Защита рабочего места средствами операционной системы РЕД ОС

Заместитель директора департамента развития системных продуктов

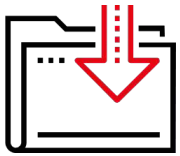
Ивлев Иван Васильевич

РЕДСОФТ

Москва, 2021

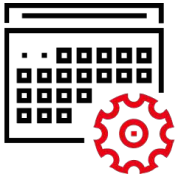
О РЕД ОС

РЕДОС



1

Linux дистрибутив RPM-формата



2

Разрабатывается с **2014** года

3

Исключительные права **РЕД СОФТ**

4

Единый реестр российских программ для ЭВМ и баз данных Минкомсвязи России (№3751)

РЕД ОС - история релизов и техническая политика

- Срок сопровождения релиза — 3 года с момента выпуска
- Ежегодный выпуск релизов
- «Мягкий» переход без необходимости переустановки
- Выпуск релизов по классической схеме (LTS)

РЕД ОС 7.3

- LTS ядро версии 5.10 с полноценной поддержкой процессоров INTEL 10 поколения и графических карт AMD iGPU Vega 6
- Расширен перечень поддержки периферийного оборудования
- Обновленные библиотеки драйверов для Epson, HP, Canon
- Актуализированы версии пакетов
- Сертификация по новым требованиям уровней доверия Приказа ФСТЭК России от 2 июня 2020 г. №76
- Сертификация ФСТЭК России плановый срок – 3 квартал 2021
- Бесплатное обновление для действующих клиентов технической поддержки
- Бесплатно для физических лиц в целях некоммерческого использования, а также для изучения и тестирования

РЕД ОС состав продукта

РЕДАКЦИИ

- «Стандартная» - наиболее свежий и актуальный набор пакетов
- «Сертифицированная» - сертифицирована ФСТЭК России

КОНФИГУРАЦИИ

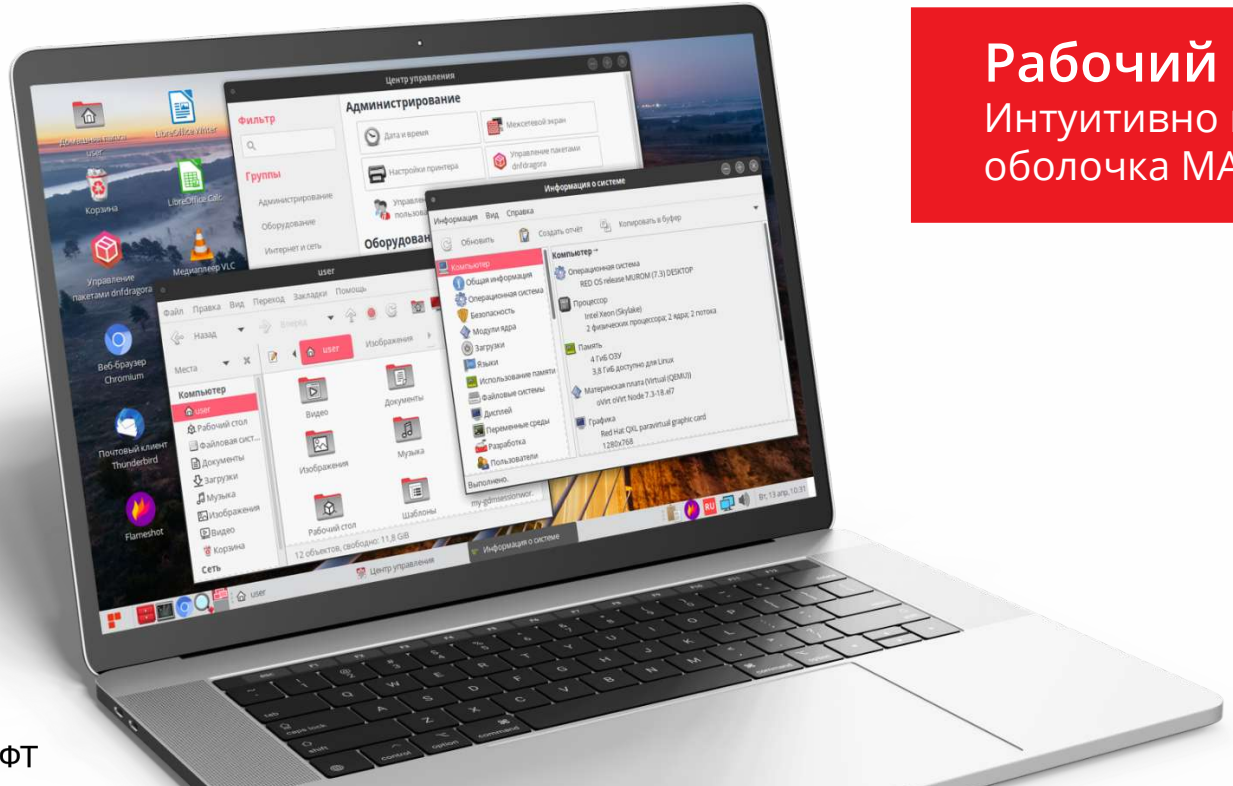
- «Сервер»
  - терминальный
  - графический
- «Рабочая станция»

АРХИТЕКТУРЫ

- x86_64, i686
- aarch64
  - Raspberry Pi
  - Байкал–M
  - Байкал-C
  - Huawei Taishan (Kunpeng)
- e2k (Эльбрус)

ЭКО-система РЕД ОС

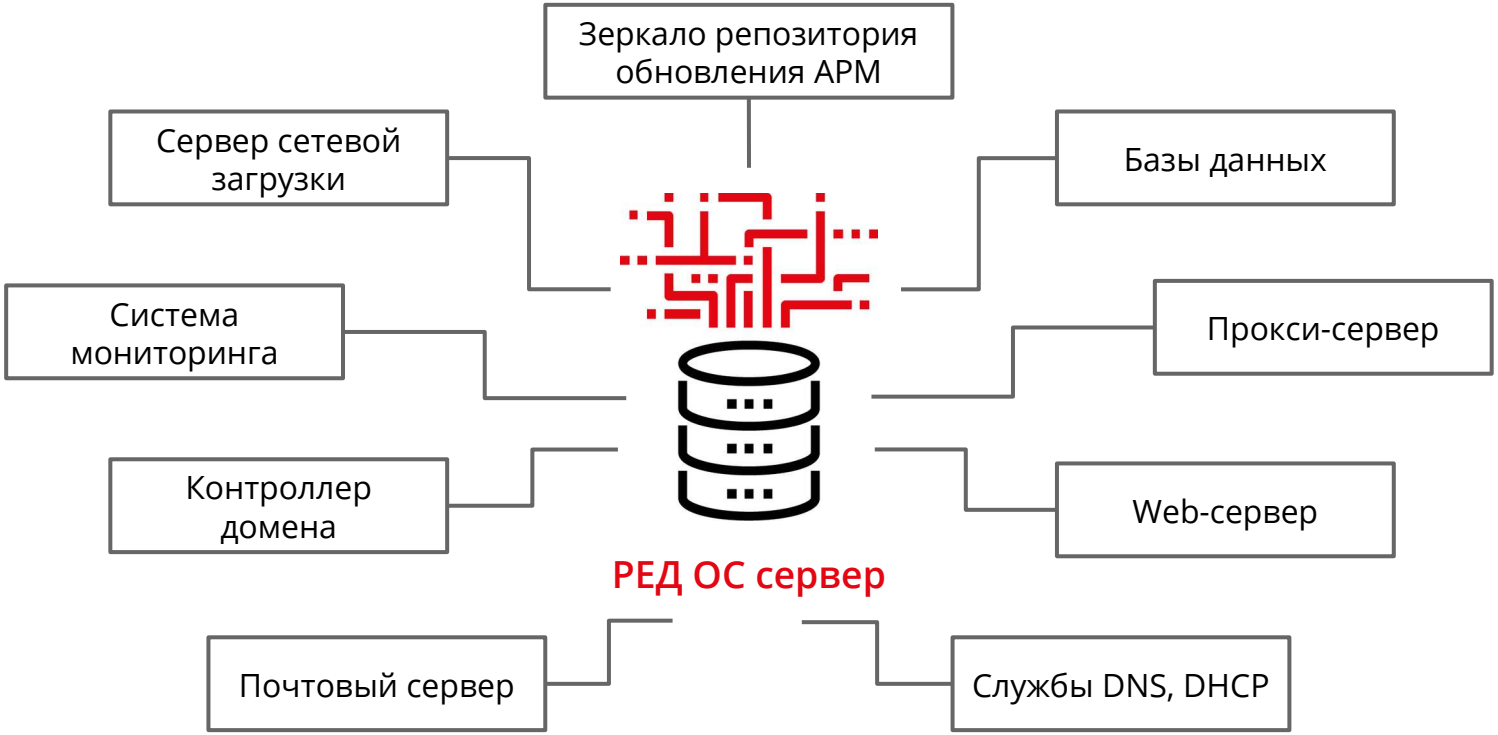
РЕД ОС сегодня



Рабочий стол

Интуитивно понятная графическая оболочка MATE

РЕД ОС конфигурация “Сервер”



Сертификация

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4060

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
12 января 2019 г.

Выдан: 12 января 2019 г.
Действителен до: 12 января 2024 г.

Настоящий сертификат удостоверяет, что **операционная система «РЕД ОС»**, разработанная и производимая ООО «РЕД СОФТ» в соответствии с техническими условиями ТУ 02.01-001-29926343-2017, является операционной системой, соответствует требованиям по безопасности информации, установленным в документах «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016) и «Профиль защиты операционных систем типа А четвертого класса защиты. ИТ.ОС.А4.ПЗ» (ФСТЭК России, 2017) при выполнении указаний по эксплуатации, приведенных в формуляре RU.29926343.02.01-01 30.

Сертификат выдан на основании технического заключения от 02.11.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией ЗАО ГИЦ ПС ВТ (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.Б005), и экспертного заключения от 26.11.2018, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: ООО «РЕД СОФТ»
Адрес: 105066, г. Москва, ул. Доброслободская, д. 6 стр. 1, эт. 4, пом. I, ком. 7
Телефон: (495) 285-6268

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Сертификат **ФСТЭК России №4060 от 12.01.2019 г.**
Профиль защиты **ИТ.ОС.А4.ПЗ**

РЕД ОС может применяться:

- **ИСОП** до **II класса** включительно
- **АСУ ТП** до **I класса** защищенности включительно
- **ГИС** до **I класса** защищенности включительно
- **ИСПДн** до **I уровня** защищенности включительно
- **КИИ** до **I категории значимости** включительно

Регулярная проверка технической поддержки с привлечением испытательной лаборатории

Элементы безопасности РЕД ОС

- списки управления доступом
- реализация доменов и типов
- журналируемая файловая система (ext4)
- подключаемые модули аутентификации (PAM)
- специализированная подсистема аудита критичных событий безопасности с возможностью конфигурирования и оценки записей
- базовые функции проверки комплекта оборудования позволяют
- администратору сверять правильность функций безопасности аппаратных средств, на которые полагается операционная система

Сертифицированная редакция РЕД ОС имеет расширенные элементы безопасности по сравнению со стандартными системами UNIX

Система производства РЕД ОС

- проведение испытаний и поддержка безопасности средства
- разработка полного комплекта проектной (программной) и эксплуатационной документации
- определение надежных и безопасных средств разработки
- управление конфигурацией средства.
- обязательное статическое, динамическое, фаззинг-тестирование средства
- выявление уязвимостей и недекларированных возможностей,
- проведение анализа скрытых каналов

Система производства РЕД ОС полностью удовлетворяет требованиям к разработке и производству средств защиты информации по профилю ОС типа «А» четвертого класса защиты ИТ.ОС.А4.ПЗ

РЕД ОС реализует 10 из 17 базовых наборов мер ИБ

Требования к мерам защиты

- I. Идентификация и аутентификация (ИАФ)
- II. Управление доступом (УПД)
- III. Ограничение программной среды (ОПС)
- IV. Защита машинных носителей информации (ЗНИ)
- V. Аудит безопасности (АУД)
- VI. Антивирусная защита (АВЗ)
- VII. Предотвращение вторжений (компьютерных атак) (СОВ)
- VIII. Обеспечение целостности (ОЦЛ)
- IX. Обеспечение доступности (ОДТ)
- X. Защита технических средств и систем (ЗТС)
- XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- XII. Реагирование на компьютерные инциденты (ИНЦ)
- XIII. Управление конфигурацией (УКФ)
- XIV. Управление обновлениями программного обеспечения (ОПО)
- XV. Планирование мероприятий по обеспечению безопасности (ПЛН)
- XVI. Обеспечение действий в нештатных ситуациях (ДНС)
- XVII. Информирование и обучение персонала (ИПО)

Требования к мерам защиты

- Формирование требований
- Разработка системы защиты
- Внедрение системы защиты
- Обеспечение защиты в ходе эксплуатации
- Обеспечение защиты при выводе из эксплуатации

Мера реализуется средствами ОС

Мера реализуется неизвестными СЗИ

Организационная мера

РЕДСОФТ

Сопоставление мер и реализации ФБО в РЕД ОС

Меры защиты информации, содержащейся в ГИС/ИСПДн, в соответствии с требованиями приказов ФСТЭК России №17/21, и способов их реализации средствами РЕД ОС

Примечание.
Иные меры, не рассмотренные в данном документе, должны быть реализованы организационными или иными мерами.

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Возможная реализация меры защиты с помощью РЕД ОС	Возможная совместная реализация меры защиты с помощью РЕД ОС и иных СЗИ	Операционная система «РЕД ОС». Руководство администратора RU.29926343.02.01-01 32 1-1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Реализована идентификация и аутентификация пользователей, в том числе с поддержкой многофакторной аутентификации на базе PAM модулей. Все запускаемые процессы однозначно сопоставляются с пользователем, запустившим его. Аутентификация осуществляется по локальной базе паролей.	Построение систем многофакторной аутентификации с применением средств идентификации и аутентификации, в том числе при построении аутентификации с помощью серверов аутентификации.	6.7. PAM, 7. Управление пользователями
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Все подключаемые устройства однозначно идентифицируются системой. Для аутентификации устройство можно использовать фреймворк Polkit и, например, разрешать монтирование новых устройств с запросом пароля определенного пользователя или с запросом пароля пользователя root.	Использование программно-аппаратных комплексов доверенной загрузки для контроля подключаемых устройств.	3. Общие принципы работы РЕД ОС
ИАФ.3	Управление идентификаторами, в том числе создание, присв[illegible] уничтож[illegible]	ОС позволяет формировать идентиф[illegible] и присваивать их. Использую у[illegible] администратор[illegible]	При использовании многофакторной аутентификации [illegible]ронних СЗИ	6.7. PAM, 7. Управление пользователями

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России
11 февраля 2014 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ
В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

2014

РЕДСОФТ

Совместимость с СЗИ и СКЗИ

Комплексная защита ИС

infotecs, Эшелон комплексная безопасность, КОД БЕЗОПАСНОСТИ

СКЗИ

КРИПТОПРО, криптоком системы защиты информации, Аладдин рд, КриптоАРМ, ФАКТОР-ТС, Компания Актив

SIEM

POSITIVE TECHNOLOGIES, GIS ГАЗИНФОРМ СЕРВИС, VISOR гибкость. ясность. безопасность

Антивирусная защита

kaspersky, Dr.WEB

DLP-системы

STAFFCOP, ГАРДА ТЕХНОЛОГИИ, SEARCHINFORM INFORMATION SECURITY, DOCSHELL, ZECURION, Ростелеком Солар

Средства анализа защищенности

Сканер-ВС анализ защищенности, RED Check

СЗИ от НСД

АПР ОКБ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА DALLAS LOCK LINUX

Обновления безопасности РЕД ОС

В соответствии с требованиями ФСТЭК России в РЕД ОС обеспечивается постоянный поиск уязвимостей, разрабатываются обновления безопасности и компенсирующие меры для невозможности эксплуатации уязвимостей. Сведения об обновлениях безопасности, а также подробная информация об их применении.

Технологические партнеры

Средства защиты информации

КРИПТОПРО
infotecs
kaspersky
Аладдин рд
Dr.WEB
КриптоАРМ
АПКОКБ
Компания Актив
КОД БЕЗОПАСНОСТИ
GIS ГАЗИНФОРМ СЕРВИС
STAFFCOP
Акронис Инфозащита
Эшелон комплексная безопасность
REDCheck
КОНФИДЕНТ ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Прикладное ПО

Р7-ОФИС
МойОфис
Циркон
Спутник
Яндекс
КонсультантПлюс надежная правовая поддержка
CommuniGate Pro
DIRECTUM Электронный документооборот и управление взаимодействием
Гарант
TrueConf
VIDEOMOST.com video conferencing server
КОДЕКС
ассистент
CompanyMedia
ЭОС

Аппаратное обеспечение

HUAWEI
Baikal ELECTRONICS
AQUARIUS
iru
DEPO [computers]
ICL ТЕХНО
МЦСТ ЭЛЬБРУС
TONK
EPSON EXCEED YOUR VISION
Lenovo
SITONICA
KYOCERA
РЕДСОФТ
brother
Canon
hp

Специализированное ПО

БФТ
Катарсис НАУЧНО-ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ
САПФИР НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ
КЕЙСИСТЕМС
НПО КРИСТА
NANOCAD УМНОЕ ПРОЕКТИРОВАНИЕ
1С
ГРАНД-Смета
БАРС ГРУП
ABBYY
1С-БИТРИКС
КОМЭКС КОМПЬЮТЕРИЗАЦИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ
BELLSOFT
AdAstrA RESEARCH GROUP, LTD

Защита рабочего места сотрудника на РЕД ОС

РЕД ОС - СЗИ, реализующее функции защиты **от несанкционированного доступа к информации.**

ОС включает функции безопасности: ИАФ, УПД, РСБ, ОПС, ЗИС, ЗНИ, ОЦЛ, АНЗ и т.д.

2ФА	Аладдин, Компания Актив
VPN	infotecs, Код безопасности
SIEM/DLP	RUSIEM, STAFFCOP, Positive Technologies, Ростелеком Солар
СКЗИ	КриптоПро, infotecs
АВЗ	kaspersky, Dr.Web
ОС	РЕДОС
МДЗ	infotecs, АПР ОКБ

РЕДСОФТ

«РАБОТАЕМ ДОМА»

ОРГАНИЗАЦИЯ УДАЛЕННОГО РАБОЧЕГО МЕСТА

1

Универсальность
Совместимо с любым x86_64 компьютером и ноутбуком.

2

Завершенность
Образ ОС содержит базовый набор приложений для работы (браузер, офисные пакеты) и удаленного доступа (RDP\VPN клиенты).

3

Безопасность
Защищенная сертифицированная ОС (сертификат ФСТЭК России по профилю ИТ.ОС.А4.ПЗ).

4

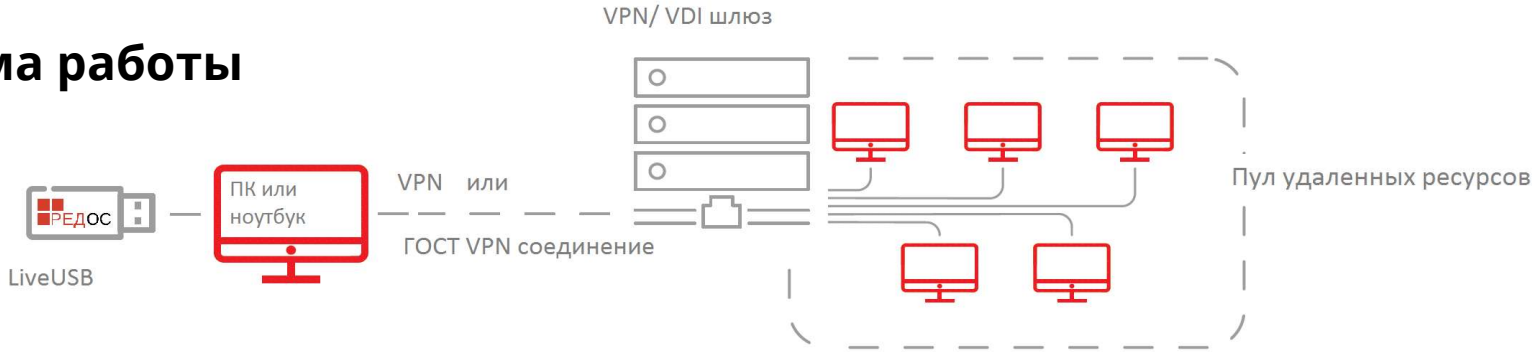
Защищенность
Работает в режиме “только чтение”, что исключает возможность внедрения в систему вредоносного кода.

РЕД ОС в режиме LiveUSB сделает любой компьютер доверенным!

«РАБОТАЕМ ДОМА»

ОРГАНИЗАЦИЯ УДАЛЕННОГО РАБОЧЕГО МЕСТА

Схема работы



1. Пользователь подключает **LiveUSB** с операционной системой **РЕД ОС** и загружается в доверенную среду, изолированную от основной ОС на компьютере. Вирусы и вредоносное ПО, которое возможно находится на домашнем ПК, недоступно в изолированной ОС.

2. Загрузив ОС, пользователь начинает работу в режиме - **«терминальный клиент»**

3. При загрузке ОС организуется защищённое VPN соединение к корпоративным ресурсам, что позволяет получить доступ к **удалённым рабочим столам** или **VDI** инфраструктуре, находящимся в закрытой сети. Базовые средства организации защищённого соединения и клиенты для удалённого доступа и VDI содержатся в составе ОС, установленной на LiveUSB.

4. По **завершении** работы пользователь выключает LiveUSB и загружает **домашнюю ОС.**

Благодарим за внимание!