлена программа и серверах локальной инфраструктуры, с которыми взаимодействует тонкий клиент.

Kaspersky Thin Client сохраняет на тонком клиенте следующую информацию:

- Журнал событий, содержащий технические сведения о работе системы за последнее время.

  Вы можете переслать журнал событий Службе технической поддержки для устранения неисправностей. О том, как передать журнал событий Службе технической поддержки, см. раздел "Отправка журнала событий на сторонний сервер".

- Параметры тонкого клиента:
  - Имя тонкого клиента.
  - Язык Kaspersky Thin Client.
- Настройки работы с Kaspersky Security Center:
  - Способ подключения Kaspersky Thin Client к Kaspersky Security Center.
  - Период синхронизации Kaspersky Thin Client и Kaspersky Security Center в минутах.
  - Имя или IP-адрес сервера, на котором развернут Kaspersky Security Center.
  - Порт SOAP интерфейса на сервере Kaspersky Security Center.
  - Хеш пароля для вывода Kaspersky Thin Client из-под политики Kaspersky Security Center.
- Параметры обновлений:
  - Адрес сервера обновлений.
  - Путь к папке на сервере обновлений, в которую распакован пакет обновлений.
- Параметры подключения к Скала-Р BPM:
  - Имя пользователя для подключения к диспетчеру подключений Скала-Р BPM.
  - Имя или IP-адрес диспетчера подключений Скала-Р BPM.
- Параметры подключения к RDP-серверу:
  - Имя или IP-адрес RDP-сервера.
  - Имя пользователя для подключения к RPD-серверу.
  - Включена ли строгая проверка SSL сертификата RDP-сервера.
- Параметры перенаправления локальных устройств:

- Разрешено ли перенаправление USB-накопителей.
- Разрешено ли перенаправление смарт-карт.

- Параметры внешнего вида окон:
  - Включено ли сглаживание шрифтов.
  - Включена ли анимация меню.
  - Включено ли отображение фона рабочего стола.
  - Включено ли отображение содержимого окна при перемещении.
  - Включено ли использование тем в Windows.
- Параметры сети:
  - Включена ли автоматическая настройка сети по DHCP.
  - IP-адрес тонкого клиента.
  - Маска подсети.
  - Список IP-адресов DNS-серверов.
  - IP-адрес сетевого шлюза.
- Параметры записи в журнал:
  - Имя или IP-адрес сервера для отправки журнала событий.
- Параметры даты и времени:
  - Смещение времени относительно UTC.

Система виртуализации Скала-Р сохраняет в базе данных следующую информацию:

- Имя пользователя.
- IP-адрес тонкого клиента.
- Идентификатор Kaspersky Thin Client.
- События установления сессии.
- События завершения сессии.

Имя или IP-адрес RDP-сервера и диспетчера подключений Скала-Р BPM перезаписываются при каждомуспешном подключении.

Имя пользователя перезаписывается при каждом успешном подключении к RDP-серверу или диспетчеруподключений Скала-Р BPM.

Адрес сервера для отправки журнала событий перезаписывается при каждой успешной отправке событий системы на сторонний сервер. При отправке журнала событий на сторонний сервер отправляются все события системы, сохраненные на тонком клиенте.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

# Запуск и завершение работы Kaspersky Thin Client

Чтобы запустить Kaspersky Thin Client, нажмите кнопку включения / выключения в средней части лицевой панели тонкого клиента.

В результате на тонком клиенте загорится индикатор питания, и начнет запускаться Kaspersky Thin Client.


Лицевая панель тонкого клиента

В процессе запуска Kaspersky Thin Client на подключенном к тонкому клиенту мониторе последовательно отображаются заставка производителя тонкого клиента, приветствие загрузчика, логи загрузчика и закладка Подключения. Появление этой закладки означает, что система включилась.

Чтобы завершить работу Kaspersky Thin Client, выполните одно из следующих действий:

- Выключите через интерфейс:

  1. Нажмите на кнопку выключения в левой части панели состояния. Появится меню завершения работы.
  2. Выберите пункт меню **Завершить работу**.

- Нажмите кнопку включения / выключения в средней части лицевой панели тонкого клиента.

# Интеграция Скала-Р BPM с Kaspersky Thin Client

## Системные требования

Kaspersky Thin Client поддерживает работу со Скала-Р BPM 1.60 и выше.

## Настройка Kaspersky Thin Client для работы с Скала-Р BPM

Для подключения к удаленному рабочему столу под управлением Скала-Р BPM пользователь должен иметь учетную запись Active Directory, связанную с этим рабочим столом.

Подробнее о настройке авторизации через Active Directory см. в *Скала-Р BPM. Руководство администратора*.

## Ограничения

Существуют следующие ограничения при работе Kaspersky Thin Client со Скала-Р BPM:

- Не поддерживается авторизация локальных пользователей на диспетчере подключений Скала-Р BPM.
- Не поддерживается авторизация пользователей по смарт-картам на диспетчере подключений Скала-PBPM.
- Не поддерживается смена пароля пользователя через Kaspersky Thin Client.
- Не поддерживается одновременное подключение к нескольким удаленным рабочим столам подуправлением Скала-Р BPM.
- Изменение параметров перенаправления USB-устройств для прямого RDP-подключения (в веб-плагинеили в интерфейсе Kaspersky Thin Client) влияет на эти же настройки при подключении через Скала-Р BPM.
- Изменение параметров отображения удаленного рабочего стола для прямого RDP-подключения (в веб-плагине или в интерфейсе Kaspersky Thin Client) влияет на эти же настройки при подключении через Скала-Р BPM.
- Kaspersky Thin Client поддерживает работу только с удаленными рабочими столами под управлением операционных систем Windows 10 и Windows Server 2012.

# Использование Kaspersky Thin Client

Основной сценарий работы с Kaspersky Thin Client предполагает подготовку системы к запуску, включение системы и подключение к удаленному рабочему столу. По завершении работы с удаленным рабочим столом предполагается завершение сеанса подключения и выключение системы. Все остальное время вы проводите в привычном для себя программном окружении и непосредственное взаимодействие синтерфейсом Kaspersky Thin Client не требуется.

Основной сценарий работы с Kaspersky Thin Client включает следующие этапы:

1. Подготовка Kaspersky Thin Client к включению

   Подключите устройства к Kaspersky Thin Client перед первым включением.

2. Запуск системы

   Включите систему для начала работы.

3. Подключение к удаленному рабочему столу

   Подключитесь к удаленному рабочему столу и начните работу.

4. Блокирование рабочего стола и возобновление работы

   В случае необходимости временно покинуть рабочее место заблокируйте рабочий стол. По возвращении на рабочее место возобновите работу.

5. Завершение сеанса подключения

Завершите сеанс подключения к удаленному рабочему столу по завершении работы.

6. Остановка системы

Выключите систему в конце рабочего дня.

## Подключение к удаленному рабочему столу

Чтобы подключиться к удаленному рабочему столу по протоколу RDP, выполните следующие действия:

1. Запустите Kaspersky Thin Client.

2. В открывшемся окне Подключения нажмите на кнопку Прямое RDP-подключение.

   Откроется окно подключения к удаленному рабочему столу.

3. Укажите параметры подключения к удаленному рабочему столу:

   a. В поле **Сервер** укажите IP-адрес или имя RDP-сервера, к которому вы хотите подключиться.

      Kaspersky Thin Client сохраняет адрес последнего RDP-сервера, к которому было совершеноподключение, и вам не нужно вводить его при повторном подключении.

   b. В поле **Имя пользователя** введите локальное или доменное имя пользователя. Если вы указываетедоменное имя, название домена указывать не обязательно, но вы можете это сделать в формате Домен\Имя пользователя.

      Kaspersky Thin Client сохраняет имя пользователя, который последний раз подключался к RDP-серверу, и вам не нужно вводить его при повторном подключении.

c. В поле **Пароль** введите пароль пользователя.

Пароль пользователя сбрасывается каждый раз, когда вы выходите из окна подключения к удаленномурабочему столу.

4. Нажмите на кнопку Подключиться.

Через несколько секунд на мониторе отобразится удаленный рабочий стол RDP-сервера, к которому выподключились.

Чтобы подключиться к удаленному рабочему столу под управлением Скала-Р BPM, выполните следующие действия:

1. Запустите Kaspersky Thin Client.
2. В открывшемся окне Подключения нажмите на кнопку Подключение к Скала-Р BPM.

   Откроется окно подключения к рабочим столам под управлением Скала-Р BPM.
3. Укажите параметры подключения к Скала-Р BPM:

   a. В поле **Сервер** укажите IP-адрес или имя диспетчера подключений Скала-Р BPM.

   Kaspersky Thin Client сохраняет адрес диспетчера подключений Скала-Р BPM, к которому былосовершено подключение, и вам не нужно вводить его при повторном подключении.

   b. В поле **Имя пользователя** введите доменное имя пользователя. Название домена указывать необязательно, но вы можете это сделать в формате Домен\Имя пользователя.

   Kaspersky Thin Client сохраняет имя пользователя, который последний раз подключался к Скала-Р BPM, и вам не нужно вводить его при повторном подключении.

   c. В поле **Пароль** введите пароль пользователя.

   Пароль пользователя сбрасывается каждый раз, когда вы выходите из окна подключения к рабочимстолам под управлением Скала-Р BPM.
4. Нажмите на кнопку Подключиться.

   Откроется окно выбора удаленного рабочего стола.
5. Нажмите на кнопку с названием рабочего стола, к которому вы хотите подключиться.

   Через несколько секунд на мониторе отобразится удаленный рабочий стол, к которому вы подключились.

## Блокирование рабочего стола и возобновление работы

Если требуется ненадолго прервать работу, следует блокировать доступ к своему рабочему месту. Дляэтого не требуется взаимодействовать непосредственно с Kaspersky Thin Client – все действия производятся в программном окружении удаленного рабочего стола.

Чтобы блокировать рабочий стол, выполните одно из следующих действий:

- Нажмите комбинацию клавиш Win +L.
- Включите блокировку в меню Пуск:

1. Нажмите на кнопку **Пуск** ( ) в панели задач Windows. Появится меню Пуск.
2. В меню Пуск нажмите на значок своей учетной записи.Появится меню параметров учетной записи.
3. В меню параметров учетной записи выберите пункт Заблокировать.

Чтобы возобновить работу, на экране входа на удаленный рабочий стол введите свой пароль и нажмите на клавишу Enter.

### Завершение сеанса подключения

Чтобы завершить сеанс подключения к удаленному рабочему столу, выполните следующие действия:

1. Нажмите на панель подключения Kaspersky Thin Client в центре верхней части удаленного рабочего стола. Панель раскроется.
2. Нажмите на кнопку Завершить сессию на панели подключения.

В результате сеанс подключения к рабочему столу будет завершен и на мониторе отобразится окно подключения к удаленному рабочему столу.

## Остановка Kaspersky Thin Client

Чтобы остановить систему Kaspersky Thin Client, следуйте инструкции из раздела Запуск и выключение Kaspersky Thin Client.

В результате подключение к удаленному рабочему столу будет прервано, и система Kaspersky Thin Client будет остановлена, и на тонком клиенте погаснет индикатор питания.

## Обновление программного обеспечения

Kaspersky Thin Client автоматически загружает доступные обновления с сервера обновлений по расписанию. Если обновление загружено, вы увидите надпись Доступны обновления в панели состояния. Выможете установить загруженные обновления в удобное для вас время.

Чтобы установить обновление, выполните следующие действия:

1. Нажмите на кнопку выключения в левой части панели состояния.  Появится меню завершения работы.
2. Выберите пункт меню Перезагрузить и обновить.

Чтобы проверить наличие обновлений вручную, выполните следующие действия:

1. Запустите Kaspersky Thin Client.
2. Выберите закладку Инструменты.
3. Выберите раздел Информация о системе.
4. Нажмите на кнопку Проверить обновления в центре экрана.

# Настройка Kaspersky Thin Client

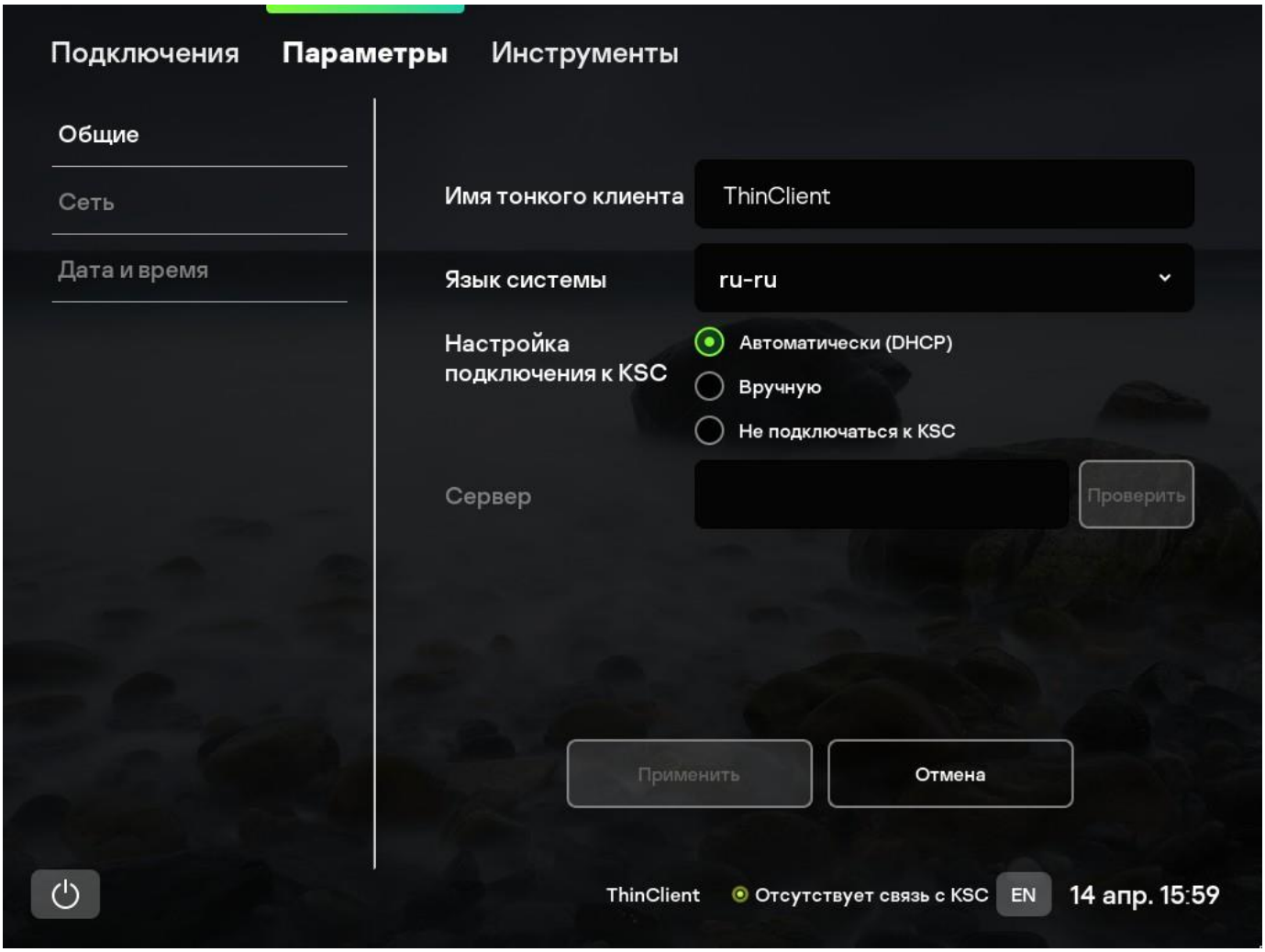
Этот раздел содержит информацию о настройке Kaspersky Thin Client.

## Настройка общих параметров

Чтобы настроить имя тонкого клиента и язык интерфейса, выполните следующие действия:

1. Выберите закладку Параметры.

   Окно параметров откроется на разделе Общие (см. рис. ниже).




Закладка Параметры. Раздел Общие

2. В поле Имя тонкого клиента введите имя, под которым Kaspersky Thin Client будет отображаться в Kaspersky Security Center.

3. В раскрывающемся списке Язык системы выберите язык интерфейса Kaspersky Thin Client (русский или английский). Изменения вступят в силу после перезагрузки системы.

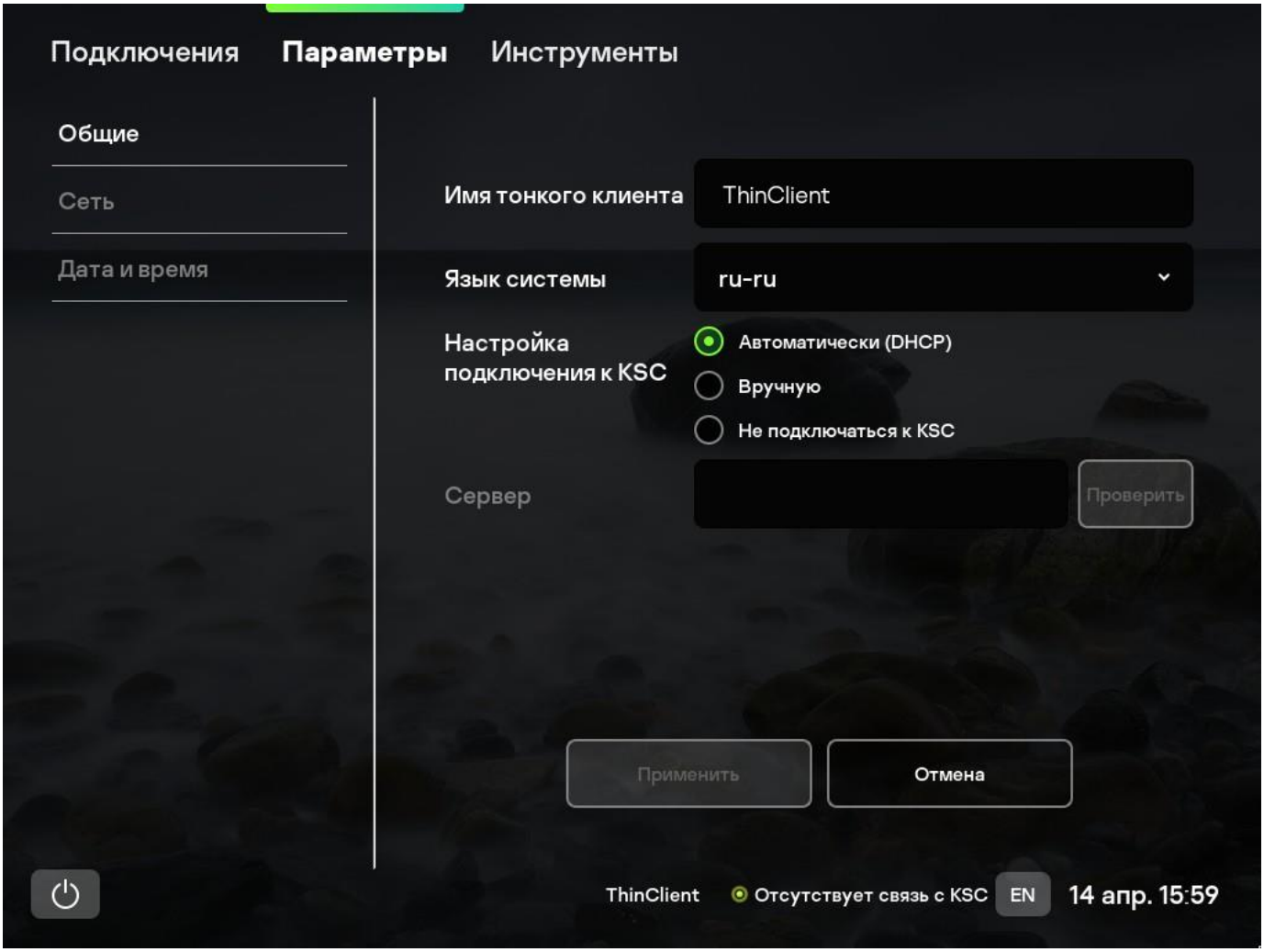
4. Нажмите на кнопку Применить в нижней части окна, чтобы сохранить изменения.

## Настройка параметров подключения к Kaspersky Security Center

Чтобы настроить параметры подключения Kaspersky Thin Client к Kaspersky Security Center, выполните следующие действия:

1. Выберите закладку Параметры.

   Окно параметров откроется на разделе Общие (см. рис. ниже).




Закладка Параметры. Раздел Общие

2. В блоке Настройка подключения к KSC настройте параметры подключения Kaspersky Thin Client к Kaspersky Security Center:

- Если вы хотите получить параметры подключения Kaspersky Thin Client к Kaspersky Security Center автоматически по протоколу DHCP, выберите вариант Автоматически (DHCP).

- Если вы хотите указать параметры подключения Kaspersky Thin Client к Kaspersky Security Center вручную, выберите вариант Вручную.

  Поле Сервер и кнопка Проверить станут доступны. Выполните следующие действия:

  a. В поле Сервер введите IP-адрес или имя сервера Kaspersky Security Center. Если вы используетепорт, отличный от 13292, обязательно укажите его в формате IP-адрес:Порт или Имя сервера:Порт.

  Если вы хотите включить строгую проверку SSL сертификатов, обязательно укажите имя сервера Kaspersky Security Center.

b. Нажмите на кнопку Проверить, чтобы протестировать соединение с Kaspersky Security Center.

Если параметры подключения к Kaspersky Security Center были заданы ранее, KasperskyOS for Thin Client уже синхронизировался с Kaspersky Security Center, и в веб-плагине был задан пароль прекращения взаимодействия с Kaspersky Security Center, то при сохранении измененных параметров откроется окно для ввода этого пароля.

- Если вы не хотите подключать Kaspersky Thin Client к Kaspersky Security Center, выберите вариант Не подключаться к KSC.

c. Нажмите на кнопку Применить в нижней части окна, чтобы сохранить изменения.

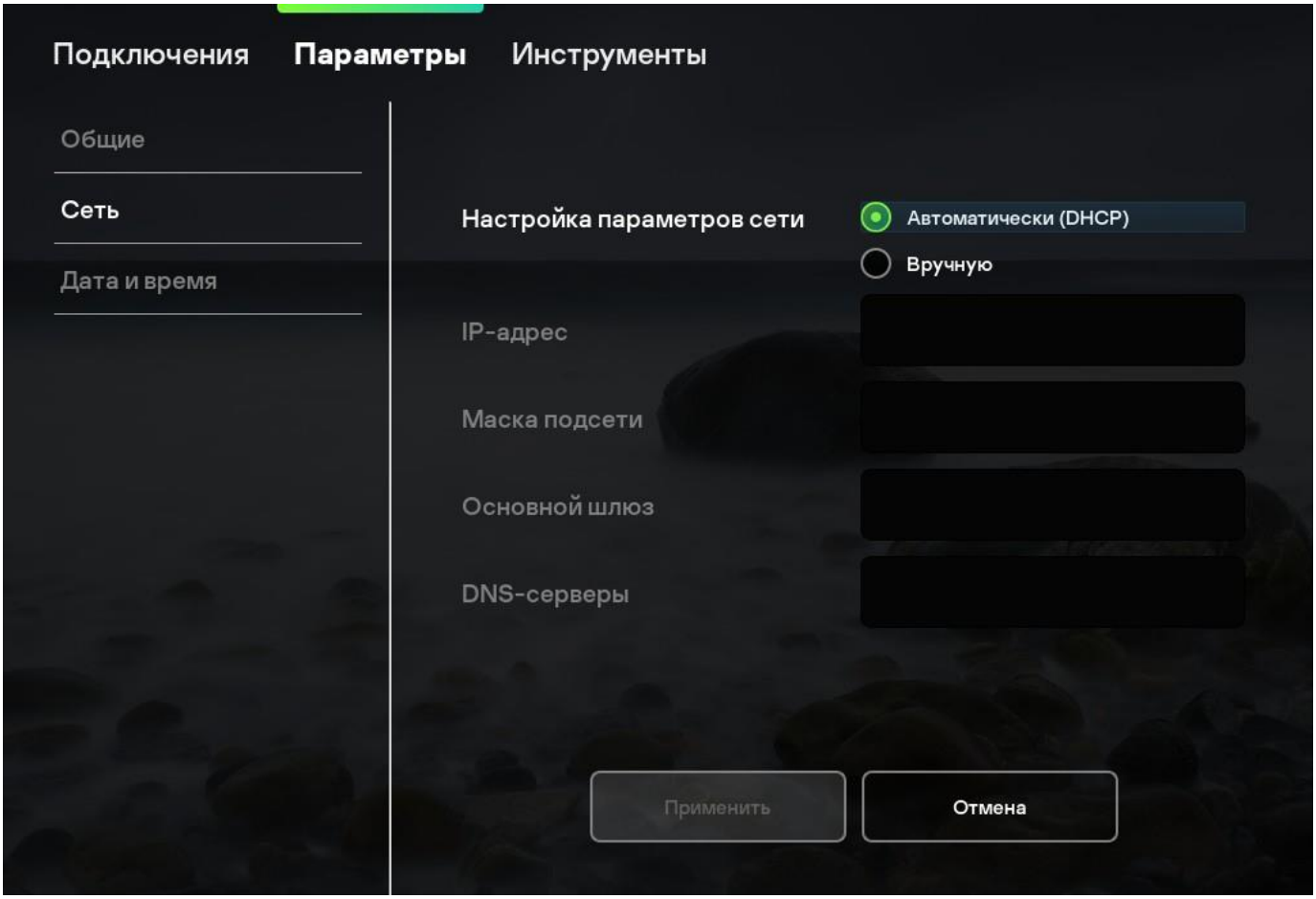
## Настройка параметров сети

Чтобы настроить параметры сети, выполните следующие действия:

1. Выберите закладку Параметры.

Окно параметров откроется на разделе Общие.

2. Выберите раздел Сеть (см. рис. ниже).




Закладка Параметры. Раздел Сеть

3. Настройте параметры подключения Kaspersky Thin Client к Kaspersky Security Center:

- Если вы хотите получить параметры сети автоматически по протоколу DHCP, выберите вариант Автоматически (DHCP) в верхней части окна.

- Если вы хотите указать параметры сети вручную, выберите вариант Вручную в верхней части окна.
  Поля IP-адрес, Маска подсети, Основной шлюз и DNS-серверы станут доступны для заполнения.
  Выполните следующие действия:
  - В поле IP-адрес введите IP-адрес Kaspersky Thin Client. Используйте IPv4.
  - В поле Маска введите маску подсети.
  - В поле Основной шлюз введите адрес сетевого шлюза.
  - В поле DNS-серверы введите адреса DNS-серверов.

4. Нажмите на кнопку Применить в нижней части окна, чтобы сохранить изменения.

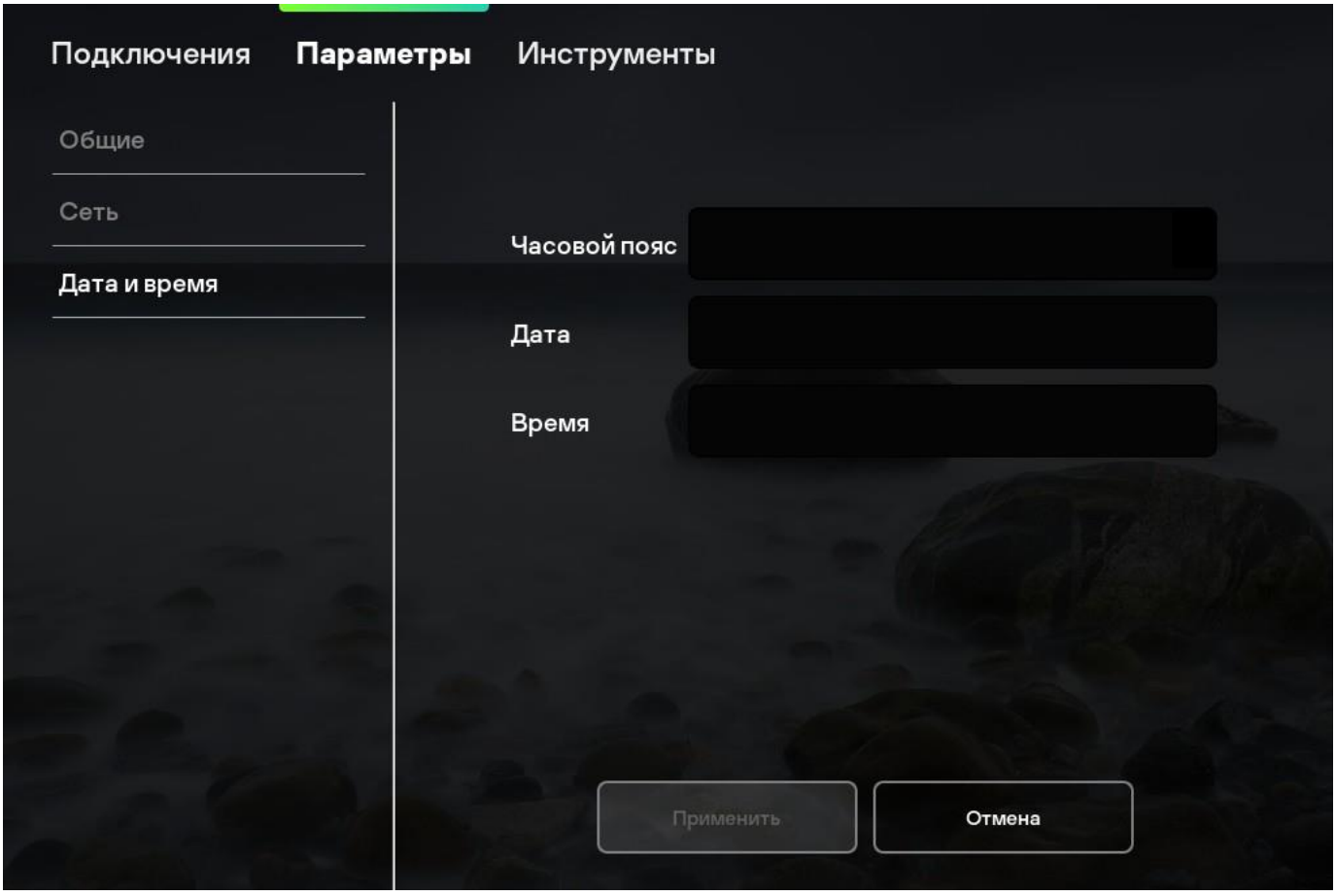
## Настройка даты и времени

Чтобы настроить параметры даты и времени, выполните следующие действия:

1. Выберите закладку Параметры.

Окно параметров откроется на разделе Общие.

2. Выберите раздел Дата и время (см. рис. ниже).




Закладка Параметры. Раздел Дата и время

3. Настройте параметры даты и времени:

- В выпадающем списке Часовой пояс выберите смещение относительно UTC.
- В поле Дата введите текущую дату в формате ДД.ММ.ГГГГ.
- В поле Время введите текущее время в формате ЧЧ:ММ:СС.

4. Нажмите на кнопку Применить в нижней части окна, чтобы сохранить изменения.

## Настройка перенаправления USB-устройств на удаленный рабочий стол

Для корректного перенаправления USB-устройств на удаленный рабочий стол в Microsoft Windows нужно включить службу Remote Desktop Services и разрешить перенаправление Plug and Play устройств в настройках Remote Desktop Services.

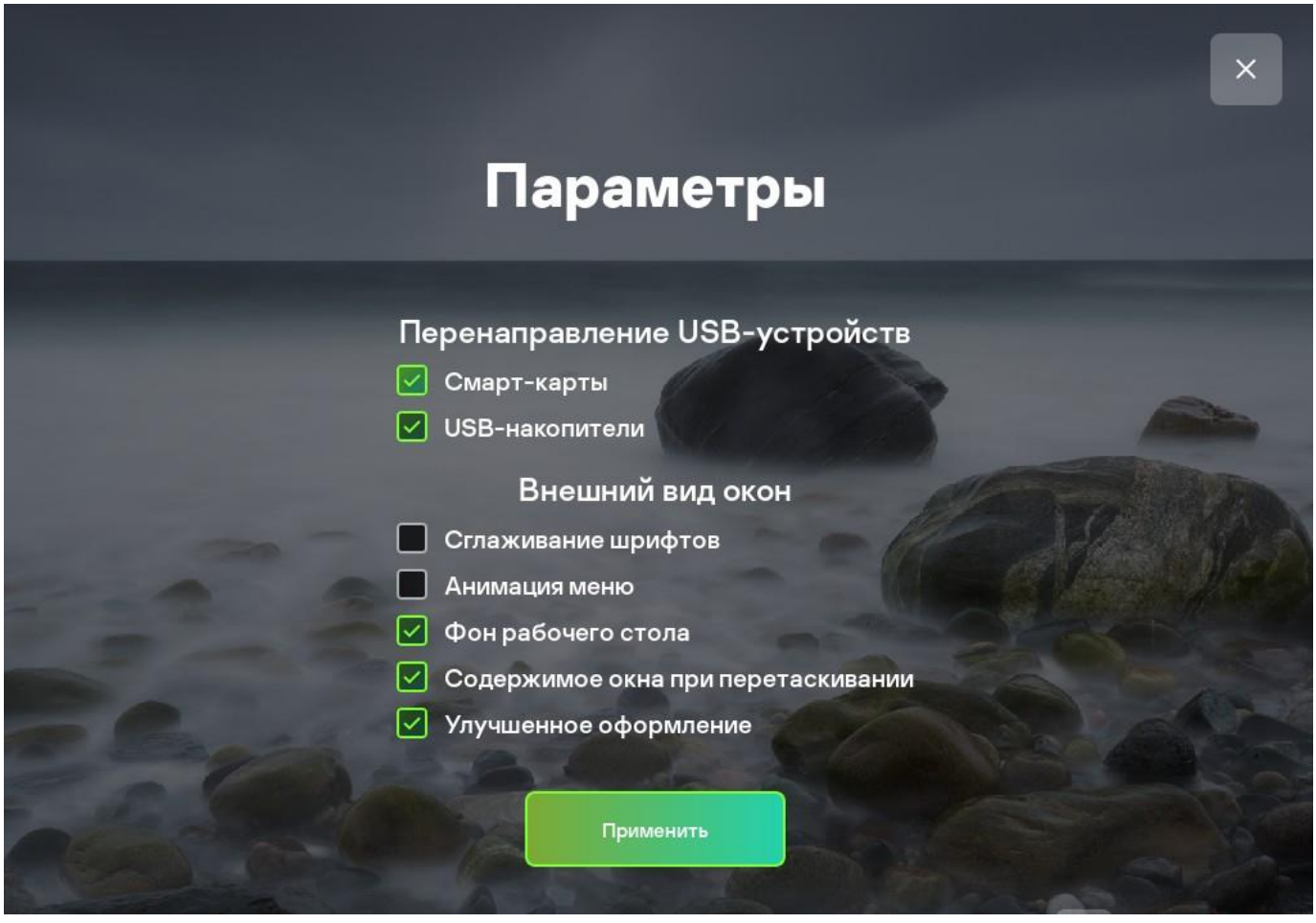
Чтобы настроить перенаправление USB-устройств на удаленный рабочий стол, выполните следующие действия:

1. Выберите закладку Подключения.

2. Нажмите на кнопку подключения к удаленному столу по протоколу RDP

3. Нажмите на кнопку Параметры в нижней части окна.

   Откроется окно параметров подключения к удаленному рабочему столу (см. рис. ниже).




Окно параметров подключения к удаленному рабочему столу

4. В блоке Перенаправление USB-устройств установите флажки напротив устройств, подключенных к Kaspersky Thin Client по USB, которые необходимо пробрасывать на удаленный рабочий стол:

- Флажок USB-накопители включает / выключает перенаправление USB-накопителей.
- Флажок Смарт-карты включает / выключает перенаправление смарт-карт и токенов.

5. Нажмите на кнопку Применить в нижней части окна, чтобы сохранить изменения.

## Настройка параметров отображения удаленного рабочего стола

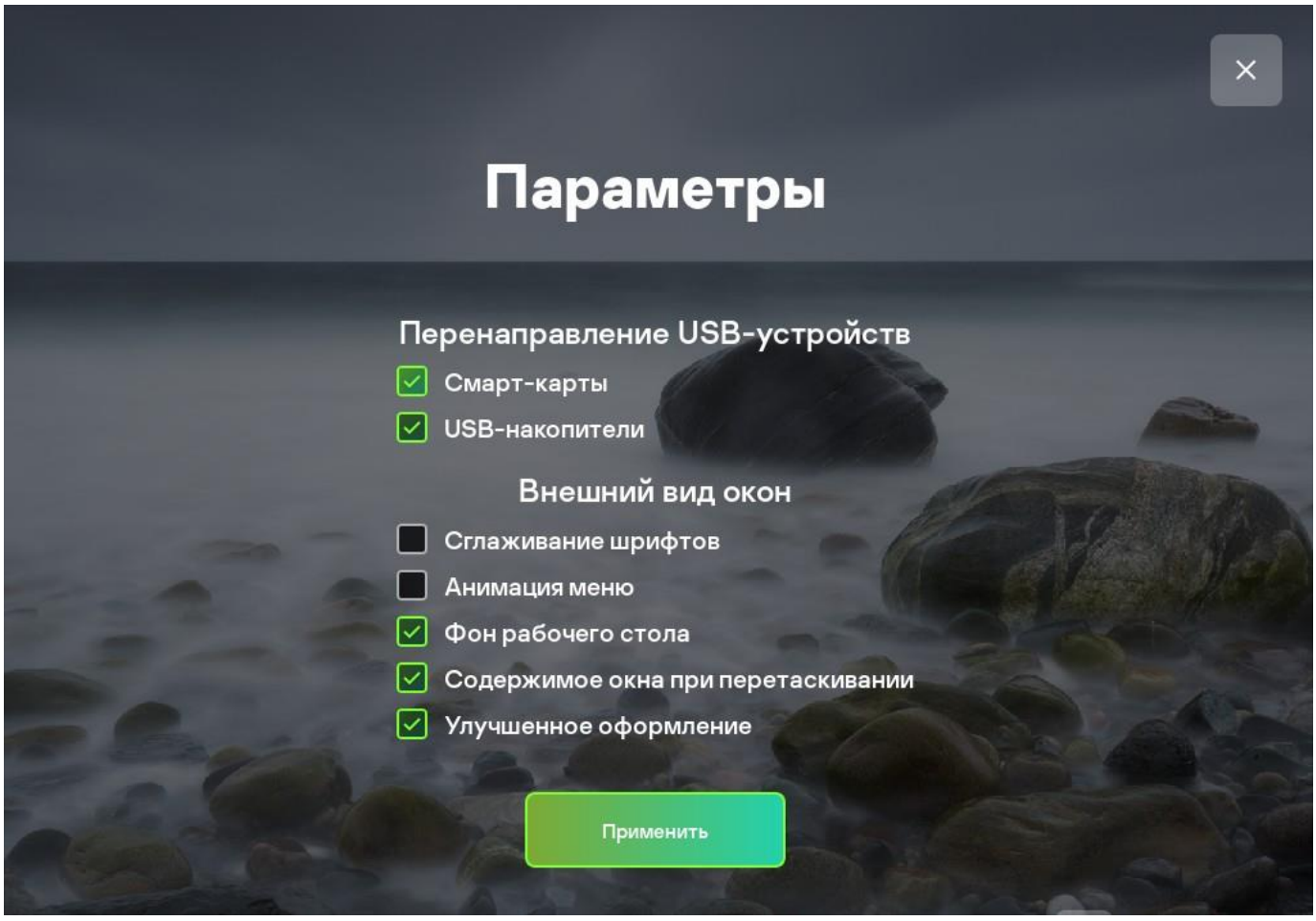
Чтобы настроить параметры отображения удаленного рабочего стола, выполните следующие действия:

1. Выберите закладку Подключения.

2. Нажмите на кнопку подключения к удаленному столу по протоколу RDP.

3. Нажмите на кнопку Параметры в нижней части окна.

Откроется окно параметров подключения к удаленному рабочему столу (см. рис. ниже).




Окно параметров подключения к удаленному рабочему столу

4. В блоке Внешний вид окон установите флажки напротив графических параметров удаленного рабочегостола, которые требуется использовать:

- Флажок Сглаживание шрифтов включает / выключает сглаживание шрифтов.
- Флажок Анимация меню включает / выключает анимацию меню.
- Флажок Фон рабочего стола включает / выключает отображение обоев рабочего стола Windows.

- Флажок Содержимое окна при перетаскивании включает / выключает отображение содержимого окон при их перетаскивании.
- Флажок Улучшенное оформление включает / выключает тему визуального оформления, установленную в Windows.

Включение параметров отображения удаленного рабочего стола может повлиять на скорость работы Kaspersky Thin Client.

5. Нажмите на кнопку Применить в нижней части окна, чтобы сохранить изменения.

# Управление программой через Kaspersky Security Management Suite

Kaspersky Security Management Suite (далее также Web Console) представляет собой программу (веб-приложение), предназначенную для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky SecurityCenter.

Программа Kaspersky Thin Client поддерживает работу с Kaspersky Security Management Suite версии 1.0.1.57. Подробную информацию о Kaspersky Security Management Suite см. в *онлайн-справке Kaspersky Security Center*.

С помощью Kaspersky Security Management Suite вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать программы "Лаборатории Касперского" на устройства вашей сети;
- управлять установленными программами;
- просматривать отчеты о состоянии системы безопасности.

## Вход и выход из Kaspersky Security Management Suite

Чтобы войти в Kaspersky Security Management Suite, вам нужно получить у администратора веб-адрес Сервера администрирования и номер порта, указанные во время установки (по умолчанию используется порт 8080). Так же требуется включить JavaScript в браузере.

Чтобы войти в Kaspersky Security Management Suite, выполните следующие действия:

1. В браузере перейдите по адресу <Веб-адрес Сервера администрирования>:<Номер порта>.

   Откроется страница входа.

2. Войдите с использованием имени пользователя и пароля локального администратора.

   Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

   После входа отобразится информационная панель с последним используемым языком и темой.

   Если вы вошли в Kaspersky Security Management Suite впервые, в нижней части экрана отобразится учебник. Можно следовать инструкциям учебника или закрыть его соответствующей кнопкой (X).

Вы можете переходить по страницам Kaspersky Security Management Suite и работать с ней. Дополнительная информация о работе Kaspersky Security Management Suite приведена в онлайн-справке Kaspersky Security Center.

Чтобы выйти из Kaspersky Security Management Suite, выполните следующие действия:

1. В правом верхнем углу экрана щелкните по вашему имени пользователя.

2. В раскрывающемся меню выберите пункт Выход.

Kaspersky Security Management Suite закроется и отобразится страница входа.

## О веб-плагине управления Kaspersky Thin Client

Веб-плагин управления Kaspersky Thin Client (далее также "веб-плагин") обеспечивает взаимодействие Kaspersky Thin Client с Kaspersky Security Center.

Веб-плагин позволяет централизованно выполнять следующие действия:

- Управлять параметрами Kaspersky Thin Client в сети с помощью политик Kaspersky Security Center.
- Получать события из Kaspersky Thin Client.
- Устанавливать сертификаты безопасности на Kaspersky Thin Client.
- Осуществлять контроль лицензионных ключей на Kaspersky Thin Client.

Для взаимодействия Kaspersky Thin Client и Kaspersky Security Center должны быть выполнены следующие условия:

- При настройке Kaspersky Thin Client указаны параметры Kaspersky Security Center.
- В Kaspersky Security Management Suite установлен плагин управления Kaspersky Thin Client.

## Обновление веб-плагина управления Kaspersky Thin Client

Чтобы обновить веб-плагин управления Kaspersky Thin Client, выполните следующие действия:

1. Получите ZIP-архив с дистрибутивом новой версии веб-плагина Kaspersky Thin Client и цифровую подпись архива у специалистов "Лаборатории Касперского".

2. В главном окне Kaspersky Security Management Suite откройте раскрывающийся список Параметры консоли. Откроется меню параметров консоли.

3. Выберите пункт Плагины.

Отобразится список доступных плагинов управления. Установите флажок напротив веб-плагина управления Kaspersky Thin Client.

4. Нажмите на кнопку Обновить из файла. Появится панель Обновить из файла.

5. На панели Обновить из файла нажмите на кнопку Загрузить файл формата ZIP. Откроется окно загрузки файлов.

6. В окне загрузки файлов выберите ZIP-архив с дистрибутивом новой версии веб-плагина Kaspersky Thin Client.

7. На панели Обновить из файла нажмите на кнопку Загрузить подпись. Откроется окно загрузки файлов.

8. В окне загрузки файлов выберите цифровую подпись архива.

9. Нажмите на кнопку Обновить в нижней части панели Обновить из файла.

## Добавление тонких клиентов в группу управляемых устройств

При первом подключении тонкого клиента к Kaspersky Security Center требуется поместить его в группу управляемых устройств.

Чтобы добавить тонкий клиент в группу управляемых устройств, выполните следующие действия:

1. В главном окне Kaspersky Security Management Suite выберите Обнаружение устройств иразвертывание → Нераспределенные устройства.

2. Установите флажок рядом с именем тонкого клиента.

3. Нажмите на кнопку Переместить в группу. Появится панель Переместить в группу.

4. Установите флажок рядом с группой администрирования Управляемые устройства.

5. Нажмите на кнопку Переместить.

# О политиках

*Политика* – это набор параметров работы Kaspersky Thin Client, определенный для группы администрирования. Для одного продукта можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе администрирования может быть создана собственная политика для программы.

Параметры политики настраиваются на Kaspersky Thin Client с помощью веб-плагина и передаются при синхронизации. Время синхронизации можно изменить в параметрах политики.

### Активная и неактивная политика

Политика предназначена для группы управляемых тонких клиентов и может быть активной или неактивной. Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру невозможно одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры программы на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например в случае вирусной атаки. В случае атаки через флеш-накопители вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.

### Наследование параметров

Политики имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – политика вложенного уровня иерархии. Вы можете выключить наследование параметров из родительской политики.

Если переключатель Принудительно, находящийся напротив названия группы параметров Kaspersky Thin Client, настраиваемых через политики, включен, то параметры из этой группы нельзя изменять в дочерних политиках, Kaspersky Thin Client или в параметрах отдельного устройства. Они принудительно передаются с Kaspersky Security Center и применяются в Kaspersky Thin Client.

## Создание политик

Чтобы создать политику, выполните следующие действия:

1. В главном окне Kaspersky Security Management Suite выберите Устройства → Политики и профили политик.

2. Нажмите на кнопку Добавить. Запустится мастер создания политики.

3. В списке **Имя программы** выберите Kaspersky Thin Client и нажмите **Далее**.

4. На закладке **Общие** вы можете выполнить следующие действия:

   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере вкачестве действующей.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - **Для автономных пользователей**. Kaspersky Thin Client не поддерживает политики для автономных пользователей.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если переключатель включен, значенияпараметров политики наследуются из политики верхнего уровня иерархии.
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерниеполитики. В свойствах дочерней политики будет автоматически включен и недоступен длявыключения переключатель **Наследовать параметры родительской политики**.

5. На закладке Параметры программ вы можете настроить параметры Kaspersky Thin Client.

6. Нажмите на кнопку **Сохранить**.

## Изменение политики

Чтобы изменить политику, выполните следующие действия:

1. На закладке **Устройства** выберите **Политики и профили политик**.

2. Выберите политику, которую требуется изменить. Откроется окно свойств политики.

3. Настройте параметры политики и параметры Kaspersky Thin Client.

4. Нажмите на кнопку **Сохранить**.

Изменения политики будут сохранены в свойствах политики в разделе **История ревизий**.

# Настройка параметров политик

## Закладка Общие

На закладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**.
    Если выбран этот вариант, политика становится активной. По умолчанию выбран этот вариант.
  - **Для автономных пользователей**.

    Этот вариант не поддерживается Kaspersky Thin Client.
  - **Неактивна**.

    Если выбран этот вариант, политика становится неактивной, но сохраняется в списке политик. Принеобходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры родительской политики**.

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнегоуровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**.

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:
    - Значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики.
    - В блоке **Наследование параметров** закладки Общие каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

      Когда параметр включен, значения параметров дочерних политик недоступны для изменения. По умолчанию параметр выключен.

## Закладка Настройка событий

На закладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности:

- **Критическое**.

  События, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- **Отказ функционирования**.

  События, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего вовремя работы программы или выполнения процедуры.
- **Предупреждение**.

События, не обязательно являющееся серьезными, однако указывающие на возможное возникновение проблем в будущем. Чаще всего события относятся к **Предупреждениям**, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.

- **Информационное сообщение**.

  События, информирующие об успешном выполнении операции, корректной работе программы или завершении процедуры.

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервереадминистрирования по умолчанию (в днях). Нажав на тип события, вы можете настроить следующие параметры:

- **Регистрация событий**.

  Вы можете указать количество дней хранения событий и выбрать, где хранить события.

- **Уведомления о событиях**.

  Вы можете выбрать способ уведомления о событиях.

По умолчанию используются параметры уведомлений, указанные на закладке свойств Сервера администрирования (например, адрес получателя). При необходимости вы можете изменить эти параметры на закладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска** в нижней части панели параметров события.

Вы можете настроить параметры следующих событий Kaspersky Thin Client:

- Ошибка синхронизации с Kaspersky Security Center.
- Ошибка обновления.
- Ошибка подключения к диспетчеру подключений Скала-Р.
- Ошибка подключения к удаленному рабочему столу.
- Срок действия пароля истек.
- Обновление успешно завершено.

## Закладка Параметры программы

О настройке параметров Kaspersky Thin Client через политики см. раздел "Настройка параметров Kaspersky Thin Client через политики".

## Закладка История ревизий

На закладке История ревизий вы можете просмотреть список ревизий политики и изменения, для которыхбыл выполнен откат.

## Настройка параметров Kaspersky Thin Client через политики

Вы можете настроить параметры Kaspersky Thin Client с помощью политики.

Чтобы настроить параметры политики, выполните следующие действия:

1. В главном окне Kaspersky Security Management Suite выберите Устройства→ Политики и профили политик.

2. Нажмите на название Kaspersky Thin Client.
Откроется окно, содержащее информацию о Kaspersky Thin Client.

3. Выберите закладку Параметры программы.

   Закладка Параметры программы содержит следующие разделы с параметрами, которыми можноуправлять через политики:

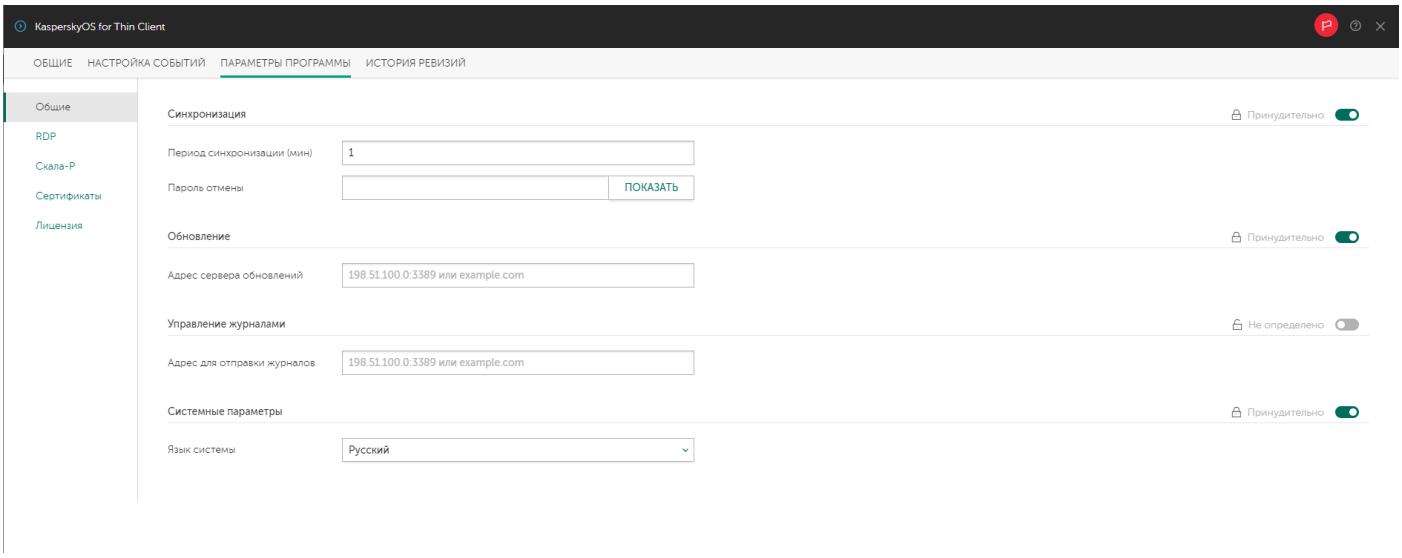
   - Общие.
   - RDP.
   - Скала-Р.
   - Сертификаты.
   - Лицензия.

4. Измените желаемые параметры.

5. Нажмите на кнопку Сохранить.

# Настройка параметров в разделе Общие

В разделе Общие (см. рис. ниже) вы можете изменять общие параметры Kaspersky Thin Client.




Раздел Общие

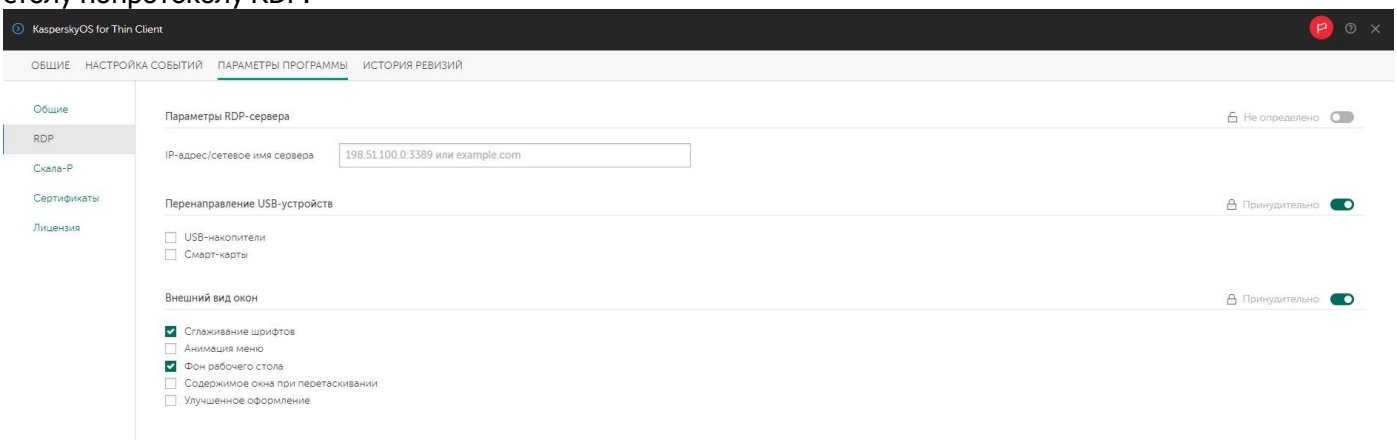
Параметры раздела Общие

| Параметр | Описание |
|---|---|
| Период синхронизации (мин) | Время синхронизации Kaspersky Thin Client с Kaspersky Security Center в минутах. |
| Пароль отмены | Пароль, который необходимо ввести для того, чтобы прекратить взаимодействие Kaspersky Thin Client с Kaspersky Security Center. |
| Адрес сервера обновлений | Веб-адрес сервера, на котором хранятся обновления для Kaspersky Thin Client. Пример: https://198.51.100.0:2020/updates |
| Адрес для отправки журналов | Веб-адрес сервера, на котором сохраняются журналы. |
| Язык системы | Язык интерфейса Kaspersky Thin Client. |

Если переключатель **Принудительно**, находящийся напротив названия группы параметров, включен, то параметры из этой группы невозможно изменять в Kaspersky Thin Client или в параметрах отдельногоустройства. Они принудительно передаются с Kaspersky Security Center и применяются в Kaspersky Thin Client.

## Настройка параметров в разделе RDP

В разделе RDP (см. рис. ниже) вы можете изменять параметры подключения к удаленному рабочему столу попротоколу RDP.




Раздел RDP

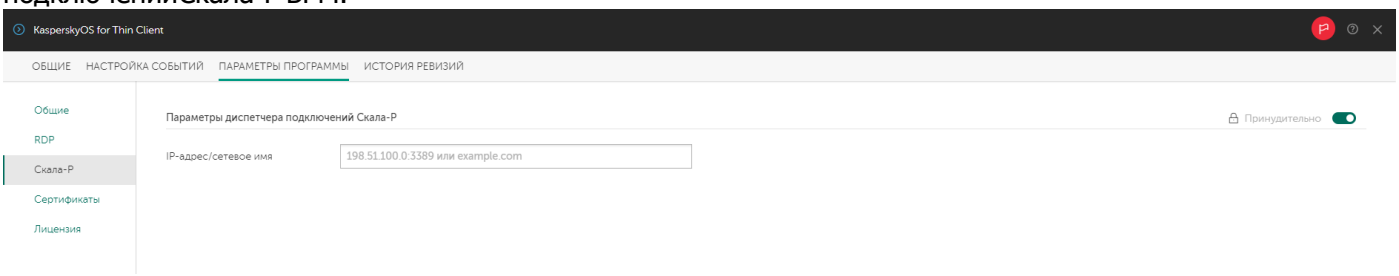
Параметры раздела RDP

| Параметр | Описание |
|---|---|
| IP-адрес/сетевое имя сервера | IP-адрес или имя сервера удаленного рабочего стола. |
| USB-накопители | Если флажок установлен, то Kaspersky Thin Client пробрасывает локальные USB-накопители на удаленный рабочий стол. |
| Смарт-карты | Если флажок установлен, то Kaspersky Thin Client пробрасывает локальные смарт-карты и токены на удаленный рабочий стол. |
| Сглаживание шрифтов | Если флажок установлен, то на удаленном рабочем столе включается сглаживание шрифтов. |
| Анимация меню | Если флажок установлен, то на удаленном рабочем столе включаетсяанимацию меню. |
| Фон рабочего стола | Если флажок установлен, то на удаленном рабочем столе отображаются обоирабочего стола Windows. |
| Содержимое окна при перетаскивании | Если флажок установлен, то при перетаскивании окон на удаленном рабочем столе отображается их содержимое. |
| Улучшенное оформление | Если флажок установлен, то на удаленном рабочем столе включается тема визуального оформления, установленная в Windows. |

Если переключатель **Принудительно**, находящийся напротив названия группы параметров, включен, то параметры из этой группы нельзя изменять в Kaspersky Thin Client или в параметрах отдельного устройства. Они принудительно передаются с Kaspersky Security Center и применяются в Kaspersky Thin Client.

# Настройка параметров в разделе Скала-Р

В разделе Скала-Р (см. рис. ниже) вы можете изменять параметры подключения к диспетчеру подключенийСкала-Р BPM.




Раздел Скала-Р

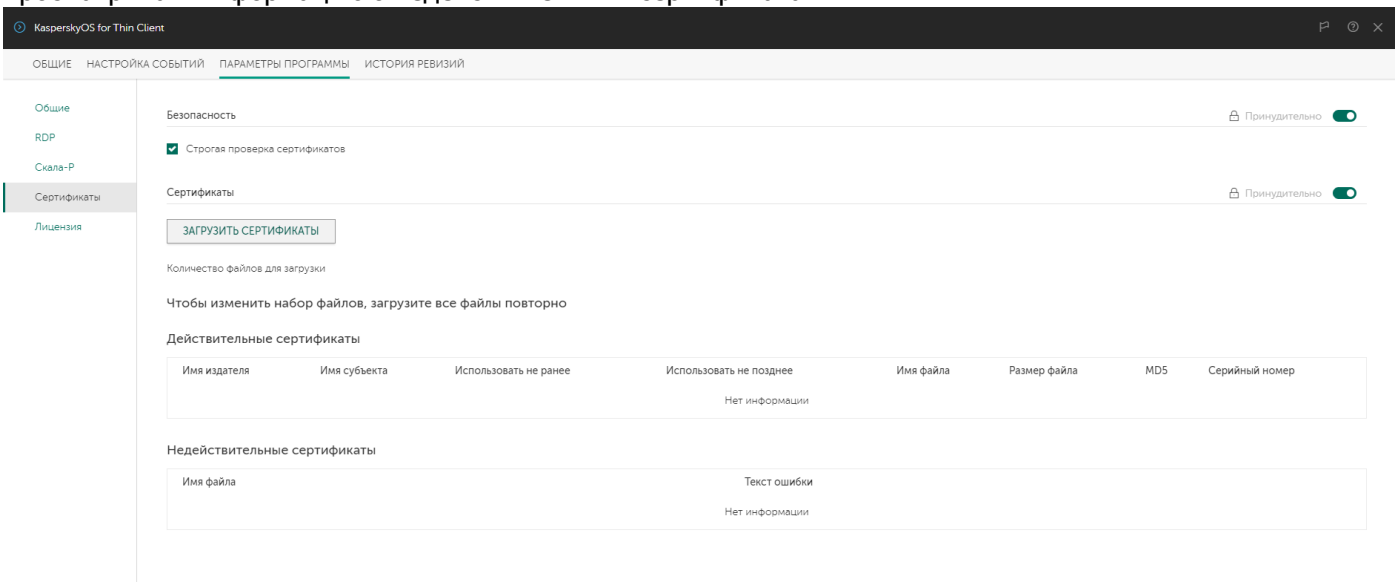
Параметры раздела Скала-Р

| Параметр | Описание |
|---|---|
| IP-адрес/сетевое имя | IP-адрес или имя сервера котором расположен диспетчер подключений Скала-Р BPM. |

Если переключатель **Принудительно**, находящийся напротив названия группы параметров, включен, то параметры из этой группы нельзя изменять в Kaspersky Thin Client или в параметрах отдельного устройства. Они принудительно передаются с Kaspersky Security Center и применяются в Kaspersky Thin Client.

## Настройка параметров в разделе Сертификаты

В разделе Сертификаты (см. рис. ниже) можно изменять параметры работы с SSL сертификатами, которые используются Kaspersky Thin Client для проверки подлинности RDP-серверов и Kaspersky Security Center. Вы можете изменять режим проверки сертификатов, загружать новые сертификаты и просматриватьинформацию о недействительных сертификатах.




Раздел Сертификаты

Параметры раздела Сертификаты

| Параметр | Описание |
|---|---|
| Строгая проверка сертификатов | Строгая проверка SSL сертификатов RDP-сервера и Kaspersky Security Center.<br><br>При первой настройке тонких клиентов рекомендуется выключить этот параметр, так как если во время подключения тонкого клиента произойдет ошибка проверки сертификата, доступ к этому тонкому клиенту из Kaspersky Security Center будет заблокирован. |

Если переключатель **Принудительно**, находящийся напротив названия группы параметров, включен, то параметры из этой группы нельзя изменять в Kaspersky Thin Client или в параметрах отдельного устройства. Они принудительно передаются с Kaspersky Security Center и применяются в Kaspersky Thin Client.

Чтобы добавить новые сертификаты, выполните следующие действия:

1. Нажмите на кнопку Загрузить сертификаты.

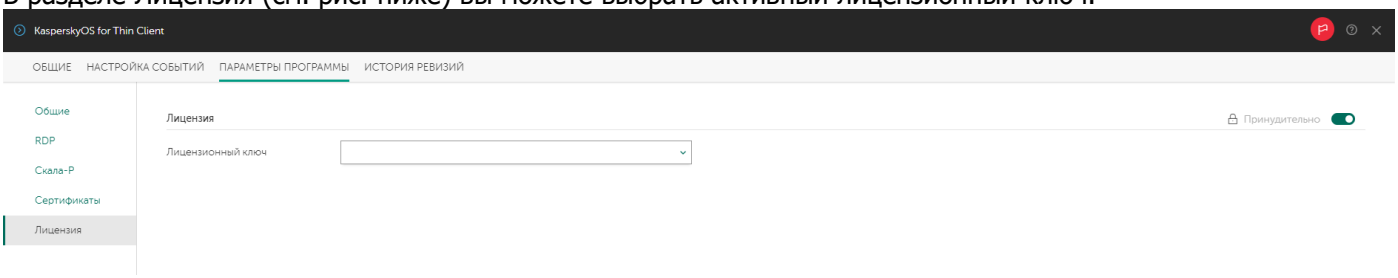
   Появится окно выбора файлов.

2. Выберите все сертификаты, которые были загружены ранее и новые сертификаты.

3. Загрузите выбранные сертификаты.

## Настройка параметров в разделе Лицензия

В разделе Лицензия (см. рис. ниже) вы можете выбрать активный лицензионный ключ.




Раздел Лицензия

Параметры раздела Лицензия

| Параметр | Описание |
|---|---|
| Лицензионный ключ | Активный лицензионный ключ. |

Если переключатель **Принудительно**, находящийся напротив названия группы параметров, включен, то параметры из этой группы нельзя изменять в Kaspersky Thin Client или в параметрах отдельного устройства. Они принудительно передаются с Kaspersky Security Center и применяются в Kaspersky Thin Client.

## Настройка параметров Kaspersky Thin Client для отдельных тонких клиентов

Вы можете настраивать параметры для отдельных тонких клиентов через Kaspersky Security Management Suite.

Чтобы настроить параметры Kaspersky Thin Client для отдельного тонкого клиента, выполните следующие действия:

В главном окне Kaspersky Security Management Suite выберите Устройства → Управляемые устройства.

1. Нажмите на имя тонкого клиента, параметры которого вы хотите настроить.Откроется окно свойств тонкого клиента.

2. Выберите закладку Программы.

3. Нажмите на название Kaspersky Thin Client.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

4. Выберите закладку Параметры программы.

Следующие разделы с параметрами доступны для изменения на отдельных тонких клиентах:

- Общие.
- RDP.
- Скала-Р.

5. Измените желаемые параметры.

6. Нажмите на кнопку Сохранить.

## Параметры отдельных тонких клиентов

### Закладка Общие

На закладке Общие можно просматривать информацию о программном обеспечении, установленном на тонком клиенте и лицензионных ключах для этого программного обеспечения:

- Закладка Информация содержит информацию о программном обеспечении, установленном на тонкийклиент.

- Закладка Лицензия содержит информацию об активном и резервном лицензионных ключах для программного обеспечения, установленного на тонкий клиент.

### Закладка События

На закладке **События** отображаются события, произошедшие на этом устройстве.

### Закладка Настройка событий

О настройке событий см. раздел "Настройка параметров политик", подраздел "Закладка Настройка событий".

### Закладка Параметры программы

О настройке параметров Kaspersky Thin Client для отдельных тонких клиентов см. раздел "Настройка параметров Kaspersky Thin Client для отдельных тонких клиентов".

# Устранение неисправностей

При возникновении ошибки требуется убедиться в следующем:

1. Тонкий клиент включен.

2. Тонкий клиент подключен к сети.

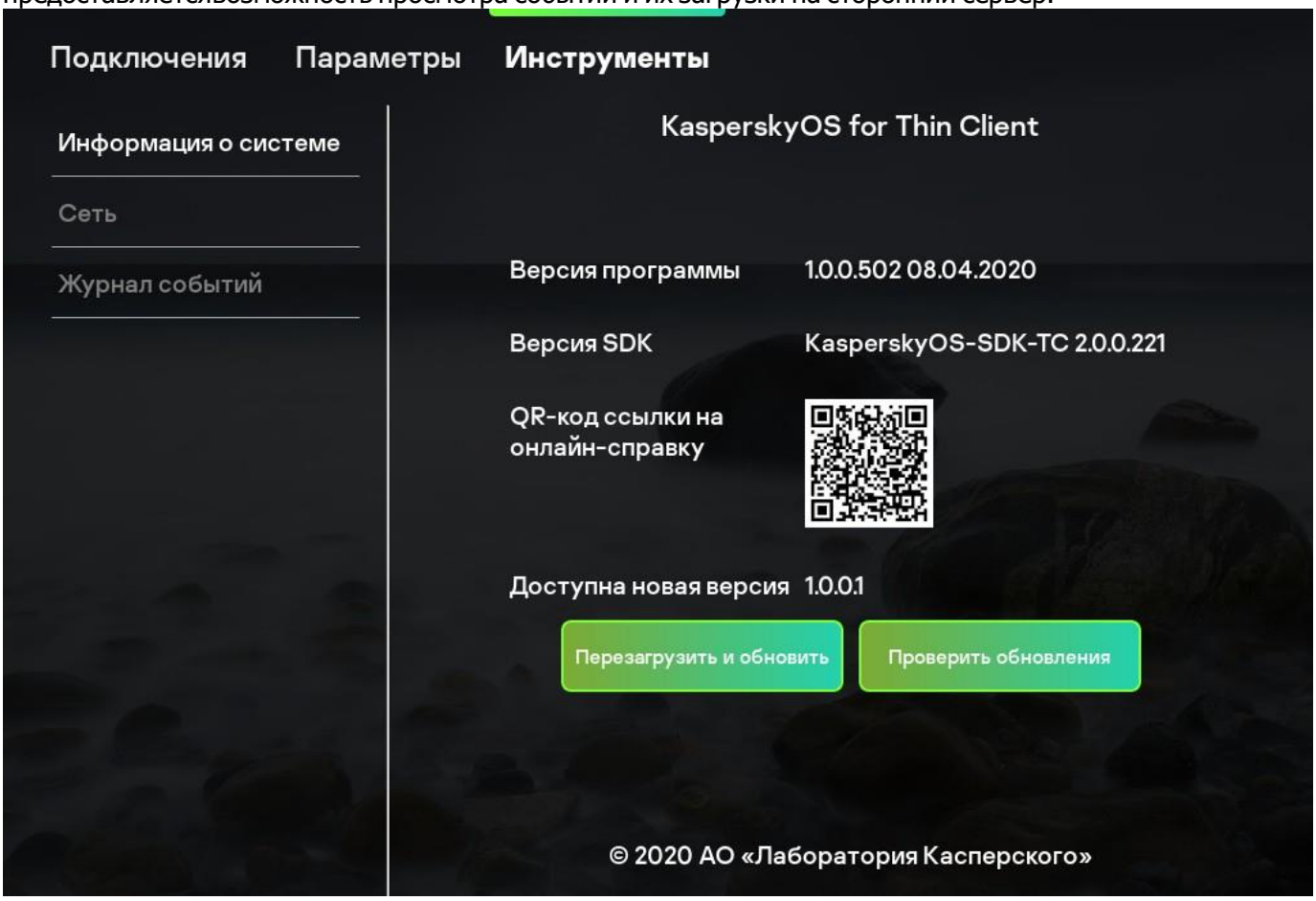
3. При подключении к удаленному рабочему столу были введены верные IP-адрес или имя сервера, имя пользователя и пароль.

Если устранить ошибку не удается, обратитесь в Службу технической поддержки. При необходимости специалисты Службы технической поддержки могут запросить у вас сведения о системе и / или журнал событий.

## Просмотр сведений о системе

На закладке Инструменты вы можете получить доступ к информации, которая требуется Службе технической поддержки для анализа и устранения сбоев в работе Kaspersky Thin Client. Закладка содержит следующие разделы:

- Информация о системе. На этой закладке отображаются версии Kaspersky Thin Client и ее компонентов, а также сведения о правообладателе.
- Сеть. На этой закладке отображаются сведения о сети (например, MAC- и IP-адреса, статус подключения).
- Журнал событий. На этой закладке отображаются записи о событиях системы, а также предоставляетсявозможность просмотра событий и их загрузки на сторонний сервер.




Окно сведений о системе

## Отправка журнала событий на сторонний сервер

В некоторых случаях Служба технической поддержки может запросить журнал событий для анализа работысистемы. Для этого вам нужно отправить журнал событий с тонкого клиента на сервер внутри вашей организации и переслать Службе технической поддержки удобным для вас способом.

Чтобы отправить журнал событий на сторонний сервер, выполните следующие действия:

1. Убедитесь, что тонкий клиент подключен к сети.

2. Выберите закладку Инструменты.

3. Перейдите в раздел Журнал событий.

В разделе Журнал событий отображаются все сохраненные на тонком клиенте события системы.

4. В поле Адрес для отправки укажите значение веб-адреса сервера для отправки журнала событий.

5. Нажмите на кнопку Отправить.

> На сервер будут отправлены все события, сохраненные на тонком клиенте.

6. Нажмите на кнопку **Да** в окне подтверждения операции.
7. Если журнал событий отправить не удалось, убедитесь, что адрес сервера журнала событий указан верно и есть подключение к сети. Если оба условия выполнены, но журнал событий не удается отправить, обратитесь в Службу технической поддержки.

## Ошибки подключения

В этом разделе перечислены возможные ошибки подключения к удаленному рабочему столу, а также описаны шаги, которые следует предпринять для их устранения.

Если в работе системы Kaspersky Thin Client возникли ошибки подключения, не описанные в этом разделе, рекомендуется обратиться в Службу технической поддержки.

## Проверка подключения к сети

Чтобы проверить, подключен ли тонкий клиент к сети, посмотрите на значок состояния сети в правой части панели состояния.

## Неверное имя пользователя или пароль

Подключение к удаленному рабочему столу может быть не установлено из-за неверно указанных именипользователя и пароля.

Чтобы подключиться к удаленному рабочему столу, выполните следующие действия:

1. Укажите верные IP-адрес или имя сервера, имя пользователя и пароль.

2. Если вы уверены, что правильно ввели имя пользователя и пароль, но при попытке подключиться все равно отображается ошибка, убедитесь, что указываете правильное имя или IP-адрес сервера, к которому хотите подключиться.

## Некорректно введенные данные

Перед инициацией подключения к удаленному рабочему столу система Kaspersky Thin Client проверяет корректность следующих введенных пользователем данных:

- IP-адреса или имени сервера.
- Имени пользователя.

Если формат указанных сведений отличается от ожидаемого системой, в нижней части окна подключения кудаленному рабочему столу отображается сообщение о некорректности данных.

> Ошибок может быть несколько: требуется навести курсор на сообщение в нижней части окна подключения к удаленному рабочему столу, чтобы в окне всплывающей подсказки просмотреть их полный список.

Чтобы подключиться к удаленному рабочему столу, укажите верные IP-адрес или имя сервера, имя пользователя и пароль.

## Разрыв соединения с удаленным рабочим столом

При возникновении ошибки, приводящей к разрыву соединения Kaspersky Thin Client с удаленным рабочим столом, экран рабочего стола закрывается и отображается сообщение с указанием причины сбоя.

Чтобы возобновить работу на удаленном рабочем столе, выполните следующие действия:

1. Закройте сообщение об ошибке, нажав на кнопку ОК.

2. Попробуйте подключиться к удаленному рабочему столу.

3. Если подключение установить не удалось, остановите систему и запустите ее заново, а затем снованопробуйте подключиться к удаленному рабочему столу.

4. Если по-прежнему не удается подключиться к удаленному рабочему столу, обратитесь в Службутехнической поддержки.

## Обращение в Службу технической поддержки

При возникновении неисправностей в работе Kaspersky Thin Client, которые не удается решить самостоятельно, обратитесь к специалистам Службы технической поддержки, используя указанные нижеканалы связи:

1. По электронной почте: kos-support@kaspersky.com

2. На портале https://companyaccount.kaspersky.com. Для регистрации на портале вам нужна действующая лицензия.

Kaspersky Thin Client включает в себя функциональность расширенного журналирования, которая может быть включена по запросу инженера технической поддержки для целей получения технической поддержки. В этом случае вам будет предоставлена инструкция по использованию этой функциональности.

# Ограничения

В этом разделе описаны ограничения системы Kaspersky Thin Client версии 1.0:

1. Не поддерживаются дисплеи, имеющие разрешение, превосходящее FullHD (1920x1080).

2. Не поддерживается подключение к тонкому клиенту более одного монитора.

3. Не поддерживается подключение мониторов во время работы Kaspersky Thin Client.

4. Пользователь не может устанавливать собственный файл в качестве обоев рабочего стола Kaspersky Thin Client.

5. Kaspersky Thin Client не поддерживает передачу звука.

6. Не поддерживается протокол IPv6.

7. Не поддерживается изменение набора доступных в Kaspersky Thin Client раскладок клавиатуры.

8. Не поддерживается изменение комбинации клавиш, используемых в системе Kaspersky Thin Client для смены раскладки клавиатуры.

9. На удаленный рабочий стол невозможно передать комбинацию клавиш **Ctrl+Alt+Home**. Если эта комбинация клавиш используется для вызова какой-либо функции программы на удаленном рабочемстоле, следует изменить настройки этой программы.

10. Пользователь не может менять положение панели подключения или полностью скрыть ее.

11. Из-за технических ограничений функциональность, связанная с лицензионными ключами для Kaspersky Thin Client, не всегда работает корректно:

- При смене лицензионного ключа в политикеKaspersky Security Center или при добавлении нового устройства в группу, информация об устройствах, использующих лицензию, будет обновляться в Kaspersky Security Center с задержкой, по мере того как тонкие клиенты будут синхронизироваться сKaspersky Security Center.

- Если лицензионный ключ был удален из Kaspersky Security Center или отозван, но политика с тех порне обновлялась, статус тонкого клиента не изменится.

12. Не поддерживается синхронизация времени по протоколу NTP.

13. Для настройки часового пояса требуется указать смещение относительно UTC.

14. Не поддерживается автоматический перевод часов на летнее и зимнее время.

# Глоссарий

## Heartbeat

Периодический сигнал, отправляющийся программным или аппаратным обеспечением для индикацииработочего состояния.

## Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими какединым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

## Событие

Запись, содержащая информацию о изменении состояния или конфигурации тонкого клиента, илипроизошедших ошибках, потенциально требующих внимания системного администратора.

# Информация о стороннем коде

Информация о стороннем коде содержится в файле LegalNotices.txt, который входит в комплект поставки.

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Google, Chrome – товарные знаки Google, Inc.

Microsoft, Access, Active Directory, Excel, Internet Explorer, Outlook, PowerPoint, Windows и Windows Server –товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

JavaScript – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.