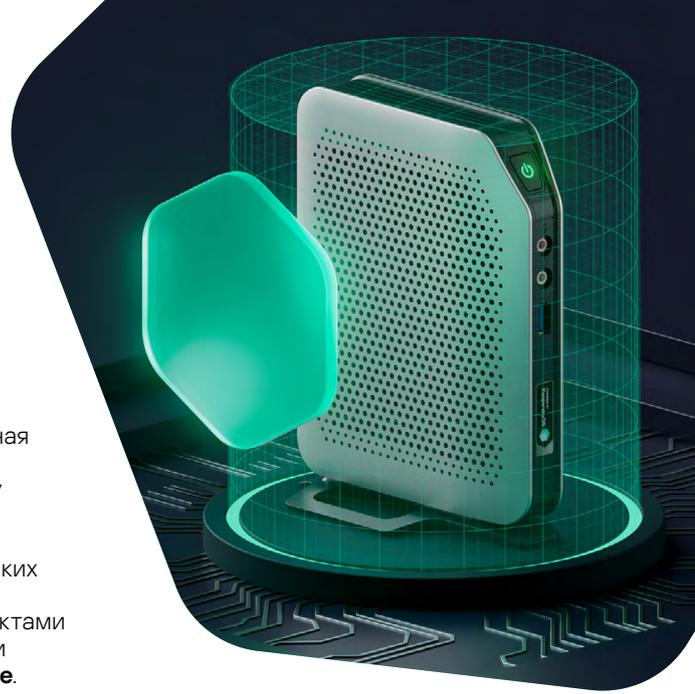




Kaspersky Thin Client

Kaspersky Thin Client — защищенная на уровне архитектуры операционная система для тонких клиентов на базе KasperskyOS. Такие тонкие клиенты предназначены для предоставления пользователю доступа к удаленному рабочему столу и служат заменой локальной рабочей станции.

Для централизованного и безопасного управления инфраструктурой тонких клиентов с Kaspersky Thin Client используется единая консоль **Kaspersky Security Center**. Также она применяется для управления и другими продуктами «Лаборатории Касперского». Для подключения тонких клиентов к консоли предусмотрен модуль расширения **Kaspersky Security Management Suite**.



Гибкое управление тонкими клиентами

Централизованная система управления	С помощью консоли Kaspersky Security Center выполняется: <ul style="list-style-type: none">• настройка тонких клиентов;• проверка наличия обновлений и обновление ПО тонких клиентов;• сбор системных событий с тонких клиентов для аудита и исправления неполадок.
Автоматическая настройка	Быстрая интеграция тонких клиентов в инфраструктуру благодаря автоматическому подключению и получению настроек от Kaspersky Security Center.
Разграничение прав доступа к настройкам администрирования	Каждый администратор может обращаться только к тем настройкам управления тонкими клиентами, которые имеют отношение к его служебным обязанностям.
Гибкая система отчетности	<ul style="list-style-type: none">• Настраиваемые отчеты с динамической фильтрацией и сортировкой по любому полю.• Информативный дашборд, позволяющий быстро получить все необходимые сведения.
Управление настройками тонкого клиента	<ul style="list-style-type: none">• Откат настроек тонкого клиента к заводским значениям.• Управление доступом пользователя к настройкам тонкого клиента.
Совместимость с Kaspersky Security Center	Поддерживается Kaspersky Security Center версий: 14.2.

Защита тонких клиентов от кибератак

Исходная безопасность (Security by Design)	Заложенный в архитектуру KasperskyOS принцип Security by Design и разработка решения с использованием кибериммунной методологии исключают возможность эксплуатации широкого набора уязвимостей, присущих тонким клиентам других производителей.
Безопасная передача данных	Обеспечение целостности данных, передаваемых между пользователями, удаленным рабочим столом, сервером централизованного управления, серверами инфраструктуры удаленных рабочих столов и журналирования. Отсутствие необходимости в наложенных средствах защиты.
Безопасное обновление	Централизованное автоматическое получение обновлений от сервера обновлений «Лаборатории Касперского» с помощью Kaspersky Security Center. Администратору доступно централизованное ознакомление и принятие условий EULA для новых версий КТС и управление доставкой обновлений на тонкие клиенты.
Контроль сетевых подключений	С помощью сертификатов контролируется: <ul style="list-style-type: none">• подключение пользователей к удаленным рабочим столам и брокерам;• подключение тонких клиентов к системе централизованного управления и серверу журналирования.
Резервные сертификаты для Kaspersky Security Center	Автоматическая и прозрачная для администратора Kaspersky Security Center доставка резервного сертификата в системное хранилище сертификатов Kaspersky Thin Client.
Безопасная миграция на новый сервер Kaspersky Security Center	Безопасное подключение тонкого клиента к Kaspersky Security Center с сертификатом, отличным от текущего.

Аппаратная платформа

TONK TN 1200

Компактный и производительный тонкий клиент для организации удаленного рабочего места пользователя. Особенности: пассивное охлаждение, ремонтпригодность, установка на подставке или за монитор (VESA-крепление).
TONK TN1200 внесен в реестр Минпромторга РФ на основании заключения № 40608/11. Номер реестровой записи – 1018\1\2023.

Сценарии подключения

Терминальные серверы и гостевые операционные системы

Подключение по протоколу RDP к гостевым операционным системам:

- Microsoft Windows 7
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Astra Linux Common Edition 2.12.43 (Орел)
- Astra Linux Special Edition 1.7 (Смоленск)
- Alt Linux 10
- РЕД ОС 7.3

Поддерживаемые инфраструктуры удаленных рабочих столов и способы подключения

Microsoft Remote Desktop Services:

- Windows Server 2016/2019/2022
- Базис.WorkPlace:
- Windows 10/11
 - Windows Server 2016/2019/2022
 - Astra Linux SE 1.7/CE 2.12, ALT Linux 10 и РЕД ОС 7.3

Citrix и VMware Horizon (no HTML5):

- Windows 10/11
- Windows Server 2016/2019/2022

Терминальное подключение:

- Windows Server 2016/2019/2022 (в том числе в MS RDS)
- Astra Linux SE 1.7/CE 2.12, ALT Linux, РЕД ОС 7.3

Прямое подключение:

- Windows 7/10/11
- Windows Server 2016/2019/2022
- Astra Linux SE 1.7/CE 2.12, ALT Linux 10, РЕД ОС 7.3

Виртуальные приложения

Поддерживается подключение к отдельным бизнес-приложениям:

- развернутым в инфраструктуре Microsoft Remote Desktop Services (Windows Server 2016/2019/2022)
- развернутым на терминальных серверах Windows Server 2016/2019/2022
- работающим под управлением Windows 10/11

Автоматическое подключение

При разрыве RDP-соединения переподключение к удаленному рабочему столу происходит автоматически.

Возможности интерфейса для пользователя

Мониторы

Поддерживается подключение до двух мониторов по HDMI и DisplayPort. Разрешение изображения удаленного рабочего стола – до FullHD+ (1920x1200).

USB-устройства

Передача флеш-накопителей, смарт-карт, принтеров и токенов, подключенных к тонкому клиенту, на удаленный рабочий стол под управлением поддерживаемых версий Windows и Linux.

Аудио

Воспроизведение и передача звука в операционную систему удаленного рабочего стола.

Аудиоконференции

Поддерживаются аудиоконференции в решениях VideoMost, IVA Technologies и SPIRIT DSP.

Дополнительные функции

Интерфейс и возможности для пользователя

- Настраиваемая панель управления Kaspersky Thin Client, не перекрывающая важные элементы удаленного рабочего стола.
- Настройка языков ввода: выбор только необходимых пользователю раскладок клавиатуры.
- Настройки интерфейса в соответствии с индивидуальными предпочтениями.
- Расширенная система уведомлений. Например, система опрашивает пользователя об удобном времени перезагрузки.
- Детализированные сообщения об ошибках с советами по их устранению.
- Автоматическое переподключение к удаленному рабочему столу в случае разрыва соединения.

Контроль со стороны администратора

Администратор может гибко управлять настройками пользователя, например, запретить использование микрофона, наушников или второго монитора.

Настройка параметров энергосбережения

Настройка выключения питания монитора и тонкого клиента при бездействии Kaspersky Thin Client.

Отложенная установка обновлений

Возможность для пользователя отложить установку обновления Kaspersky Thin Client на фиксированное количество времени.

os.kaspersky.ru
www.kaspersky.ru

© 2024 АО «Лаборатория Касперского»
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

